# Contents

# Présentation de System Center Configuration Manager

22/06/2018 • 41 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Produit de la suite Microsoft System Center de solutions de gestion, System Center Configuration Manager peut vous aider à gérer les appareils et les utilisateurs localement et dans le cloud.

**Configuration Manager peut vous aider à :**

- améliorer la productivité et l'efficacité de vos services informatiques en réduisant les tâches manuelles et en vous permettant de vous concentrer sur des projets à forte valeur ;
- optimiser les investissements matériels et logiciels ;
- maîtriser la productivité des utilisateurs en leur fournissant les bons logiciels au bon moment.

**Configuration Manager vous permet d'offrir des services informatiques plus efficaces en prenant en charge :**

- Le déploiement de logiciels sécurisés et scalables.
- La gestion des paramètres de conformité.
- La gestion complète des ressources des serveurs, ordinateurs de bureau, ordinateurs portables et appareils mobiles.

**Configuration Manager s'étend et fonctionne avec vos solutions et technologies Microsoft existantes.**

Par exemple, Configuration Manager s'intègre aux éléments suivants :

- Microsoft Intune, pour gérer un vaste éventail de plateformes d'appareils mobiles.
- Windows Server Update Services (WSUS), pour gérer les mises à jour logicielles.
- Services de certificats.
- Exchange Server et Exchange Online.
- Stratégie de groupe Windows (GPO)
- DNS.
- Kit de déploiement et d'évaluation Windows (Windows ADK) et outil de migration utilisateur (USMT).
- Services de déploiement Windows (WDS).
- Assistance à distance et Bureau à distance.

Configuration Manager utilise également :

- Les services de domaine Active Directory pour la sécurité, l'emplacement du service, la configuration et pour découvrir les utilisateurs et les appareils que vous souhaitez gérer.
- Microsoft SQL Server comme base de données de gestion des modifications distribuée, qui s'intègre à SQL Server Reporting Services (SSRS) pour créer des rapports de surveillance et de suivi des activités de gestion.
- Des rôles de système de site qui étendent les fonctionnalités de gestion et l'utilisation des services web d'IIS (Internet Information Services).
- Le service de transfert intelligent en arrière-plan (BITS) et BranchCache pour gérer la bande passante réseau disponible.

Pour réussir avec Configuration Manager, vous devez d'abord soigneusement planifier et tester les fonctionnalités

de gestion avant d'utiliser Configuration Manager dans un environnement de production. En tant qu'application de gestion performante, Configuration Manager est susceptible d'affecter tous les ordinateurs de votre organisation. Lorsque Configuration Manager est déployé et géré avec une planification minutieuse prenant en compte les exigences de votre entreprise, Configuration Manager peut réduire les frais administratifs généraux ainsi que le coût total de possession.

Utilisez les rubriques suivantes et les autres sections de cette rubrique pour en savoir plus sur Configuration Manager.

**Rubriques connexes dans la bibliothèque de documents :**

- Fonctions et fonctionnalités de System Center Configuration Manager
- Choisir une solution de gestion d'appareils pour System Center Configuration Manager
- Ce qui a changé dans System Center Configuration Manager par rapport à System Center 2012 Configuration Manager
- Principes de base de System Center Configuration Manager
- Évaluer System Center Configuration Manager en créant votre propre environnement lab
- Trouver de l'aide pour l'utilisation de System Center Configuration Manager
- Éléments supprimés et dépréciés dans System Center Configuration Manager

## Console Configuration Manager

Après l'installation de Configuration Manager, utilisez la console Configuration Manager pour configurer les sites et les clients, ainsi que pour exécuter et surveiller les tâches de gestion. Cette console est le principal point d'administration et vous permet de gérer plusieurs sites.

Elle peut également exécuter des consoles secondaires pour prendre en charge des tâches spécifiques de gestion de client. Par exemple :

- l'**Explorateur de ressources**pour afficher des informations sur la parc matériel et logiciel ;
- le**Contrôle à distance** pour se connecter à distance à un ordinateur client afin d'effectuer des tâches de dépannage.

Vous pouvez installer la console Configuration Manager sur des ordinateurs supplémentaires, ainsi que restreindre l'accès et limiter ce que les utilisateurs administratifs voient dans la console à l'aide de l'administration basée sur des rôles de Configuration Manager.

Pour plus d'informations, consultez Installer des consoles System Center Configuration Manager.

## Le catalogue d'applications, le centre logiciel et le portail d'entreprise

Le **catalogue d'applications** est un site web sur lequel les utilisateurs peuvent rechercher et demander des logiciels pour leurs PC Windows. Pour utiliser le catalogue d'applications, vous devez installer le point de service Web du catalogue d'applications et le point de site Web du catalogue d'applications pour le site.

Le**Centre logiciel** est une application installée quand le client Configuration Manager est installé sur des ordinateurs Windows. Les utilisateurs exécutent cette application pour demander des logiciels et gérer les logiciels que Configuration Manager déploie à leur intention. Le Centre logiciel permet aux utilisateurs d'effectuer les opérations suivantes :

- rechercher et installer des logiciels à partir du catalogue d'applications ;
- afficher leur historique de demande de logiciels ;
- configurer à quel moment Configuration Manager peut installer des logiciels sur leurs équipements ;
- configurer les paramètres d'accès pour le contrôle à distance, si un utilisateur administratif a activé le contrôle à distance.

**Le portail d'entreprise** est une application ou un site web qui offre des fonctions similaires au catalogue d'applications, mais pour les appareils mobiles qui sont inscrits par Windows Intune.

Pour plus d'informations, consultez Présentation de la gestion d'applications dans System Center Configuration Manager.

**Propriétés de Configuration Manager (sur les PC Windows)**

Lorsque le client Configuration Manager est installé sur les ordinateurs Windows, Configuration Manager est installé dans le Panneau de configuration. En règle générale, vous n'avez pas à configurer cette application, car la configuration du client est effectuée dans la console Configuration Manager. Cette application aide les utilisateurs administratifs et le support technique à résoudre les problèmes avec des clients individuels.

Pour plus d'informations sur le déploiement de clients, consultez Méthodes d'installation du client dans System Center Configuration Manager.

# Exemples de scénarios de Configuration Manager

Les exemples de scénarios suivants montrent comment une entreprise nommée Trey Research utilise Configuration Manager pour permettre aux utilisateurs :

- d'être plus productifs ;
- d'unifier la gestion de la conformité des appareils pour rationaliser les tâches d'administration ;
- de simplifier la gestion des appareils pour réduire les coûts d'exploitation informatiques.

Dans tous les scénarios, Adam est l'administrateur principal de Configuration Manager.

**Exemple de scénario : donner aux utilisateurs plus d'autonomie en permettant l'accès aux applications à partir de tous les appareils**

Trey Research veut s'assurer que les employés peuvent accéder aux applications dont ils ont besoin, et aussi efficacement que possible. Adam applique ces spécifications de l'entreprise aux scénarios suivants :

| EXIGENCE | ÉTAT ACTUEL DE LA GESTION DU CLIENT | ÉTAT FUTUR DE LA GESTION DU CLIENT |
|---|---|---|
| Les nouveaux employés peuvent travailler efficacement dès le premier jour. | Quand les employés intègrent l'entreprise et qu'ils ouvrent une session pour la première fois sur leur ordinateur, ils doivent attendre que les applications soient installées. | Quand les employés intègrent l'entreprise, ils ouvrent une session et voient leurs applications installées et prêtes à l'emploi sur leur ordinateur. |
| Les employés peuvent demander rapidement et facilement les logiciels supplémentaires dont ils ont besoin. | Quand les employés ont besoin d'autres applications, ils envoient une demande au support technique. Ils attendent en général deux jours avant que la demande soit traitée et que les applications soient installées. | Quand les employés ont besoin d'autres applications, ils peuvent les demander à partir d'un site web. Ils peuvent ensuite les installer immédiatement en l'absence de restrictions de licences. S'il existe des restrictions de licences, les utilisateurs doivent tout d'abord demander l'approbation avant d'installer l'application.<br><br>Le site web présente aux utilisateurs uniquement les applications qu'ils sont autorisés à installer. |

| EXIGENCE | ÉTAT ACTUEL DE LA GESTION DU CLIENT | ÉTAT FUTUR DE LA GESTION DU CLIENT |
|---|---|---|
| Les employés peuvent utiliser leurs appareils mobiles au travail si ces appareils sont conformes aux stratégies de sécurité qui sont surveillées et appliquées.<br><br>Ces stratégies incluent l'application d'un mot de passe fort, le verrouillage d'un appareil après une période d'inactivité et la réinitialisation à distance d'appareils perdus ou volés. | Les employés connectent leurs appareils mobiles au serveur Exchange Server pour accéder au service de messagerie. Toutefois, les rapports de confirmation de la conformité avec les stratégies de sécurité sont limités dans les stratégies de boîte aux lettres ActiveSync Exchange par défaut. L'utilisation personnelle des appareils mobiles risque d'être interdite si le service informatique ne peut pas confirmer le respect de la stratégie. | Le service informatique peut confirmer la compatibilité de la sécurité de l'appareil mobile avec les paramètres requis. Cette confirmation permet aux utilisateurs de continuer à utiliser leur appareil mobile au travail. Les utilisateurs peuvent réinitialiser leur appareil mobile à distance en cas de perte ou de vol, et le support technique peut réinitialiser tout appareil mobile d'utilisateur qui a été signalé comme perdu ou volé.<br><br>Il est recommandé de fournir l'inscription des appareils mobiles dans un environnement d'infrastructure à clés publiques pour plus de contrôle et de sécurité. |
| Les employés peuvent être productifs même s'ils ne sont pas à leur bureau. | Quand les employés ne sont pas à leur bureau et n'ont pas d'ordinateurs portables, ils ne peuvent pas accéder à leurs applications via les ordinateurs publics disponibles dans l'entreprise. | Les employés peuvent utiliser des ordinateurs publics pour accéder à leurs applications et données. |
| En général, la pérennité des activités est prioritaire sur l'installation des applications et des mises à jour logicielles requises. | Les applications et les mises à jour logicielles requises sont installées pendant la journée, ce qui perturbe fréquemment le travail des utilisateurs dans la mesure où leurs ordinateurs ralentissent ou redémarrent au cours de l'installation. | Les utilisateurs peuvent définir leurs heures de travail pour empêcher l'installation des logiciels obligatoires pendant qu'ils utilisent leur ordinateur. |

Pour répondre aux conditions requises, Adam utilise les fonctionnalités de gestion et les options de configuration de Configuration Manager suivantes :

- Gestion des applications
- Gestion des appareils mobiles

Il implémente ces fonctionnalités en effectuant les étapes de configuration décrites dans le tableau suivant :

| ÉTAPES DE CONFIGURATION | RÉSULTAT |
|---|---|
| Adam vérifie que les nouveaux utilisateurs ont des comptes d'utilisateur dans Active Directory, puis il crée un regroupement basé sur des requêtes dans Configuration Manager pour ces utilisateurs. Il définit ensuite l'affinité entre appareil et utilisateur pour ces utilisateurs en créant un fichier de mappage des comptes d'utilisateur aux ordinateurs principaux qui seront utilisés, et il importe ce fichier dans Configuration Manager.<br><br>Les applications dont les nouveaux utilisateurs ont besoin sont déjà créées dans Configuration Manager. Adam déploie ensuite les applications ayant l'objectif Obligatoire dans le regroupement qui contient les nouveaux utilisateurs. | En raison des informations relatives à l'affinité entre appareil et utilisateur, les applications sont installées sur l'ordinateur principal ou les ordinateurs de chaque utilisateur avant l'ouverture d'une session utilisateur.<br><br>L'utilisateur peut utiliser les applications aussitôt après avoir ouvert une session. |

| ÉTAPES DE CONFIGURATION | RÉSULTAT |
| --- | --- |
| Adam installe et configure les rôles de système de site du catalogue des applications pour permettre aux utilisateurs de rechercher les applications à installer. Il crée des déploiements d'applications dont l'objet est Disponible, puis il déploie ces applications sur le regroupement qui contient les nouveaux utilisateurs.<br><br>Dans le cas d'applications dont le nombre de licences est limité, Adam les configure pour en demander l'approbation. | Les utilisateurs peuvent maintenant accéder au catalogue des applications pour rechercher les applications qu'ils sont autorisés à installer. Ils peuvent ensuite installer les applications immédiatement, ou envoyer une demande d'approbation et revenir au catalogue des applications pour les installer une fois que le support technique a approuvé leur demande. |
| Adam crée un connecteur Exchange Server dans Configuration Manager pour gérer les appareils mobiles qui se connectent au serveur Exchange Server local de l'entreprise. Il configure ce connecteur avec les paramètres de sécurité qui exigent de définir un mot de passe fort et de verrouiller l'appareil mobile après une période d'inactivité.<br><br>Pour gérer en plus les appareils exécutant Windows Phone 8, Windows RT et iOS, Adam prend un abonnement à Microsoft Intune. Il installe ensuite le rôle de système de site de point de connexion de service. Cette solution de gestion d'appareil mobile fournit à l'entreprise une meilleure prise en charge de la gestion de ces appareils. Cela inclut la mise des applications à la disposition des utilisateurs pour l'installation sur ces appareils, ainsi que la gestion étendue des paramètres. De plus, les connexions d'appareils mobiles sont sécurisées à l'aide de certificats PKI qui sont automatiquement créés et déployés par Intune.<br><br>Après avoir configuré le point de connexion de service et l'abonnement à utiliser avec Configuration Manager, Adam envoie un e-mail aux utilisateurs de ces appareils mobiles, avec un lien leur permettant de démarrer le processus d'inscription.<br><br>Pour inscrire les appareils mobiles auprès de Microsoft Intune, Adam utilise des paramètres de compatibilité afin de configurer des paramètres de sécurité pour ces appareils mobiles. Ces paramètres exigent la définition d'un mot de passe fort et le verrouillage de l'appareil mobile après une période d'inactivité. | Ces deux solutions de gestion des appareils mobiles permettent maintenant au service informatique de fournir des informations de rapport relatives aux appareils mobiles qui sont utilisés sur le réseau de l'entreprise et à leur compatibilité avec les paramètres de sécurité configurés.<br><br>Les utilisateurs apprennent à réinitialiser leur appareil mobile à distance à partir du catalogue des applications ou du portail d'entreprise s'ils perdent ou se font voler leur appareil mobile. Les membres du support technique apprennent également à réinitialiser à distance les appareils mobiles des utilisateurs à l'aide de la console Configuration Manager.<br><br>De plus, pour les appareils mobiles inscrits auprès de Microsoft Intune, Adam peut maintenant déployer des applications mobiles que les utilisateurs peuvent installer, collecter plus de données d'inventaire à partir de ces appareils et mieux contrôler la gestion des appareils en accédant à d'autres paramètres. |
| Trey Research dispose de plusieurs ordinateurs publics, utilisés par les employés visitant les bureaux. Les employés veulent pouvoir utiliser leurs applications de n'importe quel endroit. Toutefois, Adam ne souhaite pas installer localement toutes les applications sur chaque ordinateur.<br><br>Pour ce faire, Adam crée les applications requises avec deux types de déploiement :<br><br>**Le premier :** une installation complète et locale de l'application qui ne peut être installée que sur l'appareil principal d'un utilisateur.<br><br>**Le second :** une version virtuelle de l'application qui ne doit pas être installée sur l'appareil principal de l'utilisateur. | Quand des visiteurs ouvrent une session sur un ordinateur public, ils retrouvent leurs applications affichées sous forme d'icônes sur le bureau de l'ordinateur public. Les applications qu'ils exécutent sont diffusées en continu comme des applications virtuelles. Ainsi, les utilisateurs sont aussi productifs que s'ils étaient assis à leur bureau. |

| ÉTAPES DE CONFIGURATION | RÉSULTAT |
| --- | --- |
| Adam informe les utilisateurs qu'ils peuvent définir leurs heures de travail dans le Centre logiciel, et sélectionner des options pour empêcher les activités de déploiement de logiciel pendant cette période et quand l'ordinateur se trouve en mode présentation. | Les utilisateurs sont plus productifs pendant leur journée de travail car ils peuvent contrôler le moment du déploiement des logiciels par Configuration Manager sur leurs ordinateurs. |

Ces étapes et résultats de configuration permettent à Trey Research de donner plus d'autonomie à ses employés en assurant leur accès aux applications à partir de n'importe quel appareil.

**Exemple de scénario : unifier la gestion de la conformité pour les appareils**

Trey Research souhaite appliquer une solution de gestion client unifiée pour assurer que les ordinateurs exécutent un logiciel antivirus automatiquement mis à jour. Plus précisément :

- Le Pare-feu Windows est activé.
- Toutes les mises à jour critiques sont installées.
- Des clés de Registre spécifiques sont définies.
- Les appareils mobiles gérés ne peuvent pas installer ou exécuter des applications non sécurisées.

L'entreprise souhaite également étendre cette protection à Internet pour les ordinateurs portables qui se déplacent de l'intranet à Internet.

Adam applique ces spécifications de l'entreprise aux scénarios suivants :

| EXIGENCE | ÉTAT ACTUEL DE LA GESTION DU CLIENT | ÉTAT FUTUR DE LA GESTION DU CLIENT |
| --- | --- | --- |
| Tous les ordinateurs exécutent un logiciel anti-programme malveillant avec des fichiers de définition qui sont à jour et qui activent le pare-feu Windows. | Les ordinateurs exécutent différentes solutions de logiciels anti-programme malveillant qui ne sont pas toujours à jour. Le Pare-feu Windows est activé par défaut, mais les utilisateurs le désactivent parfois.<br><br>Les utilisateurs sont invités à contacter le support technique s'ils détectent un logiciel anti-programme malveillant sur leur ordinateur. | Tous les ordinateurs exécutent la même solution de logiciel anti-programme malveillant qui télécharge automatiquement les derniers fichiers de mise à jour des définitions et qui réactivent automatiquement le pare-feu Windows s'il a été désactivé par l'utilisateur.<br><br>Le support technique est automatiquement averti par courrier électronique si un logiciel malveillant est détecté. |

| EXIGENCE | ÉTAT ACTUEL DE LA GESTION DU CLIENT | ÉTAT FUTUR DE LA GESTION DU CLIENT |
|---|---|---|
| Tous les ordinateurs installent les mises à jour logicielles critiques pendant le premier mois après leur sortie. | Bien que les mises à jour logicielles soient installées sur les ordinateurs, beaucoup d'ordinateurs n'installent pas automatiquement les mises à jour logicielles critiques avant les deux ou trois mois suivant la publication de ces mises à jour. De ce fait, ces ordinateurs sont vulnérables aux attaques pendant cette période.<br><br>Pour les ordinateurs qui n'installent pas les mises à jour logicielles critiques, le support technique envoie d'abord un e-mail demandant aux utilisateurs d'installer les mises à jour. Les ingénieurs se connectent à distance aux ordinateurs qui restent non conformes et installent manuellement les mises à jour manquantes. | Le taux de conformité actuel pour le mois spécifié est passé à plus de 95 %. Le support technique n'a pas eu à envoyer d'e-mail de rappel, ni à installer manuellement les mises à jour. |
| Les paramètres de sécurité pour des applications spécifiques sont régulièrement vérifiés et corrigés, si nécessaire. | Les ordinateurs exécutent des scripts de démarrage complexes qui s'appuient sur l'appartenance au groupe d'ordinateurs pour réinitialiser les valeurs de Registre pour des applications spécifiques.<br><br>Comme ces scripts s'exécutent uniquement au démarrage et que certains ordinateurs sont laissés sous tension pendant plusieurs jours, le support technique ne peut pas vérifier les écarts de configuration en temps voulu. | Les valeurs de Registre sont vérifiées et résolues automatiquement sans compter sur l'appartenance au groupe d'ordinateurs ou sur le redémarrage de l'ordinateur. |
| Les appareils mobiles ne peuvent pas installer ou exécuter des applications non sécurisées. | Les utilisateurs sont invités à ne pas télécharger ni exécuter d'applications potentiellement dangereuses à partir d'Internet. Aucune mesure de contrôle n'a été mise en place pour surveiller ou appliquer cette recommandation. | Les appareils mobiles qui sont gérés avec Microsoft Intune ou Configuration Manager empêchent automatiquement l'installation ou l'exécution des applications non signées. |
| Les ordinateurs portables qui passent de l'intranet à Internet doivent être sécurisés. | Les utilisateurs en déplacement ne parviennent pas toujours à se connecter quotidiennement via le réseau VPN. Ces ordinateurs portables ne sont alors plus conformes avec les conditions de sécurité requises. | Une simple connexion Internet suffit pour que les ordinateurs portables restent compatibles avec les conditions de sécurité requises. Les utilisateurs ne sont pas obligés d'ouvrir une session ou d'utiliser le réseau VPN. |

Pour répondre aux conditions requises, Adam utilise les fonctionnalités de gestion et les options de configuration de Configuration Manager suivantes :

- Endpoint Protection
- Mises à jour logicielles
- Paramètres de conformité
- Gestion des appareils mobiles
- Gestion des clients basés sur Internet

Il implémente ces fonctionnalités en effectuant les étapes de configuration décrites dans le tableau suivant :

| ÉTAPES DE CONFIGURATION | RÉSULTAT |
|---|---|
| Adam configure Endpoint Protection. Il active le paramètre client pour désinstaller les autres solutions anti-programme malveillant, puis il active le Pare-feu Windows. Il configure des règles de déploiement automatique pour permettre aux ordinateurs de rechercher et d'installer régulièrement les dernières mises à jour de définitions. | La solution anti-programme malveillant unique vous aide à protéger tous les ordinateurs avec une surcharge administrative minimale. Comme le support technique est automatiquement averti par e-mail quand un logiciel anti-programme malveillant est détecté, les problèmes peuvent être résolus rapidement. Cela permet d'empêcher des attaques sur d'autres ordinateurs. |
| Pour améliorer le taux de conformité, Adam utilise des règles de déploiement automatique, définit des fenêtres de maintenance pour les serveurs, et examine les avantages et inconvénients de l'utilisation de la fonctionnalité Wake-on-LAN pour les ordinateurs mis en veille prolongée. | La compatibilité des mises à jour logicielles critiques augmente, et la nécessité pour les utilisateurs ou le support technique d'installer des mises à jour logicielles manuellement est réduite. |
| Adam utilise des paramètres de compatibilité pour vérifier la présence des applications spécifiées. Quand les applications sont détectées, les éléments de configuration vérifient alors les valeurs de Registre et les corrigent automatiquement si elles ne sont pas conformes. | Grâce au déploiement d'éléments de configuration et de bases de référence de configuration sur tous les ordinateurs et à la vérification quotidienne de la conformité des ordinateurs, vous n'avez plus besoin de créer des scripts distincts basés sur l'appartenance de l'ordinateur, ni de redémarrer l'ordinateur. |
| Adam utilise des paramètres de compatibilité pour les appareils mobiles inscrits et configure le connecteur Exchange Server de sorte que les applications non signées ne sont pas autorisées à s'installer et s'exécuter sur des appareils mobiles. | Du fait de l'interdiction d'utiliser des applications non signées, les appareils mobiles sont protégés automatiquement contre les applications potentiellement dangereuses. |
| Adam s'assure que les ordinateurs et les serveurs de système de site ont les certificats PKI requis par Configuration Manager pour les connexions HTTPS. Il installe ensuite des rôles de système de site supplémentaires dans le réseau de périmètre qui acceptent les connexions client à partir d'Internet. | Configuration Manager continue à gérer automatiquement les ordinateurs qui passent de l'intranet à Internet lorsqu'ils disposent d'une connexion Internet. Ces ordinateurs ne comptent pas sur les utilisateurs ouvrant une session sur leur ordinateur ou se connectant au réseau VPN.<br><br>Ces ordinateurs continuent à être gérés pour les logiciels anti-programme malveillant et le Pare-feu Windows, les mises à jour logicielles et les éléments de configuration. Par conséquent, les niveaux de compatibilité augmentent automatiquement. |

Ces étapes et résultats de configuration permettent à Trey Research d'unifier la gestion de la compatibilité des appareils.

**Exemple de scénario : simplifier la gestion des clients pour les appareils**

Trey Research souhaite que tous les nouveaux ordinateurs installent automatiquement l'image d'ordinateur de base de l'entreprise qui exécute Windows 7. Une fois l'image du système d'exploitation installée sur ces ordinateurs, ceux-ci doivent être gérés et surveillés pour détecter tout autre logiciel que les utilisateurs installent. Les ordinateurs qui stockent des informations hautement confidentielles nécessitent des stratégies de gestion plus limitées que les autres ordinateurs. Par exemple, les ingénieurs du support technique ne doivent pas établir une connexion à distance à ces ordinateurs, un code confidentiel BitLocker doit être utilisé pour les redémarrages et uniquement les administrateurs locaux sont autorisés à installer un logiciel.

Adam applique ces spécifications de l'entreprise aux scénarios suivants :

| EXIGENCE | ÉTAT ACTUEL DE LA GESTION DU CLIENT | ÉTAT FUTUR DE LA GESTION DU CLIENT |
|---|---|---|
| Windows 7 est installé sur les nouveaux ordinateurs. | L'équipe du support technique installe et configure Windows 7 pour les utilisateurs, puis envoie l'ordinateur à l'emplacement prévu. | Les nouveaux ordinateurs sont envoyés directement à leur destination finale. Ils sont connectés au réseau, puis installent et configurent automatiquement Windows 7. |
| Les ordinateurs doivent être gérés et surveillés. Cela inclut la collecte des données d'inventaire matériel et logiciel qui vous aident à déterminer les conditions de licence. | Le client Configuration Manager est déployé en utilisant l'installation Push automatique du client. Le support technique examine les échecs d'installation et vérifie les clients qui n'envoient pas de données d'inventaire comme prévu.<br><br>Les échecs sont fréquents à cause des dépendances d'installation qui ne sont pas respectées et de la corruption de WMI sur le client. | Les données d'installation et d'inventaire client collectées depuis des ordinateurs sont plus fiables et requièrent moins d'intervention du support technique. Les rapports indiquent l'utilisation du logiciel pour les informations de licence. |
| Certains ordinateurs doivent avoir des stratégies de gestion plus rigoureuses. | En raison des stratégies de gestion plus rigoureuses, Configuration Manager ne gère pas encore ces ordinateurs. | Ces ordinateurs sont gérés à l'aide de Configuration Manager pour prendre en compte les exceptions, sans aucune surcharge administrative. |

Pour répondre aux conditions requises, Adam utilise les fonctionnalités de gestion et les options de configuration de Configuration Manager suivantes :

- Déploiement du système d'exploitation
- Déploiement du client et état du client
- Paramètres de conformité
- Paramètres du client
- Méthodes d'inventaire et Asset Intelligence
- Administration basée sur des rôles

Il implémente ces fonctionnalités en effectuant les étapes de configuration décrites dans le tableau suivant :

| ÉTAPES DE CONFIGURATION | RÉSULTAT |
|---|---|
| Adam capture une image du système d'exploitation à partir d'un ordinateur qui exécute Windows 7 et qui est configuré selon les spécifications de l'entreprise. Il déploie ensuite le système d'exploitation sur les nouveaux ordinateurs à l'aide de la prise en charge d'ordinateur inconnu et de l'environnement PXE. Il installe également le client Configuration Manager dans le cadre du déploiement de système d'exploitation. | Les nouveaux ordinateurs sont prêts et s'exécutent plus rapidement sans intervention du support technique. |

| ÉTAPES DE CONFIGURATION | RÉSULTAT |
| --- | --- |
| Adam configure l'installation Push automatique du client à l'échelle du site pour installer le client Configuration Manager sur les ordinateurs découverts. Cela garantit que tous les ordinateurs non imagés avec le client installent toujours le client afin que l'ordinateur soit géré par Configuration Manager.<br><br>Adam configure l'état client pour corriger automatiquement les éventuels problèmes de client qui sont découverts. Il configure également des paramètres client pour la collecte des données d'inventaire requises et configure Asset Intelligence. | L'installation du client en même temps que le système d'exploitation est plus rapide et plus fiable que d'attendre que Configuration Manager découvre l'ordinateur et tente d'y installer les fichiers sources du client. Toutefois, en activant l'option d'installation Push automatique du client, vous fournissez une méthode de sauvegarde qui permet à un ordinateur où le système d'exploitation est déjà installé d'installer le client quand il se connecte au réseau.<br><br>Les paramètres client assurent que les clients envoient régulièrement leurs informations d'inventaire au site. Grâce à cela et aux tests de l'état du client, le client reste opérationnel avec une intervention minimale du support technique. Par exemple, les altérations de WMI sont détectées et résolues automatiquement.<br><br>Les rapports Asset Intelligence permettent de surveiller l'utilisation des logiciels et des licences. |
| Adam crée un regroupement pour les ordinateurs auxquels il souhaite appliquer des paramètres de stratégie plus stricts. Il crée ensuite un paramètre d'appareil client personnalisé pour ce regroupement. Ce paramètre désactive le contrôle à distance, active l'entrée du code PIN BitLocker et autorise uniquement les administrateurs locaux à installer des logiciels.<br><br>Adam configure l'administration basée sur des rôles pour empêcher les ingénieurs du support technique de voir ce regroupement d'ordinateurs. Cette mesure évite que ces ordinateurs soient gérés comme des ordinateurs standard par inadvertance. | Ils sont désormais gérés par Configuration Manager, mais avec des paramètres spécifiques qui ne nécessitent pas l'installation d'un nouveau site.<br><br>Le regroupement de ces ordinateurs n'est pas visible par les ingénieurs du support technique. Cela réduit le risque que ces ordinateurs reçoivent accidentellement des déploiements et des scripts destinés aux ordinateurs standard. |

Ces étapes et résultats de configuration permettent à Trey Research de simplifier la gestion des clients pour les appareils.

## Étapes suivantes

Avant d'installer Configuration Manager, familiarisez-vous avec certains concepts de base et les termes qui sont spécifiques à Configuration Manager.

- Si vous connaissez déjà System Center 2012 Configuration Manager, consultez Changements dans System Center Configuration Manager par rapport à System Center 2012 Configuration Manager pour comprendre les nouvelles fonctionnalités.
- Pour obtenir une vue d'ensemble technique globale de System Center Configuration Manager, consultez Principes de base de System Center Configuration Manager.

Quand vous êtes familiarisé avec les concepts de base, aidez-vous de la documentation de System Center Configuration Manager pour déployer et utiliser correctement Configuration Manager.

# Trouver de l'aide pour l'utilisation de System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cet article contient les sections suivantes avec plusieurs ressources permettant de trouver de l'aide pour utiliser Configuration Manager :

- Documentation du produit
- Partage de commentaires sur le produit
- Suivre le blog de l'équipe Configuration Manager
- Options de support et ressources de la communauté

Pour obtenir de l'aide sur l'accessibilité du produit, consultez Fonctionnalités d'accessibilité dans Configuration Manager.

## Documentation du produit

Pour accéder à la documentation la plus récente du produit, commencez à l'index de la bibliothèque.

Pour des conseils sur la recherche, l'ajout de commentaires et plus d'informations sur l'utilisation de la documentation du produit, consultez Comment utiliser la documentation.

## Commentaires sur le produit

Signalez les éventuels défauts du produit à l'aide de l'application Hub de commentaires intégrée à Windows 10. Quand vous **ajoutez de nouveaux commentaires**, veillez à sélectionner la catégorie **Enterprise Management**, puis choisissez parmi les sous-catégories suivantes :

- Client de Configuration Manager
- Console Configuration Manager
- Déploiement de système d'exploitation Configuration Manager
- Serveur Configuration Manager

Continuez à utiliser notre page User Voice afin de voter sur de nouvelles idées de fonctionnalités dans Configuration Manager.

## Blog de l'équipe Configuration Manager

Les équipes techniques et partenaires de Configuration Manager utilisent le blog Enterprise Mobility + Security pour vous donner des informations techniques et d'autres informations sur Configuration Manager et les technologies associées. Les publications de ce blog complètent la documentation et le support du produit.

## Options de support et ressources de la communauté

Les liens suivants fournissent des informations sur les options de support et les ressources communautaires :

- Support Microsoft

- Communauté Configuration Manager : Guide de survie de System Center Configuration Manager (Current Branch)
- Page Forums de Configuration Manager

# Guide pratique pour utiliser la documentation de Configuration Manager

22/06/2018 • 11 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cet article fournit les sections suivantes, ainsi que plusieurs ressources et conseils sur l'utilisation de la bibliothèque de documentation de Configuration Manager :

- Comment effectuer une recherche
- Soumission de bogues, d'améliorations, de questions et de nouvelles idées concernant la documentation
- Comment être notifié des changements apportés
- Comment contribuer à la documentation

Pour obtenir une aide générale sur le produit, consultez Trouver de l'aide.

## Rechercher

Utilisez les conseils de recherche suivants pour vous aider à trouver les informations dont vous avez besoin :

- Quand vous utilisez votre moteur de recherche favori pour rechercher du contenu relatif à Configuration Manager, ajoutez `SCCM` à vos mots clés de recherche.
  - Recherchez les résultats provenant de docs.microsoft.com pour l'édition Current Branch de Configuration Manager. Les résultats provenant de technet.microsoft.com ou msdn.microsoft.com concernent des versions de produits plus anciennes.
  - Pour concentrer davantage les résultats de la recherche sur la bibliothèque de contenu actuelle, ajoutez `site:docs.microsoft.com` afin de définir l'étendue à couvrir par le moteur de recherche.
- Utilisez des termes de recherche correspondant à la terminologie qui se trouve dans l'interface utilisateur et la documentation en ligne. Évitez les termes ou les abréviations non officiels que vous pouvez voir dans le contenu de la communauté. Par exemple, rechercher « point de gestion » plutôt que « MP », « type de déploiement » plutôt que « DT » et « mises à jour logicielles » plutôt que « SUM ».
- Pour effectuer une recherche dans un article que vous consultez, utilisez la fonctionnalité **Rechercher** de votre navigateur. Dans la plupart des navigateurs web actuels, appuyez sur **Ctrl**+**F**, puis entrez vos termes de recherche.
- Chaque article sur docs.microsoft.com contient les champs suivants qui vous permettent d'effectuer des recherches dans le contenu :
  - **Rechercher** en haut à droite. Pour effectuer une recherche dans tous les articles, entrez des termes dans ce champ. Les articles de la bibliothèque de Configuration Manager incluent automatiquement l'étendue « ConfigMgr ».
  - **Filtrer par titre** au-dessus de la table des matières de gauche. Pour effectuer une recherche dans la table des matières, entrez des termes dans ce champ. Ce champ permet de rechercher uniquement les termes qui apparaissent dans les titres d'articles du nœud actuel. Par exemple, Infrastructure de base ou Gestion des applications.

- Vous n'arrivez pas à trouver quelque chose ? Soumettez des commentaires ! Quand vous soumettez un problème, indiquez le moteur de recherche utilisé, les mots clés essayés et l'article cible. Ces commentaires aident Microsoft à optimiser le contenu pour une meilleure recherche.

## Commentaires

Accédez à la section Commentaires au bas de la page en cliquant sur le lien **Commentaires** en haut à droite d'un article. Cette section est intégrée aux problèmes GitHub. Pour plus d'informations sur l'intégration aux problèmes GitHub, consultez le billet de blog consacré à la plateforme de documentation.

Pour partager vos commentaires sur le produit Configuration Manager, cliquez sur **Give product feedback** (Fournir des commentaires sur le produit). Pour plus d'informations, consultez Commentaires produit.

Si vous souhaitez fournir des commentaires sur la documentation, la possession d'un compte GitHub est un prérequis. Une fois que vous vous êtes connecté, vous disposez d'une autorisation à usage unique pour l'accès à MicrosoftDocs. Cliquez ensuite sur **Give documentation feedback** (Fournir des commentaires sur la documentation), entrez un titre et un commentaire, puis cliquez sur **Submit feedback** (Envoyer des commentaires). Cette action permet de soumettre un nouveau problème relatif à l'article cible dans le dépôt SCCMdocs.

Cette intégration permet également d'afficher tous les problèmes ouverts ou fermés pour l'article cible. S'il en existe, passez-les en revue avant de soumettre un nouveau problème. Si vous trouvez un problème connexe, cliquez sur l'émoticône pour ajouter une réaction, ou développez l'entrée correspondante pour ajouter un commentaire.

#### Types de commentaire

Utilisez la fonctionnalité Problèmes GitHub pour soumettre les types de commentaire suivants :

- Bogue de la documentation : le contenu est obsolète, vague, confus ou fragmenté.
- Amélioration de la documentation : suggestion d'amélioration de l'article.
- Question sur la documentation : vous avez besoin d'aide pour trouver de la documentation existante.
- Idée de documentation : suggestion d'un nouvel article. Utilisez cette méthode à la place de UserVoice pour les commentaires relatifs à la documentation.
- Félicitations : commentaires positifs sur un article utile ou instructif !
- Localisation : commentaires sur la traduction du contenu.
- SEO (optimisation du référencement d'un site auprès d'un moteur de recherche) : commentaires sur les problèmes de recherche de contenu. Incluez le moteur de recherche, les mots clés et l'article cible dans les commentaires.

Si des problèmes sont soumis pour des rubriques non liées à la documentation, par exemple des commentaires sur le produit, des questions sur le produit ou des demandes de support, ces problèmes sont fermés et les utilisateurs redirigés vers le canal de commentaires approprié.

Pour partager vos commentaires sur la plateforme docs.microsoft.com, accédez aux commentaires sur la documentation. La plateforme inclut tous les composants de wrapper tels que l'en-tête, la table des matières et le menu de droite. Elle inclut également le rendu des articles dans le navigateur, par exemple la police, les zones d'alerte et les ancres de page.

## Notifications

Pour recevoir des notifications en cas de changement du contenu dans la bibliothèque de documentation, suivez les étapes ci-dessous :

1. Utilisez la recherche de documentation pour trouver un article ou un ensemble d'articles. Par exemple :
   - Recherchez un article unique par son titre : « Fichiers journaux pour la résolution des problèmes -

Configuration Manager ».

- Recherchez un article relatif à SQL.

2. Dans le coin supérieur droit, cliquez sur le lien **RSS**.
3. Utilisez ce flux dans une application RSS pour recevoir des notifications en cas de changement de l'un des résultats de la recherche.

> **TIP**
>
> Vous pouvez également **suivre** le dépôt SCCMdocs sur GitHub. Cette méthode génère un grand nombre de notifications. De plus, elle n'inclut pas les changements apportés à un dépôt privé utilisé par Microsoft.

# Contribuer

La bibliothèque de documentation de Configuration Manager, comme la plupart des contenus de docs.microsoft.com, est open source sur GitHub. Cette bibliothèque accepte et encourage les contributions de la communauté. Pour plus d'informations sur la procédure à suivre, consultez le Guide du contributeur. La création d'un compte GitHub est le seul prérequis.

#### Étapes de base pour contribuer à SCCMdocs

1. Dans l'article cible, cliquez sur **Modifier**. Cette action permet d'ouvrir le fichier source dans GitHub.
2. Pour modifier le fichier source, cliquez sur l'icône de crayon.
3. Apportez vos changements à la source Markdown. Pour plus d'informations, consultez Guide pratique pour utiliser Markdown et rédiger de la documentation.
4. Dans la section Propose file change (Proposer le changement d'un fichier), entrez un commentaire de validation publique décrivant *ce que* vous avez changé. Cliquez ensuite sur **Propose file change** (Proposer le changement d'un fichier).
5. Faites défiler vers le bas et vérifiez les changements apportés. Cliquez sur **Create pull request** (Créer une demande de tirage (pull request)) pour ouvrir le formulaire. Indiquez *pourquoi* vous avez effectué ce changement. Identifiez l'auteur de l'article, et demandez-lui de le réviser. Cliquez sur **Create pull request** (Créer une demande de tirage).

### Type de contribution

Si vous souhaitez apporter votre contribution mais que vous ne savez pas par où commencer, consultez les suggestions suivantes :

- Vérifiez l'exactitude d'un article. Mettez ensuite à jour les métadonnées **ms.date** au format `mm/dd/yyyy`. Ce type de contribution permet d'actualiser le contenu.
- Ajoutez des éclaircissements, des exemples ou des conseils d'aide en fonction de votre expérience utilisateur. Ce type de contribution tire parti de la puissance de la communauté pour permettre le partage des connaissances.
- Corrigez les traductions effectuées à partir de l'anglais. Ce type de contribution améliore la facilité d'utilisation du contenu localisé.
- Recherchez dans la liste des problèmes les étiquettes destinées à la communauté, par exemple good-first-issue (problème prioritaire) et help-wanted (aide souhaitée). Les auteurs Microsoft affectent ces étiquettes aux problèmes qui sont de bons candidats pour une contribution à la communauté.

# Fonctionnalités d'accessibilité dans System Center Configuration Manager

22/06/2018 • 11 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

System Center Configuration Manager inclut des fonctionnalités d'accessibilité pour les personnes en situation de handicap.

## Fonctionnalités d'accessibilité pour la console Configuration Manager

**Raccourcis et améliorations apportées avec la version 1706**

| RACCOURCI CLAVIER | FONCTION |
|---|---|
| Ctrl + M | Définit le focus sur le volet principal (central). |
| Ctrl + T | Définit le focus sur le nœud supérieur dans le volet de navigation. Si le focus était déjà dans ce volet, le focus est défini sur le dernier nœud que vous avez visité. |
| Ctrl + I | Définit le focus sur la barre de navigation, sous le ruban. |
| Ctrl + L | Définit le focus sur le champ **Recherche**, quand il est disponible. |
| Ctrl + D | Définit le focus sur le volet de détails, quand il est disponible. |
| Alt | Fait basculer le focus vers et hors du ruban. |

- Amélioration de la navigation dans le volet de navigation lorsque vous saisissez les lettres d'un nom de nœud.
- La navigation au clavier via la vue principale et le ruban est désormais circulaire.
- La navigation au clavier dans le volet d'informations est désormais circulaire. Pour revenir à l'objet ou au volet précédent, utilisez Ctrl + D, puis MAJ + TAB.
- Après l'actualisation d'une vue de l'espace de travail, le focus est défini sur le volet principal de cet espace de travail.
- Correction d'un problème pour activer les lecteurs d'écran pour annoncer les noms des éléments de liste.
- Ajout des noms accessibles de plusieurs contrôles sur la page qui active les lecteurs d'écran pour annoncer des informations importantes.

**Les raccourcis suivants sont disponibles pour toutes les versions**

- Pour accéder à un espace de travail, utilisez les raccourcis clavier suivants :

| RACCOURCI CLAVIER | ESPACE DE TRAVAIL |
|---|---|
| Ctrl + 1 | Biens et conformité |
| Ctrl + 2 | Bibliothèque de logiciels |

| RACCOURCI CLAVIER | ESPACE DE TRAVAIL |
|---|---|
| Ctrl + 3 | Analyse |
| Ctrl + 4 | Administration |

- Pour accéder au menu d'un espace de travail, sélectionnez la touche Tab jusqu'à ce que l'icône de réduction/développement soit active. Sélectionnez ensuite la flèche Bas pour accéder au menu de l'espace de travail.
- Pour naviguer dans le menu d'un espace de travail, utilisez les touches de direction.
- Pour accéder aux différentes zones de l'espace de travail, utilisez la touche Tab et les touches Maj+Tab. Pour naviguer dans une zone de l'espace de travail telle que le ruban, utilisez les touches de direction.
- Pour accéder à la barre d'adresses quand le focus se trouve dans le nœud de l'arborescence, utilisez Maj+Tab à trois reprises.
- Sur une page d'Assistant ou une page de propriétés, vous pouvez vous déplacer entre les zones à l'aide de raccourcis clavier. Sélectionnez la touche Alt et le caractère souligné (Alt+*) pour sélectionner une zone spécifique*.
- Pour parcourir les différents nœuds d'un espace de travail, entrez la première lettre du nom d'un nœud. Chaque appui sur une touche déplace le curseur au nœud suivant qui commence par cette lettre. Si vous utilisez un lecteur d'écran, le lecteur lit le nom de ce nœud.

> **NOTE**
>
> Les informations présentes dans cette section ne s'appliquent qu'aux utilisateurs détenteurs de licences de produits Microsoft aux États-Unis. Si vous avez obtenu ce produit en dehors des États-Unis, vous pouvez utiliser la carte d'information de filiale fournie avec le package logiciel ou consulter le site web Accessibilité de Microsoft pour obtenir les coordonnées des services de support technique Microsoft. Vous pouvez contacter votre filiale pour savoir si les types de produits ou de services décrits dans cette section sont disponibles dans votre région. Les informations sur l'accessibilité sont disponibles dans d'autres langues, notamment en japonais et en français.

## Fonctionnalités d'accessibilité dans l'aide de Configuration Manager

L'aide de Configuration Manager intègre des fonctionnalités qui la rendent accessible à un plus grand nombre d'utilisateurs, notamment ceux présentant une mobilité réduite, une acuité visuelle réduite ou d'autres handicaps.

| TÂCHE | UTILISER CE RACCOURCI CLAVIER |
|---|---|
| Afficher la fenêtre d'aide. | F1 |
| Basculer le curseur entre les volets Rubrique d'aide et Navigation (onglets **Sommaire**, **Rechercher**et **Index** ). | F6 |
| Changer d'onglet (par exemple, **Contenu**, **Rechercher** et **Index**) dans le volet de navigation. | ALT+lettre soulignée de l'onglet |
| Sélectionner le texte masqué ou le lien hypertexte suivant. | Onglet |
| Sélectionner le texte masqué ou le lien hypertexte précédent. | Maj+Tabulation |

| TÂCHE | UTILISER CE RACCOURCI CLAVIER |
|---|---|
| Effectuer l'action pour l'élément sélectionné (option Afficher tout, Masquer tout, texte masqué ou lien hypertexte). | Touche Entrée |
| Afficher le menu **Options** pour accéder à n'importe quelle commande de la barre d'outils de l'aide. | Alt+O |
| Masquer ou afficher le volet contenant les onglets **Contenu**, **Rechercher** et **Index**. | Alt+O, puis sélectionner T |
| Afficher la rubrique précédemment consultée. | Alt+O, puis sélectionner B |
| Afficher la rubrique suivante dans une séquence de rubriques précédemment affichées. | Alt+O, puis sélectionner F |
| Revenir à la page d'accueil spécifiée. | Alt+O, puis sélectionner H |
| Arrêter l'ouverture d'une rubrique dans la fenêtre d'aide, par exemple pour arrêter le téléchargement d'une page web. | Alt+O, puis sélectionner S |
| Ouvrir la boîte de dialogue **Options Internet** pour Windows Internet Explorer, dans laquelle vous pouvez modifier les paramètres d'accessibilité. | Alt+O, puis sélectionner I |
| Actualiser la rubrique, par exemple une page Web accessible via un lien. | Alt+O, puis sélectionner R |
| Imprimer toutes les rubriques d'un livre ou seulement une rubrique sélectionnée. | Alt+O, puis sélectionner P |
| Fermer la fenêtre d'aide. | Alt+F4 |

**Pour modifier l'apparence d'une rubrique d'aide**

1. Pour vous préparer à personnaliser les couleurs, les styles et les tailles de police utilisés dans l'Aide, ouvrez la fenêtre de l'Aide.
2. Choisissez **Options**, puis **Options Internet**.
3. Sous l'onglet **Général**, choisissez **Accessibilité**. Choisissez **Ignorer les couleurs spécifiées sur les pages Web**, **Ignorer les styles de police spécifiés sur les pages Web** et **Ignorer les tailles de police spécifiées sur les pages Web**. Vous pouvez également choisir d'utiliser les paramètres qui sont spécifiés dans votre propre feuille de style.

**Pour modifier la couleur de l'arrière-plan ou du texte dans l'aide**

1. Ouvrez la fenêtre d'aide.
2. Choisissez **Options**, puis **Options Internet**.
3. Sous l'onglet **Général**, choisissez **Accessibilité**. Choisissez ensuite **Ignorer les couleurs spécifiées sur les pages Web**. Vous pouvez également choisir d'utiliser les paramètres qui sont spécifiés dans votre propre feuille de style.
4. Pour personnaliser les couleurs utilisées dans l'aide, choisissez **Couleurs** sous l'onglet **Général**. Décochez la case **Utiliser les couleurs Windows**, puis choisissez les couleurs de police et d'arrière-plan que vous souhaitez utiliser.

> **NOTE**
> Si vous modifiez la couleur d'arrière-plan des rubriques d'aide dans la fenêtre de l'Aide, la modification affecte également la couleur d'arrière-plan des pages Web dans Windows Internet Explorer.

**Pour modifier la police dans l'aide**

1. Ouvrez la fenêtre d'aide.
2. Choisissez **Options**, puis **Options Internet**.
3. Sous l'onglet **Général**, choisissez **Accessibilité**. Pour utiliser les mêmes paramètres que ceux utilisés dans votre instance d'Internet Explorer, choisissez **Ignorer les styles de police spécifiés sur les pages Web** et **Ignorer les tailles de police spécifiées sur les pages Web**. Vous pouvez également choisir d'utiliser les paramètres qui sont spécifiés dans votre propre feuille de style.
4. Pour personnaliser le style de police utilisé dans l'Aide, sous l'onglet **Général**, choisissez **Polices**, puis sur le style de police souhaité.

> **NOTE**
> Si vous modifiez la police des rubriques d'aide dans la fenêtre de l'Aide, la modification affecte également la police des pages Web dans Windows Internet Explorer.

# Guide de l'utilisateur du Centre logiciel

18/06/2018 • 9 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

L'administrateur informatique de votre organisation utilise le Centre logiciel pour installer des applications, des mises à jour logicielles et mettre à niveau Windows. Ce guide de l'utilisateur décrit les fonctionnalités du Centre logiciel pour les utilisateurs de l'ordinateur.

**Remarques générales sur les fonctionnalités du Centre logiciel**

- Cet article décrit les dernières fonctionnalités du Centre logiciel. Si votre organisation utilise une version antérieure du Centre logiciel, même si elle est prise en charge, les fonctionnalités ne sont pas toutes disponibles. Pour plus d'informations, contactez votre administrateur informatique.
- Votre administrateur informatique peut désactiver certains aspects du Centre logiciel. Votre expérience spécifique peut varier.

## Comment ouvrir le Centre logiciel

La méthode la plus simple de démarrer le Centre logiciel sur un ordinateur Windows 10 est d'appuyer sur **Démarrer** et taper `Software Center`.

Si vous naviguez dans le menu Démarrer, recherchez sous le groupe **Microsoft System Center** l'icône **Centre logiciel**.

## Applications

Cliquez sur l'onglet **Applications** pour rechercher et installer les applications que votre administrateur informatique déploie pour vous ou sur cet ordinateur.

- **Tout** : Affiche toutes les applications que vous pouvez installer
- **Obligatoire** : Votre administrateur informatique impose ces applications. Si vous désinstallez l'une de ces applications, le Centre logiciel la réinstalle.
- **Filtres** : Votre administrateur informatique peut créer des catégories d'applications. Si elle est disponible, cliquez sur la liste déroulante pour filtrer l'affichage sur ces applications uniquement dans une catégorie spécifique. Sélectionnez **Tout** pour afficher toutes les applications.
- **Trier par** : Réorganisez la liste d'applications. Par défaut cette liste est triée selon **Le plus récent**.
- **Rechercher** : Vous ne trouvez toujours pas ce que vous cherchez ? Entrez des mots clés dans la zone de recherche pour le trouver.
- **Basculer la vue** : cliquez sur les icônes pour basculer entre le mode Liste et le mode Mosaïque. Par défaut, la liste d'applications s'affiche sous forme de vignettes de graphique.
  - Mode Mosaïque : Votre administrateur informatique peut personnaliser les icônes. Sous chaque vignette s'affiche le nom de l'application, l'éditeur et la version.
  - Mode Liste : Cette vue affiche l'icône, le nom, l'éditeur, la version et l'état de l'application.

**Installer plusieurs applications**

Installez plusieurs applications à la fois au lieu d'attendre la fin de l'une pour lancer la suivante. Les applications ne répondent pas toutes aux critères suivants :

- L'application est visible par vous
- L'application n'est pas encore en cours de téléchargement ou installée

- Votre administrateur informatique ne demande pas d'approbation pour installer l'application

Pour installer plusieurs applications à la fois :

1. Pour activer le mode de multisélection dans le mode Liste, cliquez sur l'icône de multisélection dans le coin supérieur droit.
2. Sélectionnez plusieurs applications à installer en cochant la case à gauche des applications dans la liste.
3. Cliquez sur le bouton **Installer les éléments sélectionnés**.

Les applications s'installent normalement, l'une après l'autre.

## Mises à jour

Cliquez sur l'onglet **Mises à jour** pour afficher et installer les mises à jour logicielles que votre administrateur informatique déploie sur cet ordinateur.

- **Tout** : Affiche toutes les mises à jour que vous pouvez installer
- **Obligatoire** : Votre administrateur informatique impose ces mises à jour.
- **Trier par** : Réorganisez la liste de mises à jour. Par défaut cette liste est triée par **Nom d'application : A-Z**.

Pour installer les mises à jour, cliquez sur **Tout installer**.

Pour installer uniquement des mises à jour spécifiques, cliquez sur l'icône pour basculer sur le mode multisélection. Examinez les mises à jour à installer, puis cliquez sur **Installer la sélection**.

## Systèmes d'exploitation

Cliquez sur l'onglet **Systèmes d'exploitation** pour afficher et installer les versions de Windows que votre administrateur informatique déploie sur cet ordinateur.

- **Tout** : Affiche toutes les versions de Windows que vous pouvez installer
- **Obligatoire** : Votre administrateur informatique impose ces mises à niveau.
- **Trier par** : Réorganisez la liste de mises à jour. Par défaut cette liste est triée par **Nom d'application : A-Z**.

## État de l'installation

Cliquez sur l'onglet **État d'installation** pour afficher l'état des applications. Vous pouvez voir les états suivants :

- **Installé**: Le Centre logiciel a déjà installé cette application sur cet ordinateur.
- **Téléchargement** : Le Centre logiciel télécharge le logiciel à installer sur cet ordinateur.
- **Échec** : Le Centre logiciel a rencontré une erreur en essayant d'installer le logiciel.

## Conformité de l'appareil

Cliquez sur l'onglet **Conformité de l'appareil** pour afficher l'état de conformité de cet ordinateur.

Cliquez sur **Vérifier la conformité** pour évaluer les paramètres de l'appareil par rapport aux stratégies de sécurité définies par votre administrateur informatique.

## Options

Cliquez sur l'onglet **Options** pour afficher les paramètres supplémentaires pour cet ordinateur.

**Informations d'utilisation**

Indiquer vos heures de travail habituelles. Votre administrateur informatique peut planifier des installations de logiciels en dehors des heures de travail. Réservez au moins quatre heures par jour pour les tâches de maintenance

système. Votre administrateur informatique peut toujours installer les applications et les mises à jour logicielles critiques pendant les heures de travail.

- Cliquez sur les listes déroulantes pour sélectionner la plage horaire la plus large pendant laquelle vous êtes susceptible d'utiliser l'ordinateur. Par défaut, ces valeurs vont de **5 h 00** à **22 h 00**
- Cochez la case à côté des jours de la semaine pendant lesquels vous utilisez généralement cet ordinateur. Le Centre logiciel sélectionne uniquement les jours de semaine par défaut.

**Gestion de l'alimentation**

Votre administrateur informatique peut définir des stratégies de gestion d'alimentation. Ces stratégies permettent à votre organisation d'économiser l'électricité quand l'ordinateur n'est pas utilisé.

Pour exempter cet ordinateur de ces stratégies, cochez la case **Ne pas appliquer les paramètres d'alimentation de mon service informatique à cet ordinateur**. Ce paramètre est désactivé par défaut, l'ordinateur applique les paramètres d'alimentation.

**Maintenance de l'ordinateur**

Spécifier la façon dont le Centre logiciel applique les modifications de logiciel avant l'échéance

- **Installer ou désinstaller automatiquement les logiciels obligatoires et redémarrer l'ordinateur uniquement en dehors des heures de bureau spécifiées** : Ce paramètre est désactivé par défaut.
- **Suspendre les activités du Centre logiciel quand mon ordinateur est en mode présentation** : Ce paramètre est activé par défaut.
- **Stratégie de synchronisation** : Cliquez sur ce bouton quand votre administrateur informatique vous l'indique. Cet ordinateur recherche sur les serveurs toutes les nouveautés en termes d'applications, de mises à jour logicielles ou de systèmes d'exploitation.

# Principes de base de System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Si vous découvrez System Center Configuration Manager, lisez les rubriques sur les principes fondamentaux pour en savoir plus sur les concepts de base de Configuration Manager avant d'exécuter le programme d'installation pour installer votre premier site. Si vous connaissez déjà Configuration Manager, vous pouvez l'utiliser directement. Nous vous recommandons de commencer avec la section Nouveautés de System Center Configuration Manager.

Pour plus d'informations sur les systèmes d'exploitation et les environnements pris en charge, sur la configuration matérielle requise et sur la capacité, consultez Configurations prises en charge pour System Center Configuration Manager.

Quand vous déployez Configuration Manager, vous déployez un ou plusieurs sites :

- **Quand vous déployez plusieurs sites**, les sites établissent des relations enfant/parent qui, ensemble, constituent une hiérarchie. Utilisez une hiérarchie pour gérer de manière centralisée un plus grand nombre de sites et d'appareils. Les données et les informations parcourent la hiérarchie de haut en bas jusqu'aux appareils que vous gérez. À l'inverse, les informations sur les appareils et les résultats des tâches de configuration et des demandes parcourent la hiérarchie de bas en haut.
- **Si vous déployez un site unique**, il est également appelé hiérarchie.

  Certains paramètres et tâches de configuration s'appliquent à tous les sites d'une hiérarchie, tandis que d'autres ne s'appliquent qu'à certains d'entre eux.

## Concepts fondamentaux de System Center Configuration Manager

Consultez les rubriques suivantes pour en savoir plus sur les concepts fondamentaux de System Center Configuration Manager :

- Notions de base des sites et des hiérarchies pour System Center Configuration Manager
- Notions de base de la gestion des appareils avec System Center Configuration Manager
- Notions de base des tâches de gestion des clients pour System Center Configuration Manager
- Notions de base de la sécurité pour System Center Configuration Manager

# Notions de base des sites et des hiérarchies pour System Center Configuration Manager

22/06/2018 • 10 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Un déploiement de System Center Configuration Manager doit être installé dans un domaine Active Directory. La base de ce déploiement inclut un ou plusieurs sites Configuration Manager qui forment une hiérarchie de sites. Qu'il s'agisse d'un site unique ou d'une hiérarchie à plusieurs sites, le type et l'emplacement des sites que vous installez permettent de faire monter en puissance (développer) votre déploiement si nécessaire et d'offrir des services clés aux appareils et utilisateurs gérés.

## Hiérarchies de sites

Quand vous installez System Center Configuration Manager pour la première fois, le premier site Configuration Manager que vous installez détermine l'étendue de votre hiérarchie. Le premier site Configuration Manager constitue la base à partir de laquelle vous allez gérer les appareils et les utilisateurs dans votre entreprise. Ce premier site doit être un site d'administration centrale ou un site principal autonome.

Un *site d'administration centrale* convient aux déploiements à grande échelle. Il fournit un point d'administration centrale et offre la flexibilité nécessaire pour prendre en charge les appareils distribués dans une infrastructure réseau globale. Après avoir installé un site d'administration centrale, vous devez installer un ou plusieurs sites principaux comme sites enfants. Cette configuration est requise du fait qu'un site d'administration centrale ne prend pas directement en charge la gestion des appareils, ce qui est la fonction d'un site principal. Un site d'administration centrale peut prendre en charge plusieurs sites principaux enfants. Les sites principaux enfants permettent de gérer directement des appareils, mais aussi de contrôler la bande passante réseau quand vos appareils gérés ne se trouvent pas tous au même emplacement géographique.

Un *site principal autonome* convient pour des déploiements plus petits et permet de gérer des appareils sans devoir installer des sites supplémentaires. Un site principal autonome peut limiter la taille de votre déploiement, mais il prend en charge un scénario d'extension ultérieure de votre hiérarchie par l'installation d'un nouveau site d'administration centrale. Dans ce scénario d'extension du site, votre site principal autonome devient un site principal enfant, et vous pouvez installer des sites principaux enfants supplémentaires sous votre nouveau site d'administration centrale. Vous pouvez alors étendre votre déploiement initial dans la perspective d'une croissance future de votre entreprise.

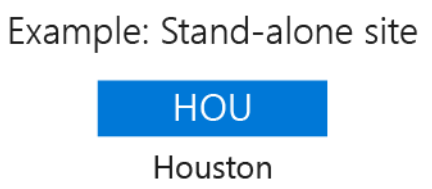
> **TIP**
> Un site principal autonome et un site principal enfant sont en fait du même type : il s'agit de sites principaux. La différence de nom est basée sur la relation de hiérarchie qui est créée quand vous utilisez également un site d'administration centrale. Cette relation de hiérarchie peut également limiter l'installation de certains rôles système de site qui étendent les fonctionnalités de Configuration Manager. Cette limitation est due au fait que certains rôles de système de site peuvent uniquement être installés sur le site de niveau supérieur de la hiérarchie, un site d'administration centrale ou un site principal autonome.

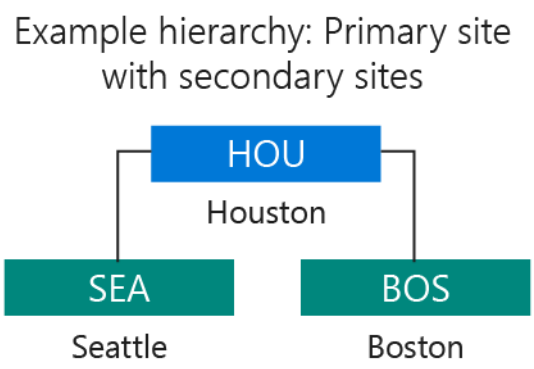
Après avoir installé votre premier site, vous pouvez installer des sites supplémentaires. Si votre premier site est un site d'administration centrale, vous pouvez installer un ou plusieurs sites principaux enfants. Après avoir installé un site principal (autonome ou principal de l'enfant), vous pouvez installer un ou plusieurs sites secondaires.

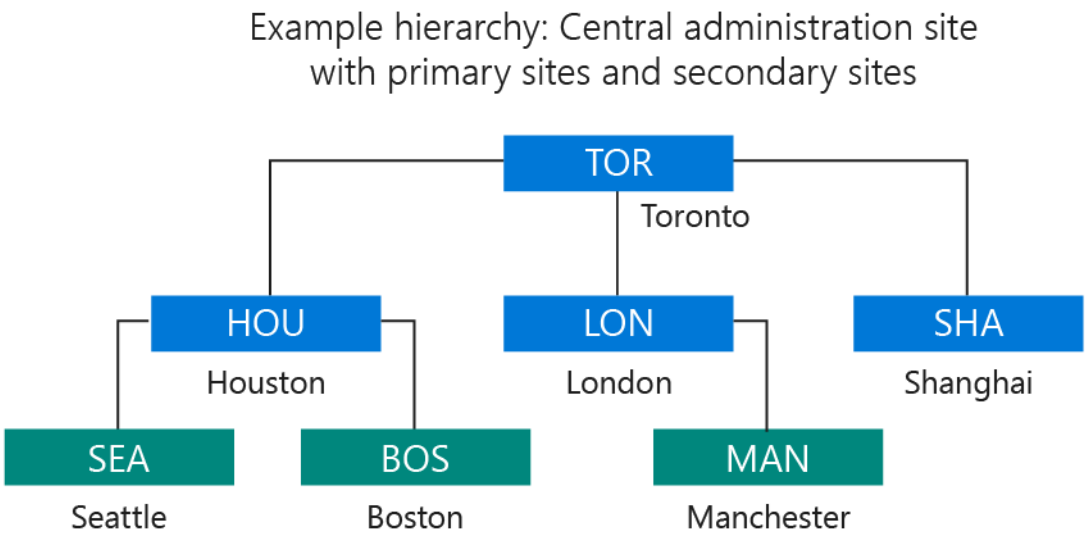
Un *site secondaire* peut uniquement être installé en tant que site enfant sous un site principal. Ce type de site étend

la portée d'un site principal à la gestion de périphériques situés dans des emplacements où la connexion réseau au site principal est lente. Même si un site secondaire étend le site principal, le site principal gère l'ensemble des clients. Le site secondaire assure la prise en charge des appareils de l'emplacement distant. Pour cela, il comprime les informations que vous envoyez (déployez) aux clients et celles que ces clients renvoient au site, et gère leur transfert sur votre réseau.

Les schémas suivants offrent des exemples d'architecture de site.




Pour plus d'informations, consultez les rubriques suivantes :

- Présentation de System Center Configuration Manager
- Concevoir une hiérarchie de sites pour System Center Configuration Manager
- Installer des sites System Center Configuration Manager

## Serveurs de système de site et rôles de système de site

Chaque site Configuration Manager installe des *rôles de système de site* qui prennent en charge les opérations de gestion. Les rôles suivants sont installés par défaut quand vous installez un site :

- Le rôle serveur de site est affecté à l'ordinateur sur lequel vous installez le site.
- Le rôle serveur de base de données de site est affecté à l'ordinateur SQL Server qui héberge la base de données du site.

Les autres rôles de système de site sont facultatifs. Utilisez-les uniquement si vous souhaitez utiliser des fonctionnalités qui sont actives dans ces rôles de système de site. Tout ordinateur hébergeant un rôle système de

site est considéré comme un serveur de système de site.

Pour un déploiement plus petit de Configuration Manager, vous pouvez initialement exécuter tous vos rôles de système de site directement sur l'ordinateur du serveur de site. Ensuite, à mesure que votre environnement géré et vos besoins augmentent, vous pouvez installer des serveurs de système de site supplémentaires pour héberger des rôles de système de site supplémentaires. Cela vous permet d'optimiser le site en fournissant des services à davantage d'appareils.

Pour plus d'informations sur les différents rôles de système de site, consultez Rôles de système de site dans Planifier des serveurs de système de site et des rôles de système de site pour System Center Configuration Manager.

## Publication d'informations de site vers les services de domaine Active Directory

Pour simplifier la gestion de Configuration Manager, vous pouvez étendre le schéma Active Directory pour qu'il prenne en charge les informations utilisées par Configuration Manager, puis faire en sorte que les sites publient leurs informations clés sur les services de domaine Active Directory (AD DS). Les ordinateurs que vous souhaitez gérer peuvent ensuite récupérer en toute sécurité les informations relatives au site à partir de la source approuvée d'AD DS. Les informations que les clients peuvent récupérer identifient les sites disponibles, les serveurs de système de site et les services que ces serveurs fournissent.

*L'extension du schéma Active Directory* n'est effectuée qu'une fois pour chaque forêt, au choix avant ou après l'installation de Configuration Manager. Quand vous étendez le schéma, vous devez créer un conteneur Active Directory nommé System Management dans chaque domaine. Le conteneur fournit un site Configuration Manager qui publie les données dont les clients ont besoin. Pour plus d'informations, consultez Préparer Active Directory pour la publication de site.

La *publication des données du site* renforce la sécurité de votre hiérarchie Configuration Manager et réduit la surcharge administrative, mais elle est facultative pour les fonctionnalités de base de Configuration Manager.

# À propos de la mise à niveau, de la mise à jour et de l'installation pour l'infrastructure de site et de hiérarchie

22/06/2018 • 4 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Lors de la gestion de l'infrastructure de site et de hiérarchie de System Center Configuration Manager, les termes *mise à niveau*, *mise à jour* et *installation* sont utilisés pour décrire trois concepts distincts.

## Mettre à niveau

La *mise à niveau* ou *mise à niveau en place* est utilisée lors de la conversion de votre site ou hiérarchie Configuration Manager 2012 vers un site ou une hiérarchie qui exécute System Center Configuration Manager. Lorsque vous mettez à niveau System Center 2012 Configuration Manager vers System Center Configuration Manager, vous continuez à utiliser les mêmes serveurs pour héberger vos sites et serveurs de site, et vous conservez vos données et configurations existantes pour Configuration Manager. Cela est différent de la migration qui est une façon de conserver vos configurations et données concernant les périphériques gérés tout en utilisant de nouveaux sites System Center Configuration Manager installés sur du nouveau matériel.

Pour plus d'informations, consultez Mettre à niveau vers System Center Configuration Manager.

## Mise à jour

La *mise à jour* est utilisée pour l'installation de mises à jour dans la console pour System Center Configuration Manager et pour les mises à jour hors bande qui sont des mises à jour qui ne peuvent pas être fournies à partir de la console Configuration Manager. Les mises à jour dans la console peuvent modifier la version de votre site Current Branch (ou site Technical Preview) afin qu'il exécute une version ultérieure. Par exemple, si votre site exécute la version 1606, vous pouvez installer une mise à jour pour la version 1610. Les mises à jour peuvent également installer des correctifs pour un problème connu, sans modifier la version des sites.

En règle générale, les mises à jour ajoutent des correctifs de sécurité, apportent une amélioration de la qualité et de nouvelles fonctionnalités à votre déploiement existant. Si vous utilisez la branche Technical Preview, une mise à jour peut installer une version plus récente de Technical Preview.

- Vous choisissez quand installer la mise à jour dans la console, en commençant par le site de niveau supérieur dans votre hiérarchie.
- Vous pouvez installer toute mise à jour disponible à partir de la console. Par exemple, si votre site exécute la version 1602 et que les versions 1606 et 1610 sont proposées, envisagez d'installer la version 1610, car chaque version inclut les fonctionnalités qui ont été mises à disposition dans les versions précédentes.
- Une fois l'installation d'une nouvelle mise à jour terminée sur votre site de niveau supérieur, les sites principaux enfants démarrent automatiquement le processus de mise à jour. Toutefois, vous pouvez définir des fenêtres de maintenance pour contrôler la planification des mises à jour.
- Les sites secondaires n'installent pas automatiquement les mises à jour. Vous devez démarrer manuellement la mise à jour à partir de la console Configuration Manager.

Pour plus d'informations, consultez Mises à jour pour System Center Configuration Manager et Technical Preview pour System Center Configuration Manager.

# Installez

*L'installation* est utilisée lors de la création d'une nouvelle hiérarchie Configuration Manager ou l'ajout de sites supplémentaires à une hiérarchie existante.

Lorsque vous installez un nouveau site principal ou un site d'administration centrale, l'emplacement de setup.exe et de ses fichiers source associés que vous utilisez dépend de votre scénario d'installation.

Pour plus d'informations, consultez Préparer l'installation des sites.

# Notions de base de la gestion des appareils avec System Center Configuration Manager

22/06/2018 • 8 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

System Center Configuration Manager peut gérer deux grandes catégories d'appareils :

- Les *clients* sont des appareils comme les stations de travail, les ordinateurs portables, les serveurs et les appareils mobiles sur lesquels vous installez le logiciel client Configuration Manager. Certaines fonctions de gestion, comme l'inventaire matériel, nécessitent ce logiciel client.
- Les *appareils gérés* peuvent inclure des *clients*, mais il s'agit généralement d'un appareil mobile sur lequel le logiciel client Configuration Manager n'est pas installé. Sur ce type d'appareil, vous effectuez la gestion en utilisant Intune ou la fonctionnalité de gestion locale des appareils mobiles intégrée de Configuration Manager.

Vous pouvez aussi regrouper et identifier des appareils en fonction de l'utilisateur, et pas seulement du type de client.

## Gestion des appareils avec le client Configuration Manager

Il existe deux façons d'utiliser le logiciel client Configuration Manager pour gérer un appareil. La première consiste à détecter l'appareil sur votre réseau, puis à déployer le logiciel client sur cet appareil. L'autre consiste à installer manuellement le logiciel client sur un nouvel ordinateur, puis à faire en sorte que cet ordinateur rejoigne votre site quand il rejoint votre réseau. Pour détecter les appareils sur lesquels le logiciel client n'est pas installé, exécutez une ou plusieurs des méthodes de découverte intégrées. Après la découverte d'un appareil, vous pouvez utiliser une des différentes méthodes disponibles pour installer le logiciel client. Pour plus d'informations sur l'utilisation de la découverte, consultez Exécuter la découverte pour System Center Configuration Manager.

Après la découverte des appareils pris en charge pour exécuter le logiciel client Configuration Manager, vous pouvez installer le logiciel avec l'une des différentes méthodes disponibles. Une fois le logiciel installé et le client affecté à un site principal, vous pouvez commencer à gérer l'appareil. Les méthodes d'installation courantes sont les suivantes :

- Installation Push du client.
- Installation basée sur une mise à jour logicielle.
- Stratégie de groupe.
- Installation manuelle sur un ordinateur.
- Client inclus comme partie d'une image de système d'exploitation que vous déployez.

Une fois le client installé, vous pouvez simplifier les tâches de gestion des appareils en utilisant des regroupements. Les regroupements sont des groupes d'appareils ou d'utilisateurs que vous créez afin de pouvoir les gérer en tant que groupe. Imaginons, par exemple, que vous souhaitez installer une application d'appareil mobile sur tous les appareils mobiles inscrits par Configuration Manager. Dans ce cas, vous pouvez utiliser le regroupement Tous les appareils mobiles.

Pour plus d'informations, consultez ces rubriques :

- Choisir une solution de gestion d'appareils pour System Center Configuration Manager
- Méthodes d'installation du client dans System Center Configuration Manager
- Présentation des regroupements dans System Center Configuration Manager

**Paramètres du client**

Quand vous installez Configuration Manager pour la première fois, tous les clients de la hiérarchie sont configurés avec les paramètres client par défaut. Vous pouvez ensuite modifier ces paramètres, si vous le souhaitez. Les paramètres client comprennent des options de configuration suivantes :

- Fréquence à laquelle les appareils communiquent avec le site.
- Configuration éventuelle du client pour les mises à jour logicielles et autres opérations de gestion.
- La possibilité, pour les utilisateurs, d'inscrire leurs appareils mobiles afin qu'ils soient gérés par Configuration Manager.

Vous pouvez créer des paramètres client personnalisés et les affecter ensuite à des regroupements. Les membres du regroupement sont configurés pour utiliser les paramètres personnalisés, et vous pouvez créer plusieurs paramètres client personnalisés qui s'appliquent dans l'ordre (numérique) que vous spécifiez. En cas de conflit entre paramètres, le paramètre dont le numéro d'ordre est le plus petit remplace les autres paramètres.

Le schéma ci-dessous montre comment créer et appliquer des paramètres client personnalisés.

Pour en savoir plus sur les paramètres client, consultez
Guide pratique pour configurer les paramètres client dans System Center Configuration Manager et À propos des paramètres client dans System Center Configuration Manager.

## Gestion des appareils sans client Configuration Manager

Configuration Manager prend en charge la gestion de certains appareils sur lesquels le logiciel client n'est pas installé et qui ne sont pas gérés par Intune. Pour plus d'informations, consultez Gérer des appareils mobiles avec une infrastructure locale dans System Center Configuration Manager et Gérer des appareils mobiles à l'aide de System Center Configuration Manager et d'Exchange.

## Gestion basée sur l'utilisateur

Configuration Manager prend en charge les regroupements d'utilisateurs des services de domaine Active Directory. Quand vous utilisez un regroupement d'utilisateurs, vous pouvez installer le logiciel sur tous les ordinateurs utilisés par les membres du regroupement. Pour garantir que les logiciels que vous déployez s'installent uniquement sur les appareils spécifiés en tant qu'appareil principal d'un utilisateur, configurez l'affinité entre appareil et utilisateur. Un utilisateur peut posséder un ou plusieurs appareils principaux.

L'une des façons pour les utilisateurs de contrôler leur expérience de déploiement de logiciels consiste à utiliser l'interface client du **Centre logiciel**. Le **Centre logiciel** est automatiquement installé sur les ordinateurs clients, et est exécuté à partir du menu **Démarrer**. Le **Centre logiciel** permet aux utilisateurs de gérer leurs propres logiciels et d'exécuter les tâches suivantes :

- Installez le logiciel.
- Planifiez l'installation automatique du logiciel en dehors des heures de travail.
- Configurez le moment où Configuration Manager peut installer le logiciel sur un appareil.
- Configurez les paramètres d'accès pour le contrôle à distance, si ce dernier est configuré dans Configuration Manager.

- Configurez les options de gestion de l'alimentation si un administrateur configure cette option.

Un lien disponible dans le **Centre logiciel** permet aux utilisateurs de se connecter au **catalogue d'applications**, où ils peuvent parcourir, installer et demander des logiciels. Le **catalogue d'applications** est également utilisé pour configurer les paramètres de préférence, pour réinitialiser des appareils mobiles et, quand il est configuré, pour spécifier un appareil principal pour l'affinité entre appareil et utilisateur.

Les utilisateurs peuvent également accéder au **catalogue d'applications** par le biais d'un intranet de navigateur ou une session Internet.

# Principes de base des tâches de gestion des clients pour System Center Configuration Manager

22/06/2018 • 6 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Après avoir installé les clients System Center Configuration Manager, vous les gérez en exécutant plusieurs tâches. Certaines tâches sont exécutées à partir de la console Configuration Manager. D'autres sont exécutées à partir de l'application cliente Configuration Manager. L'application cliente Configuration Manager est installée avec le logiciel client Configuration Manager.

## Tâches de la console Configuration Manager

Dans la console Configuration Manager, vous pouvez effectuer diverses tâches de gestion de clients :

- Déployer des applications, des mises à jour logicielles, des scripts de maintenance et des systèmes d'exploitation. Configurer l'installation à une date et une heure précises, rendre le logiciel disponible pour que les utilisateurs l'installent sur demande ou configurer la désinstallation des applications.
- Protéger les ordinateurs contre les logiciels malveillants et menaces de sécurité, et recevoir un avertissement lorsque des problèmes sont détectés.
- Définir les paramètres de configuration client que vous voulez surveiller et corriger s'ils ne sont pas conformes.
- Recueillir des informations d'inventaire matériel et logiciel, qui comprennent la surveillance et le rapprochement des informations de licence de Microsoft.
- Dépanner des ordinateurs à l'aide d'un contrôle à distance.
- Implémenter des paramètres de gestion de l'alimentation pour gérer et surveiller la consommation d'énergie des ordinateurs.

La console Configuration Manager surveille les tâches précédentes presqu'en temps réel. Les informations sur l'état et les notifications pour chaque tâche sont disponibles dans la console Configuration Manager. Pour capturer des données et des tendances historiques, utilisez les fonctions de rapport intégrées de SQL Server Reporting Services. Les clients envoient des détails au site en tant qu'état du client. Les informations d'état du client fournissent des indications sur l'intégrité et l'activité du client ; elles sont visibles dans la console ou à l'aide de rapports intégrés pour Configuration Manager. Ces données permettent d'identifier les ordinateurs qui ne répondent pas. Dans certains cas, les problèmes sont résolus automatiquement.

Pour plus d'informations sur les tâches de gestion pour les clients, consultez Comment gérer les clients dans System Center Configuration Manager et Comment gérer les clients pour des serveurs Linux et UNIX dans System Center Configuration Manager. Pour en savoir plus sur l'utilisation de rapports, consultez Présentation des rapports dans System Center Configuration Manager.

## Application cliente Configuration Manager

Quand vous installez le logiciel client Configuration Manager, l'application cliente Configuration Manager est également installée. Contrairement au Centre logiciel, l'application cliente Configuration Manager s'adresse plus au service de support technique qu'aux utilisateurs finaux. Certaines options de configuration nécessitent des autorisations administratives locales et la plupart des options requièrent des connaissances techniques sur le

fonctionnement de l'application cliente Configuration Manager. Vous pouvez utiliser cette application pour effectuer les tâches suivantes sur un client :

- Consulter les propriétés sur le client : numéro de version, site attribué, point de gestion avec lequel il communique et certificat utilisé, à savoir certificat d'infrastructure à clé publique (PKI) ou certificat auto-signé.
- Vérifier que le client a correctement téléchargé une stratégie client après son installation initiale. Vérifier également que les paramètres client sont activés ou désactivés comme prévu, en fonction des paramètres client configurés dans la console Configuration Manager.
- Démarrer les actions du client, par exemple télécharger la stratégie client si une modification a été récemment apportée à la configuration dans la console Configuration Manager et que vous ne souhaitez pas attendre la prochaine heure planifiée.
- Affecter manuellement un client à un site Configuration Manager ou essayer de trouver un site. Spécifier ensuite le suffixe DNS pour les points de gestion qui publient sur DNS.
- Configurer le cache du client qui stocke temporairement les fichiers. Supprimer ensuite les fichiers du cache si vous avez besoin de plus d'espace disque pour installer les logiciels.
- Configurer les paramètres de gestion des clients basés sur Internet.
- Consulter les lignes de base de configuration qui ont été déployées sur le client, lancer une évaluation de la compatibilité et consulter les rapports de compatibilité.

# Notions de base de la sécurité pour System Center Configuration Manager

22/06/2018 • 8 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

La sécurité pour System Center Configuration Manager se compose de plusieurs couches. La première couche est fournie par les fonctionnalités de sécurité Windows tant pour le système d'exploitation que pour le réseau, qui incluent :

- Le partage de fichiers pour transférer des fichiers entre les composants Configuration Manager.
- Des listes de contrôle d'accès pour sécuriser les fichiers et les clés de Registre.
- La sécurité du protocole Internet (IPsec) pour sécuriser les communications.
- Une stratégie de groupe pour définir la stratégie de sécurité.
- Des autorisations DCOM (Distributed Component Object Model) pour les applications distribuées, comme la console Configuration Manager.
- Des services de domaine Active Directory pour stocker les entités de sécurité.
- La sécurité de compte Windows, notamment certains groupes qui sont créés pendant la configuration de Configuration Manager.

Des composants de sécurité supplémentaires (pare-feu, détection d'intrusion, par exemple) aident à protéger l'ensemble de l'environnement. Les certificats émis par des implémentations d'infrastructure à clé publique (PKI) standard permettent de fournir une authentification, une signature et un chiffrement.

Outre la sécurité fournie par l'infrastructure réseau et de serveur Windows, Configuration Manager contrôle l'accès à la console Configuration Manager et à ses ressources de plusieurs façons. Par défaut, seuls les administrateurs locaux disposent d'autorisations sur les fichiers et les clés de Registre nécessaires à l'exécution de la console Configuration Manager sur les ordinateurs où elle est installée.

La couche de sécurité suivante est basée sur l'accès via WMI (Windows Management Instrumentation), en particulier le fournisseur SMS. Le fournisseur SMS est un composant Configuration Manager qui octroie un accès à un utilisateur pour interroger la base de données du site afin d'obtenir des informations. Par défaut, l'accès au fournisseur est restreint aux membres du groupe Administrateurs SMS local. À l'origine, ce groupe contient uniquement l'utilisateur qui a installé Configuration Manager. Pour accorder d'autres autorisations de compte à l'emplacement de stockage CIM (Common Information Model) et au fournisseur SMS, ajoutez les autres comptes au groupe Administrateurs SMS.

Les autorisations d'accès aux objets de la base de données de site constituent la dernière couche de sécurité. Par défaut, le compte système local et le compte d'utilisateur que vous utilisez pour installer Configuration Manager peuvent administrer tous les objets de la base de données du site. Vous pouvez accorder et limiter les autorisations à des utilisateurs administratifs supplémentaires dans la console Configuration Manager à l'aide de l'administration basée sur des rôles.

## Administration basée sur des rôles

Configuration Manager utilise l'administration basée sur des rôles pour sécuriser les objets (regroupements, déploiements, sites, etc.). Ce modèle d'administration définit et gère de façon centralisée les paramètres d'accès de

sécurité à l'échelle de la hiérarchie pour tous les sites et les paramètres du site. Les rôles de sécurité sont attribués aux utilisateurs administratifs et aux autorisations de groupe. Les autorisations sont connectées à différents types d'objet Configuration Manager, comme les autorisations qui sont utilisées pour créer ou modifier les paramètres du client. Les étendues de sécurité regroupent des instances d'objets spécifiques qu'un utilisateur administratif est chargé de gérer, par exemple une application qui installe Microsoft Office. La combinaison des rôles de sécurité, des étendues de sécurité et des regroupements définit les objets qu'un utilisateur administratif peut afficher et gérer. Configuration Manager installe des rôles de sécurité par défaut pour les tâches de gestion classiques. Vous pouvez toutefois créer vos propres rôles de sécurité, en fonction des besoins propres à votre activité.

Pour plus d'informations, consultez Configurer l'administration basée sur des rôles pour System Center Configuration Manager.

## Sécurisation des points de terminaison des clients

La communication du client vers les rôles de système de site est sécurisée à l'aide de certificats auto-signés ou de certificats PKI. Vous devez utiliser un certificat PKI pour les ordinateurs clients que Configuration Manager détecte sur Internet ainsi que pour les clients d'appareil mobile. Le certificat PKI utilise le protocole HTTPS pour sécuriser les points de terminaison clients. Les rôles de système de site auxquels les clients se connectent peuvent être configurés pour utiliser les protocoles HTTPS ou HTTP dans le cadre de la communication avec les clients. Les ordinateurs clients communiquent toujours à l'aide de la méthode la plus sécurisée disponible. Les ordinateurs clients n'utilisent le protocole HTTP sur l'intranet que si vos rôles de système de site permettent la communication HTTP.

Pour plus d'informations, consultez Informations techniques de référence sur les contrôles de chiffrement pour System Center Configuration Manager.

## Comptes et groupes de Configuration Manager

Configuration Manager utilise le compte Système local pour la plupart des opérations de site. Certaines tâches de gestion peuvent nécessiter la création et la gestion de comptes supplémentaires. Plusieurs groupes par défaut et rôles SQL Server sont créés pendant l'installation. Vous devez peut-être ajouter manuellement des comptes d'ordinateur ou d'utilisateur à ces groupes par défaut et à ces rôles SQL Server.

Pour plus d'informations, consultez Comptes utilisés dans System Center Configuration Manager.

## Confidentialité

Bien que les produits de gestion d'entreprise offrent de nombreux avantages, car ils permettent de gérer efficacement un grand nombre de clients, vous devez également être conscient de l'impact de ces logiciels sur la confidentialité des utilisateurs de votre organisation. System Center Configuration Manager comprend de nombreux outils pour collecter les données et surveiller les appareils. Certains outils sont susceptibles de poser des problèmes de confidentialité.

Par exemple, quand vous installez le client Configuration Manager, de nombreux paramètres de gestion sont activés par défaut. Par conséquent, le logiciel client envoie des informations au site Configuration Manager. Les informations du client sont stockées dans la base de données Configuration Manager et ne sont pas envoyées à Microsoft. Avant d'implémenter System Center Configuration Manager, pensez à vos exigences en matière de confidentialité.

# Principes de base de l'administration basée sur des rôles pour System Center Configuration Manager

22/06/2018 • 16 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Avec System Center Configuration Manager, l'administration basée sur des rôles vous permet de sécuriser l'accès nécessaire à l'administration de Configuration Manager. Vous sécurisez également l'accès aux objets que vous gérez, tels que les regroupements, les déploiements et les sites. À présent que vous comprenez les concepts présentés dans cette rubrique, vous pouvez configurer l'administration basée sur des rôles pour System Center Configuration Manager.

Le modèle d'administration basée sur des rôles définit et gère de façon centralisée les paramètres d'accès de sécurité à l'échelle de la hiérarchie pour tous les sites ainsi que les paramètres de site à l'aide des éléments suivants :

- Les *rôles de sécurité* sont attribués aux utilisateurs administratifs pour octroyer à ceux-ci (ou à des groupes d'utilisateurs) des autorisations relatives à différents objets Configuration Manager, par exemple, celles de créer ou modifier des paramètres client.
- Les *étendues de sécurité* permettent de regrouper des instances d'objets spécifiques qu'un utilisateur administratif est chargé de gérer, par exemple une application qui installe Microsoft Office 2010.
- Les *regroupements* permettent de spécifier des groupes de ressources d'utilisateurs et d'appareils que l'utilisateur administratif peut gérer.

  L'utilisation combinée de rôles de sécurité, d'étendues de sécurité et de regroupements permet de séparer les attributions administratives répondant aux besoins de votre organisation, ainsi que de définir l'étendue administrative d'un utilisateur, autrement dit ce qu'il peut afficher et gérer dans votre déploiement de Configuration Manager.

## Avantages de l'administration basée sur des rôles

- Les sites ne sont pas utilisés comme limites administratives.
- Après avoir créé des utilisateurs administratifs pour la hiérarchie, il vous suffit de leur attribuer une étendue de sécurité une seule fois.
- Toutes les attributions de sécurité sont répliquées et disponibles dans la hiérarchie.
- Il existe des rôles de sécurité intégrés permettent d'attribuer les tâches d'administration classiques, mais vous pouvez aussi créer vos propres rôles de sécurité personnalisés en fonction des besoins propres à votre activité.
- Les utilisateurs administratifs voient uniquement les objets qu'ils sont autorisés à gérer.
- Vous pouvez auditer des actions administratives de sécurité.

Quand vous concevez et implémentez la sécurité administrative pour Configuration Manager, créez une *étendue administrative* pour un utilisateur administratif à l'aide des éléments suivants :

- Rôles de sécurité
- Regroupements

- Étendues de sécurité

L'étendue administrative contrôle les objets qu'un utilisateur administratif peut afficher dans la console Configuration Manager et les autorisations dont dispose cet utilisateur sur ces objets. Les configurations d'administration basées sur des rôles sont répliquées sur chaque site de la hiérarchie en tant que données globales, puis sont appliquées à toutes les connexions administratives.

> **IMPORTANT**
> Les retards de réplication intersite peuvent empêcher un site de recevoir des modifications pour l'administration basée sur les rôles. Pour plus d'informations sur la manière de surveiller la réplication intersite de base de données, consultez la rubrique Transfert de données entre sites dans System Center Configuration Manager.

## Rôles de sécurité

Utilisez des rôles de sécurité pour accorder des autorisations de sécurité aux utilisateurs administratifs. Les rôles de sécurité sont des groupes d'autorisations de sécurité que vous affectez aux utilisateurs administratifs afin qu'ils puissent effectuer leurs tâches administratives. Ces autorisations de sécurité définissent les actions administratives réalisables par un utilisateur administratif ainsi que les autorisations sont accordées pour des types d'objet particulier. Comme bonne pratique de sécurité, affectez les rôles de sécurité qui fournissent des autorisations minimales.

Configuration Manager possède plusieurs rôles de sécurité intégrés pour prendre en charge des regroupements typiques de tâches administratives et vous pouvez créer vos propres rôles de sécurité personnalisés pour prendre en charge vos besoins professionnels spécifiques. Exemples de rôles de sécurité intégrés :

- *Administrateur complet* : accorde toutes les autorisations dans Configuration Manager.
- *Gestionnaire de biens* : accorde des autorisations permettant de gérer le point de synchronisation Asset Intelligence, les classes de création de rapports Asset Intelligence, l'inventaire logiciel, l'inventaire matériel et les règles de contrôle.
- *Gestionnaire des mises à jour logicielles* : accorde les autorisations de définir et déployer des mises à jour logicielles. Les utilisateurs administratifs qui sont associés à ce rôle peuvent créer des regroupements, des groupes de mises à jour logicielles, des déploiements et des modèles.

> **TIP**
> Vous pouvez afficher la liste des rôles de sécurité intégrés et les rôles de sécurité personnalisés que vous créez, ainsi que leurs descriptions, dans la console Configuration Manager. Pour afficher les rôles, dans l'espace de travail **Administration**, développez **Sécurité**, puis sélectionnez **Rôles de sécurité**.

Chaque rôle de sécurité dispose d'autorisations spécifiques à différents types d'objets. Par exemple, le rôle de sécurité *Auteur d'application* a les autorisations suivantes pour les applications : Approuver, Créer, Supprimer, Modifier, Modifier un dossier, Déplacer un objet, Lire, Exécuter un rapport et Définir l'étendue de sécurité.

Vous ne pouvez pas modifier les autorisations pour les rôles de sécurité intégrés, mais vous pouvez copier le rôle, y apporter des modifications, puis enregistrer ces modifications sous un nouveau rôle de sécurité personnalisé. Vous pouvez également importer des rôles de sécurité que vous avez exportés depuis une autre hiérarchie, par exemple depuis un réseau de test. Passez en revue les rôles de sécurité et leurs autorisations pour déterminer si vous allez utiliser les rôles de sécurité intégrés ou devoir créer vos propres rôles de sécurité personnalisés.

**Pour faciliter la planification des rôles de sécurité**

1. Identifiez les tâches que les utilisateurs administratifs effectuent dans Configuration Manager. Ces tâches peuvent concerner un ou plusieurs groupes de tâches de gestion, tels que le déploiement d'applications et de packages, le déploiement de systèmes d'exploitation et de paramètres pour la conformité, la configuration de sites et de la sécurité, l'audit, le contrôle d'ordinateurs à distance et le recueil de données d'inventaire.
2. Mappez ces tâches administratives vers un ou plusieurs rôles de sécurité intégrés.
3. Si certains des utilisateurs administratifs effectuent des tâches de rôles de sécurité multiples, attribuez les rôles de sécurité multiples à ces utilisateurs administratifs au lieu de créer un nouveau rôle de sécurité qui combine les tâches.
4. Si les tâches que vous avez identifiées ne correspondent pas aux rôles de sécurité intégrés, créez et testez de nouveaux rôles de sécurité.

Pour plus d'informations sur la façon de créer et de configurer des rôles de sécurité pour l'administration basée sur des rôles, consultez Créer des rôles de sécurité personnalisés et Configurer des rôles de sécurité dans la rubrique Configurer l'administration basée sur des rôles pour System Center Configuration Manager.

## Regroupements

Les regroupements spécifient les ressources d'utilisateur et d'ordinateur qu'un utilisateur administratif peut consulter ou gérer. Par exemple, pour que les utilisateurs administratifs puissent déployer des applications ou effectuer un contrôle à distance, un rôle de sécurité qui leur permet d'accéder à un regroupement contenant ces ressources doit leur être attribué. Vous pouvez sélectionner des regroupements d'utilisateurs ou d'appareils.

Pour plus d'informations sur les regroupements, consultez Présentation des regroupements dans System Center Configuration Manager.

Avant de configurer l'administration basée sur les rôles, vérifiez si vous devez créer de nouveaux regroupements pour l'une des raisons suivantes :

- Organisation fonctionnelle. Par exemple, des regroupements distincts de serveurs et de stations de travail.
- Implantation géographique. Par exemple, des regroupements distincts pour l'Amérique du Nord et l'Europe.
- Exigences de sécurité et procédures commerciales. Par exemple, des regroupements distincts pour les ordinateurs de production et de test.
- Alignement de l'organisation. Par exemple, des regroupements distincts pour chaque unité d'exploitation.

Pour plus d'informations sur la façon de configurer des regroupements pour l'administration basée sur des rôles, consultez Configurer des regroupements pour gérer la sécurité dans la rubrique Configurer l'administration basée sur des rôles pour System Center Configuration Manager.

## Étendues de sécurité

Utilisez les étendues de sécurité pour permettre aux utilisateurs administratifs d'accéder à des objets sécurisables. Une étendue de sécurité est un ensemble nommé d'objets sécurisables attribués aux utilisateurs administratifs en tant que groupe. Tous les objets sécurisables doivent être affectés à une ou plusieurs étendues de sécurité. Configuration Manager possède deux étendues de sécurité intégrées :

- L'étendue de sécurité intégrée *Toutes* accorde l'accès à toutes les étendues. Vous ne pouvez pas attribuer d'objets à cette étendue de sécurité.
- L'étendue de sécurité intégrée *Par défaut* est utilisée pour tous les objets, par défaut. Lorsque vous

installez Configuration Manager pour la première fois, tous les objets sont attribués à cette étendue de sécurité.

Si vous souhaitez restreindre les objets que les utilisateurs administratifs peuvent voir et gérer, vous devez créer et utiliser vos propres étendues de sécurité personnalisées. Les étendues de sécurité ne prennent pas en charge une structure hiérarchique et ne peuvent pas être imbriquées. Les étendues de sécurité peuvent contenir un ou plusieurs types d'objet, dont les suivants :

- Abonnements aux alertes
- Applications
- Images de démarrage
- Groupes de limites
- Éléments de configuration
- Paramètres client personnalisés
- Points de distribution et groupes de points de distribution
- Packages de pilotes
- Conditions globales
- Tâches de migration
- Images du système d'exploitation
- Packages d'installation du système d'exploitation
- Packages
- Requêtes
- Sites
- Règles de contrôle de logiciel
- Groupes de mises à jour logicielles
- Packages de mises à jour logicielles
- Packages de séquence de tâches
- Éléments et packages des paramètres de l'appareil Windows CE

Certains objets ne peuvent pas être ajoutés aux étendues de sécurité, car ils ne sont sécurisés que par les rôles de sécurité. L'accès administratif à ces objets ne peut pas être limité à un sous-ensemble des objets disponibles. Par exemple, vous pouvez être un utilisateur administratif et créer des groupes de limites qui sont utilisés pour un site spécifique. Comme l'objet de la limite ne prend pas en charge les étendues de sécurité, vous ne pouvez pas attribuer à cet utilisateur une étendue de sécurité ne lui accordant que l'accès aux limites qui pourraient être associées à ce site. Comme l'objet de la limite ne peut pas être associé à une étendue de sécurité, lorsque vous attribuez un rôle de sécurité qui comprend l'accès aux objets de la limite à un utilisateur, celui-ci peut accéder à toutes les limites de la hiérarchie.

Parmi les objets qui ne sont pas limités par des étendues de sécurité, on compte les objets suivants :

- Forêts Active Directory
- Utilisateurs administratifs

- Alertes
- Stratégies anti-programme malveillant
- Limites
- Associations d'ordinateurs
- Paramètres client par défaut
- Modèles de déploiement
- Pilotes d'appareils
- Connecteur Exchange Server
- Mappages de site à site de migration
- Profil d'inscription d'appareil mobile
- Rôles de sécurité
- Étendues de sécurité
- Adresses de site
- Rôles système de site
- Titres des logiciels
- Mises à jour logicielles
- Messages d'état
- Affinités des appareils d'utilisateur

Créez des étendues de sécurité lorsque vous devez limiter l'accès à des instances d'objets distinctes. Par exemple :

- Vous disposez d'un groupe d'utilisateurs administratifs qui doit être capable de consulter les applications de production, mais pas les applications de test. Créer une étendue de sécurité pour les applications de production et une autre pour les applications de test.
- Différents utilisateurs administratifs nécessitent différents accès pour certaines instances d'un type d'objet. Par exemple, un groupe d'utilisateurs administratifs requiert l'autorisation Lire pour des groupes de mises à jour logicielles spécifiques et un autre groupe d'utilisateurs administratifs requiert les autorisations Modifier et Supprimer pour d'autres groupes de mises à jour logicielles. Créez différentes étendues de sécurité pour ces groupes de mises à jour logicielles.

Pour plus d'informations sur la façon de configurer des étendues de sécurité pour l'administration basée sur des rôles, consultez Configurer des étendues de sécurité pour un objet dans la rubrique Configurer l'administration basée sur des rôles pour System Center Configuration Manager.

# Présentation de Long-Term Servicing Branch dans System Center Configuration Manager

22/06/2018 • 6 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Long-Term Servicing Branch)*

Long-Term Servicing Branch (LTSB) de System Center Configuration Manager est une branche distincte de Configuration Manager, conçue comme une option d'installation disponible pour tous les clients. Mais elle n'est pas la seule option proposée aux clients qui ont laissé expirer leur Software Assurance (SA) ou leurs droits d'abonnement équivalents pour Configuration Manager.

À partir de Configuration Manager version 1606, LTSB offre moins de fonctionnalités que la branche actuelle de Configuration Manager.

> **TIP**
> Si vous recherchez des informations sur les branches de **Windows Server**, consultez Nouvelle option de maintenance Current Branch for Business Windows Server 2016.

## Fonctionnalités non disponibles dans la branche LTSB de Configuration Manager

La branche actuelle de Configuration Manager prend en charge les fonctionnalités suivantes, qui ne sont pas disponibles lorsque vous utilisez LTSB :

- Des mises à jour dans la console qui ajoutent de nouvelles fonctionnalités et améliorations.
- Prise en charge des derniers systèmes d'exploitation à utiliser comme clients et serveurs sur site.
- Utilisez un abonnement Microsoft Intune pour prendre en charge :
  - Intune dans une configuration hybride de gestion des appareils mobiles
  - Gestion des appareils mobiles locale
- Le tableau de bord et les plans de maintenance de Windows 10, y compris la prise en charge des dernières versions de la branche CB (Current Branch) et de la branche CBB (Current Branch for Business) de Windows 10.
- Prise en charge des futures versions de Windows Server et Windows 10 LTSB
- Asset Intelligence
- Points de distribution cloud
- Exchange Online en tant que connecteur Exchange

Bien que la prise en charge de ces fonctionnalités ne soit pas disponible dans LTSB, certaines restent visibles dans la console Configuration Manager, mais ne peuvent pas être sélectionnées ou utilisées.

## Rechercher de la documentation sur LTSB

LTSB est basé sur la version 1606 de Current Branch. Pour obtenir une documentation sur le produit, utilisez la documentation Current Branch, avec les mises en garde et limitations propres à LTSB. Ces mises en garde et limitations sont identifiées dans les rubriques en ligne suivantes :

- Présentation de Long-Term Servicing Branch : (cette rubrique)

- Installation de Long-Term Servicing Branch
- Mettre à niveau Long-Term Servicing Branch vers Current Branch
- Configurations prises en charge pour Long-Term Servicing Branch
- Gérer Long-Term Servicing Branch dans Configuration Manager

Lorsque vous référencez la documentation Current Branch pour LTSB, les détails qui s'appliquent à la version 1606 s'appliquent également à LTSB. Les fonctionnalités ou les détails introduits avec la version 1610 ou version ultérieure ne sont pas pris en charge par LTSB.

## Vue d'ensemble des licences pour LTSB

Les clients qui ont un contrat Software Assurance (SA) sur les licences de System Center Configuration Manager ou qui ont des droits d'abonnement équivalents à la date du 1er octobre 2016 ont le droit d'utiliser la version 1606 d'octobre 2016 de System Center Configuration Manager. Les clients qui ont des droits pour System Center Configuration Manager au 1er octobre 2016 ou après cette date ont deux options de licence lors de l'installation : CB (Current Branch) et LTSB (Long-Term Servicing Branch).

Les clients dotés de droits perpétuels sur System Center Configuration Manager, ou qui laissent leur contrat SA ou leur abonnement expirer après le 1er octobre, peuvent installer la version LTSB de System Center Configuration Manager qui est en vigueur au moment de l'expiration.

Les conditions générales des produits que vous achetez par le biais des programmes de licence en volume Microsoft se trouvent ici.

Consultez Licences et branches pour System Center Configuration Manager afin d'obtenir plus d'informations sur les options de licence pour les branches Configuration Manager.

## Étapes suivantes

Si vous décidez que Configuration Manager LTSB est la branche correcte pour votre environnement, installez un nouveau site LTSB dans le cadre d'une nouvelle hiérarchie, ou mettez à niveau un site System Center 2012 Configuration Manager et une hiérarchie.

Si vous n'avez pas de support d'installation, consultez la documentation de System Center 2016 pour plus d'informations sur l'obtention de System Center 2016, qui inclut le support vous permettant d'installer System Center Configuration Manager LTSB.

# Configurations prises en charge pour la branche Long-Term Servicing Branch de System Center Configuration Manager

22/06/2018 • 24 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Long-Term Servicing Branch)*

Utilisez les informations de cette rubrique pour découvrir les systèmes d'exploitation et dépendances de produits pris en charge par la branche Long-Term Servicing Branch (LTSB) de Configuration Manager. Sauf indication contraire dans cette rubrique (ou les rubriques spécifiques à LTSB), les configurations et limitations qui s'appliquent à la branche Current Branch version 1606 s'appliquent également à la branche LTSB. En cas de conflits, utilisez les informations qui s'appliquent à l'édition dont vous vous servez. En règle générale, LTSB est plus limité que Current Branch.

## Informations générales sur la prise en charge

Les produits et technologies suivants sont pris en charge par cette branche de Configuration Manager. En revanche, leur inclusion dans ce contenu ne signifie pas une extension de prise en charge des produits ou versions au-delà de leur cycle de vie individuel. L'utilisation de produits qui ont dépassé leur cycle de vie n'est pas prise en charge avec Configuration Manager. Pour plus d'informations, visitez le site web Politique de support Microsoft et lisez la page Politique de support Microsoft - FAQ.

En outre, les produits et versions de produits non répertoriés dans les rubriques suivantes ne sont pas pris en charge, sauf s'ils ont été annoncés dans le Blog Enterprise Mobility + Security.

**Limitations de la prise en charge future :** LTSB offre une prise en charge limitée pour les futures versions des systèmes d'exploitation client/serveur et dépendances de produits. La liste des plateformes pour LTSB est fixée pour la durée de vie de la version :

**Windows :**

- Seules les mises à jour de qualité et de sécurité pour Windows sont prises en charge.
- Aucune prise en charge n'est ajoutée pour les branches CB (Current Branch), CBB (Current Branch For Business) ou LTSB de Windows 10.
- Aucune prise en charge n'est ajoutée pour les nouvelles versions majeures de Windows Server.

**SQL Server :**

- Seules les mises à jour de qualité et de sécurité, ou les mises à niveau mineures comme les Service Packs, sont prises en charge pour SQL Server.
- Aucune prise en charge n'est ajoutée pour les nouvelles versions majeures de SQL Server.

## Systèmes et serveurs de site

LTSB prend en charge l'utilisation des systèmes d'exploitation Windows suivants comme systèmes de site. Chaque système d'exploitation a les mêmes exigences et limitations que l'entrée correspondante dans Systèmes d'exploitation pris en charge pour les serveurs de système de site. Par exemple, l'installation minimale de Windows 2012 R2 doit être une version x64, elle est prise en charge uniquement pour l'hébergement d'un point de distribution et elle ne prend pas en charge PXE ou la multidiffusion.

**Systèmes d'exploitation pris en charge :**

- Windows Server 2016
- Windows Server 2012 R2 (x64) : Standard, Datacenter
- Windows Server 2012 (x64) : Standard, Datacenter
- Windows Server 2008 R2 avec SP1 (x64) : Standard, Entreprise, Datacenter
- Windows Server 2008 avec SP2 (x86, x64) : Standard, Enterprise, Datacenter *(voir la remarque 1)*
- Windows 10 Entreprise 2015 LTSB (x86, x64)
- Windows 10 Entreprise 2016 LTSB (x86, x64)
- Windows 8.1 (x86, x64) : Professionnel, Entreprise
- Windows 7 avec SP1 (x86, x64) : Professionnel, Entreprise, Édition Intégrale
- Installation minimale de Windows Server 2012
- Installation minimale de Windows Server 2012 R2

*Remarque 1* : Ce système d'exploitation n'est pas pris en charge pour les serveurs de site ou les rôles de système de site, à l'exception du point de distribution et du point de distribution d'extraction. Vous pouvez continuer à utiliser ce système d'exploitation comme point de distribution jusqu'à l'annonce de la dépréciation de ce support ou jusqu'à l'expiration du support étendu de ce système d'exploitation. Pour plus d'informations, consultez Échec de l'installation de System Center Configuration Manager CB et LTSB sur Windows Server 2008.

## Gestion des clients

Les sections suivantes identifient les systèmes d'exploitation clients que vous pouvez gérer à l'aide de LTSB. LTSB ne prend pas en charge l'ajout de nouveaux systèmes d'exploitation comme clients pris en charge.

**Ordinateurs Windows**

Vous pouvez utiliser LTSB pour gérer les systèmes d'exploitation Windows suivants avec le logiciel client Configuration Manager inclus dans Configuration Manager. Pour plus d'informations, consultez Guide pratique pour déployer des clients sur des ordinateurs Windows dans System Center Configuration Manager.

**Systèmes d'exploitation pris en charge :**

- Windows Server 2016
- Windows Server 2012 R2 (x64) : Standard, Datacenter (Remarque 1)
- Windows Server 2012 (x64) : Standard, Datacenter (Remarque 1)
- Windows Storage Server 2012 R2 (x64)
- Windows Storage Server 2012 (x64)
- Windows Server 2008 R2 avec SP1 (x64) : Standard, Enterprise, Datacenter (Remarque 1)
- Windows Storage Server 2008 R2 (x86, x64) : Workgroup, Standard, Enterprise
- Windows Server 2008 avec SP2 (x86, x64) : Standard, Enterprise, Datacenter (Remarque 1)
- Windows 10 Entreprise 2015 LTSB (x86, x64)
- Windows 10 Entreprise 2016 LTSB (x86, x64)
- Windows 8.1 (x86, x64) : Professionnel, Entreprise
- Windows 7 avec SP1 (x86, x64) : Professionnel, Entreprise, Édition Intégrale
- Installation minimale de Windows Server 2012 R2 (x64) (Remarque 2)
- Installation minimale de Windows Server 2012 (x64) (Remarque 2)
- Installation minimale de Windows Server 2008 R2 SP1 (x64)
- Installation minimale de Windows Server 2008 SP2 (x86, x64)

**(Remarque 1)** Les versions de Datacenter sont prises en charge mais ne sont pas certifiées pour Configuration Manager.

**(Remarque 2)** Pour prendre en charge l'installation Push du client, l'ordinateur exécutant cette version du système d'exploitation doit exécuter le service de rôle Serveur de fichiers pour le rôle serveur Services de fichiers et de stockage. Pour plus d'informations sur l'installation des fonctionnalités Windows sur un ordinateur Server Core, consultez Installer des rôles et fonctionnalités de serveur sur un serveur en mode d'installation minimale dans la bibliothèque TechNet de Windows Server 2012.

**Windows Embedded**

Vous pouvez utiliser LTSB pour gérer les appareils Windows Embedded suivants en installant le logiciel client sur l'appareil. Pour plus d'informations, consultez Planification du déploiement de clients sur des appareils Windows Embedded dans System Center Configuration Manager.

**Configuration requise et limitations :**

- Toutes les fonctionnalités du client sont prises en charges sur les systèmes Windows Embedded pris en charge qui ne disposent pas de filtres d'écriture activés.
- Les clients qui utilisent l'un des éléments suivants sont pris en charge pour toutes les fonctionnalités, à l'exception de la gestion de l'alimentation :
  - Filtres d'écriture améliorés (EWF)
  - Filtres d'écriture basés sur des fichiers RAM (FBWF)
  - Filtres d'écriture unifiés (UWF)
- Le catalogue des applications n'est pris en charge pour aucun appareil Windows Embedded.
- Avant de pouvoir surveiller les programmes malveillants détectés sur les appareils Windows Embedded basés sur Windows XP, vous devez installer le package de script Microsoft Windows WMI sur les appareils intégrés. Utilisez Windows Embedded Target Designer pour installer ce package. Les fichiers *WBEMDISP.DLL* et *WBEMDISP.TLB* doivent exister et être inscrits dans le dossier %windir%\System32\WBEM sur l'appareil Windows Embedded pour garantir que les programmes malveillants sont signalés.

**Systèmes d'exploitation pris en charge :**

- Windows 10 Entreprise 2016 LTSB (x86, x64)
- Windows 10 Entreprise 2015 LTSB (x86, x64)
- Windows Embedded 8.1 Industry (x86, x64)
- Windows Thin PC (x86, x64)
- Windows Embedded POSReady 7 (x86, x64)
- Windows Embedded Standard 7 avec SP1 (x86, x64)
- Windows Embedded POSReady 2009 (x86)
- Windows Embedded Standard 2009 (x86)

**Windows CE**

Vous pouvez gérer les appareils Windows CE avec le client hérité d'appareil mobile Configuration Manager inclus dans Configuration Manager.

**Configuration requise et limitations :**

- L'installation du client d'appareil mobile nécessite 0,78 Mo d'espace de stockage. La connexion sur l'appareil mobile peut nécessiter jusqu'à 256 Ko d'espace de stockage supplémentaire.
- Les fonctionnalités de ces appareils mobiles varient selon la plateforme et le type de client. Pour plus d'informations sur le type des fonctions de gestion que Configuration Manager prend en charge pour un client hérité d'appareil mobile, consultez Choisir une solution de gestion d'appareils pour System Center

Configuration Manager.

**Systèmes d'exploitation pris en charge :**

- Windows CE 7.0 (processeurs ARM et x86)

**Langues prises en charge :**

- Chinois (simplifié et traditionnel)
- Anglais (États-Unis)
- Français (France)
- Allemand
- Italien
- Japonais
- Coréen
- Portugais (Brésil)
- Russe
- Espagnol (Espagne)

**Ordinateurs Mac**

Vous pouvez utiliser LTSB pour gérer les ordinateurs Mac OS X avec le client Configuration Manager pour Mac.

Le package d'installation de client Mac n'est pas fourni avec le support d'installation de Configuration Manager. Vous pouvez le télécharger en même temps que les « clients pour d'autres systèmes d'exploitation » à partir du Centre de téléchargement Microsoft.

La prise en charge des systèmes d'exploitation Mac est limitée à ceux qui sont répertoriés dans cette section. Elle n'inclut pas d'autres systèmes d'exploitation pouvant être pris en charge par une mise à jour future des packages d'installation de client Mac pour Current Branch.

Pour plus d'informations, consultez Guide pratique pour déployer des clients sur des ordinateurs Mac dans System Center Configuration Manager.

**Versions prises en charge :**

- Mac OS X 10.9 (Mavericks)
- Mac OS X 10.10 (Yosemite)
- Mac OS X 10.11 (El Capitan)

## Serveurs Linux et UNIX

Vous pouvez utiliser LTSB pour gérer les serveurs Linux et UNIX avec le client Configuration Manager pour Linux et UNIX.

Les packages d'installation du client Linux et UNIX ne sont pas fournis avec le média Configuration Manager. Vous pouvez les télécharger en même temps que les « clients pour d'autres systèmes d'exploitation » à partir du Centre de téléchargement Microsoft. En plus des packages d'installation du client, le client inclut le script d'installation qui gère l'installation du client sur chaque ordinateur.

La prise en charge des systèmes d'exploitation Linux et UNIX est limitée à ceux qui sont répertoriés dans cette section. Elle n'inclut pas d'autres systèmes d'exploitation pouvant être pris en charge par une mise à jour future des packages de client Linux et UNIX pour Current Branch.

**Configuration requise et limitations :**

- Pour vérifier les dépendances des fichiers du système d'exploitation pour le client pour Linux et UNIX, consultez Conditions préalables pour le déploiement du client pour les serveurs Linux et UNIX.

- Pour une vue d'ensemble des fonctionnalités de gestion prises en charge pour les ordinateurs exécutant Linux ou UNIX, consultez Guide pratique pour déployer des clients sur des serveurs UNIX et Linux dans System Center Configuration Manager.
- Pour versions prises en charge de Linux et UNIX, la version répertoriée inclut toutes les versions mineures suivantes. Par exemple, quand la prise en charge est indiquée pour CentOS version 6, elle inclut également toute version mineure suivante de CentOS 6, telle CentOS 6.3. De même, quand la prise en charge est indiquée pour un système d'exploitation utilisant des Service Packs, comme SUSE Linux Enterprise Server 11 SP1, elle inclut les Service Packs suivants pour cette version du système d'exploitation.
- Pour plus d'informations sur les packages d'installation client et l'agent universel, consultez Guide pratique pour déployer des clients sur des serveurs UNIX et Linux dans System Center Configuration Manager.

**Versions prises en charge :**
Les versions suivantes sont prises en charge à l'aide du fichier .tar indiqué.

### AIX

| VERSION | FICHIER |
|---|---|
| Version 5.3 (Power) | ccm-Aix53ppc.<version>.tar |
| Version 6.1 (Power) | ccm-Aix61ppc.<version>.tar |
| Version 7.1 (Power) | ccm-Aix71ppc.<version>.tar |

### CentOS

| VERSION | FICHIER |
|---|---|
| Version 5 x86 | ccm-Universalx86.<version>.tar |
| Version 5 x64 | ccm-Universalx64.<version>.tar |
| Version 6 x86 | ccm-Universalx86.<version>.tar |
| Version 6 x64 | ccm-Universalx64.<version>.tar |
| Version 7 x64 | ccm-Universalx64.<version>.tar |

### Debian

| VERSION | FICHIER |
|---|---|
| Version 5 x86 | ccm-Universalx86.<version>.tar |
| Version 5 x64 | ccm-Universalx64.<version>.tar |
| Version 6 x86 | ccm-Universalx86.<version>.tar |
| Version 6 x64 | ccm-Universalx64.<version>.tar |
| Version 7 x86 | ccm-Universalx86.<version>.tar |
| Version 7 x64 | ccm-Universalx64.<version>.tar |

| VERSION | FICHIER |
| --- | --- |
| Version 8 x86 | ccm-Universalx86.<version>.tar |
| Version 8 x64 | ccm-Universalx64.<version>.tar |

### HP-UX

| VERSION | FICHIER |
| --- | --- |
| Version 11iv2 IA64 | ccm-HpuxB.11.23i64.<version>.tar |
| Version 11iv2 PA-RISC | ccm-HpuxB.11.23PA.<version>.tar |
| Version 11iv3 IA64 | ccm-HpuxB.11.31i64.<version>.tar |
| Version 11iv3 PA-RISC | ccm-HpuxB.11.31PA.<version>.tar |

### Oracle Linux

| VERSION | FICHIER |
| --- | --- |
| Version 5 x86 | ccm-Universalx86.<version>.tar |
| Version 5 x64 | ccm-Universalx64.<version>.tar |
| Version 6 x86 | ccm-Universalx86.<version>.tar |
| Version 6 x64 | ccm-Universalx64.<version>.tar |
| Version 7 x64 | ccm-Universalx64.<version>.tar |

### Red Hat Enterprise Linux (RHEL)

| VERSION | FICHIER |
| --- | --- |
| Version 4 x86 | ccm-RHEL4x86.<version>.tar |
| Version 4 x64 | ccm-RHEL4x64.<version>.tar |
| Version 5 x86 | ccm-Universalx86.<version>.tar |
| Version 5 x64 | ccm-Universalx64.<version>.tar |
| Version 6 x86 | ccm-Universalx86.<version>.tar |
| Version 6 x64 | ccm-Universalx64.<version>.tar |
| Version 7 x64 | ccm-Universalx64.<version>.tar |

### Solaris

| VERSION | FICHIER |
| --- | --- |
| SPARC version 9 | ccm-Sol9sparc.<version>.tar |
| Version 10 x86 | ccm-Sol10x86.<version>.tar |
| SPARC version 10 | ccm-Sol10sparc.<version>.tar |
| Version 11 x86 | ccm-Sol11x86.<version>.tar |
| SPARC version 11 | ccm-Sol11sparc.<version>.tar |

### SUSE Linux Enterprise Server (SLES)

| VERSION | FICHIER |
| --- | --- |
| Version 9 x86 | ccm-SLES9x86.<version>.tar |
| Version 10 SP1 x86 | ccm-Universalx86.<version>.tar |
| Version 10 SP1 x64 | ccm-Universalx64.<version>.tar |
| Version 11 SP1 x86 | ccm-Universalx86.<version>.tar |
| Version 11 SP1 x64 | ccm-Universalx64.<version>.tar |
| Version 12 x64 | ccm-Universalx64.<version>.tar |

### Ubuntu

| VERSION | FICHIER |
| --- | --- |
| Version 10.04 LTS x86 | ccm-Universalx86.<version>.tar |
| Version 10.04 LTS x64 | ccm-Universalx64.<version>.tar |
| Version 12.04 LTS x86 | ccm-Universalx86.<version>.tar |
| Version 12.04 LTS x64 | ccm-Universalx64.<version>.tar |
| Version 14.04 LTS x86 | ccm-Universalx86.<version>.tar |
| Version 14.04 LTS x64 | ccm-Universalx64.<version>.tar |

### Connecteur Exchange Server

LTSB prend en charge une gestion limitée des appareils qui se connectent à votre instance Exchange Server, sans installation d'un logiciel client. Pour plus d'informations, consultez Gérer les appareils mobiles avec System Center Configuration Manager et Exchange.

### Configuration requise et limitations :

- Configuration Manager permet une gestion limitée des appareils mobiles. La gestion limitée est disponible quand vous utilisez le connecteur du serveur Exchange Server pour les appareils compatibles EAS (Exchange Active Sync) qui se connectent à un serveur exécutant Exchange Server ou Exchange Online.

- Pour plus d'informations sur les fonctions de gestion que Configuration Manager prend en charge pour les appareils mobiles gérés par le connecteur du serveur Exchange Server, consultez Choisir une solution de gestion d'appareils pour System Center Configuration Manager.

**Versions d'Exchange Server prises en charge** :

- Exchange Server 2010 SP1
- Exchange Server 2010 SP2
- Exchange Server 2013

> **NOTE**
> LTSB ne prend pas en charge la gestion des appareils qui se connectent via un service en ligne, comme Exchange Online (Office 365).

## Console Configuration Manager

LTSB prend en charge les systèmes d'exploitation suivants pour l'exécution de la console Configuration Manager. Chaque ordinateur qui héberge la console doit avoir au minimum .NET Framework version 4.5.2, sauf pour Windows 10, qui nécessite au minimum .NET Framework 4.6.

**Systèmes d'exploitation pris en charge :**

- Windows Server 2016
- Windows Server 2012 R2 (x64) : Standard, Datacenter
- Windows Server 2012 (x64) : Standard, Datacenter
- Windows Server 2008 R2 avec SP1 (x64) : Standard, Entreprise, Datacenter
- Windows Server 2008 avec SP2 (x86, x64) : Standard, Entreprise, Datacenter
- Windows 10 Entreprise 2016 LTSB (x86, x64)
- Windows 10 Entreprise 2015 LTSB (x86, x64)
- Windows 8.1 (x86, x64) : Professionnel, Entreprise
- Windows 7 avec SP1 (x86, x64) : Professionnel, Entreprise, Édition Intégrale

## Versions de SQL Server prises en charge pour la base de données du site et le point de rapport

LTSB prend en charge les versions suivantes de SQL Server pour héberger la base de données du site et le point de rapport. Pour chaque version prise en charge, les mêmes exigences et limitations de configuration apparaissant dans Prise en charge des versions de SQL Server pour Current Branch s'appliquent à LTSB. Cela inclut l'utilisation d'un cluster SQL Server ou d'un groupe de disponibilité AlwaysOn SQL Server.

**Versions prises en charge :**

- SQL Server 2016 : Standard, Enterprise
- SQL Server 2014 SP2 : Standard, Enterprise
- SQL Server 2014 SP1 : Standard, Enterprise
- SQL Server 2012 SP3 : Standard, Enterprise
- SQL Server 2008 R2 SP3 : Standard, Enterprise, Datacenter
- SQL Server 2016 Express
- SQL Server 2014 Express SP2
- SQL Server 2014 Express SP1
- SQL Server 2012 Express SP3

## Prise en charge des domaines Active Directory

Tous les systèmes de site LTSB doivent être membres d'un domaine Windows Active Directory pris en charge. La prise en charge des domaines Active Directory présente les mêmes exigences et limitations que celles décrites dans Prise en charge des domaines Active Directory. Toutefois, elle se limite aux niveaux fonctionnels de domaine suivants :

**Niveaux pris en charge :**

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

## Rubriques de prise en charge supplémentaires qui s'appliquent à Long-Term Servicing Branch

Les informations contenues dans les rubriques Current Branch suivantes s'appliquent à LTSB :

- Taille et échelle en chiffres
- Prérequis des sites et systèmes de site
- Options de haute disponibilité
- Matériel recommandé
- Prise en charge des fonctionnalités et réseaux Windows
- Prise en charge des environnements de virtualisation

# Installer et mettre à niveau avec le support de la base de référence de la version 1606 pour System Center Configuration Manager

22/06/2018 • 15 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch), (Long-Term Servicing Branch)*

Lorsque vous exécutez le programme d'installation à partir du support de la base de référence 1606 pour Configuration Manager, vous pouvez installer Long-Term Servicing Branch ou à un site Current Branch de System Center Configuration Manager.

Le support de la base de référence est disponible sous forme de DVD dans le cadre de Microsoft System Center 2016 ou de System Center Configuration Manager (Current Branch et Long-Term Servicing Branch 1606). Pour en savoir plus sur le support de la base de référence, consultez Versions de base et de mise à jour.

Quand vous utilisez le média de la base de référence de la version 1606, le site que vous installez (ou vers lequel vous effectuez la mise à niveau) est le suivant :

- Un *site Current Branch* qui équivaut à un site initialement installé à l'aide du média de la base de référence 1511, puis mis à jour vers la version 1606 plus le correctif cumulatif 1606 (KB3186654).
- Un *site LTSB* qui équivaut au site Current Branch exécutant la version 1606 plus le correctif cumulatif 1606 (KB3186654). Le média de la base de référence contient déjà le correctif cumulatif. Toutefois, le site LTSB ne prend pas en charge toutes les fonctionnalités disponibles avec Current Branch, comme cela est indiqué dans Présentation de Long-Term Servicing Branch dans System Center Configuration Manager.

Si vous ne connaissez pas déjà les différentes branches de System Center Configuration Manager, consultez Déterminer la branche de Configuration manager à utiliser.

## Modifications apportées au programme d'installation avec le support de la base de référence 1606

Le support de la base de référence 1606 inclut les modifications suivantes dans l'installation de Configuration Manager.

**Branche et édition**

Quand vous exécutez le programme d'installation, une page dédiée à la gestion des licences vous est proposée, où vous pouvez sélectionner la branche de Configuration Manager à installer. Vous pouvez choisir une installation sous licence Current Branch ou LTSB, ou une version d'évaluation de Current Branch dans le cadre d'une installation sans licence.

Pour plus d'informations, consultez Licences et branches pour System Center Configuration Manager.

**Expiration de Software Assurance**

Pendant l'installation, vous avez la possibilité d'entrer la valeur de la **date d'expiration de Software Assurance**. Il s'agit d'une valeur facultative que vous pouvez spécifier pour des raisons pratiques.

> **NOTE**
> Microsoft ne valide pas la date d'expiration que vous entrez et ne l'utilise pas pour la validation de la licence. Vous pouvez ainsi l'utiliser en guise de rappel de votre date d'expiration. Ce rappel est pratique, car Configuration Manager vérifie régulièrement les nouvelles mises à jour logicielles proposées en ligne, et l'état de votre licence Software Assurance doit être actualisé pour être éligible à ces mises à jour supplémentaires.

- Vous pouvez spécifier cette valeur de date dans la page **Clé de produit** de l'Assistant Installation quand vous exécutez le programme d'installation à partir du média de la base de référence de la version 1606 de System Center Configuration Manager.
- Vous pouvez également spécifier cette date en sélectionnant **Propriétés des paramètres de hiérarchie** > **Licences** dans la console Configuration Manager.

Pour plus d'informations, consultez « Contrats Software Assurance » dans Licences et branches pour System Center Configuration Manager.

**Autres configurations préalables à la mise à niveau**

Avant de démarrer une mise à niveau de System Center 2012 Configuration Manager vers LTSB, vous devez exécuter les étapes supplémentaires suivantes dans le cadre de la liste de contrôle préalable à la mise à niveau. Désinstallez les rôles de système de site que LTSB ne prend pas en charge :

- Point de synchronisation Asset Intelligence
- Connecteur Microsoft Intune
- Points de distribution cloud

Pour plus d'informations, consultez Mettre à niveau vers System Center Configuration Manager.

**Nouvelles options d'installation par script**

Le média de la base de référence de la version 1606 prend en charge une nouvelle clé de fichier de script sans assistance pour les installations par script d'un nouveau site de niveau supérieur. Elle s'applique à l'installation d'un nouveau site principal autonome ou à l'ajout d'un site d'administration centrale dans le cadre d'un scénario de développement de site.

Quand vous utilisez un script sans assistance pour installer une branche sous licence, vous devez ajouter la section, les noms de clés et les valeurs ci-dessous dans la section Options de votre script. Vous n'avez pas besoin d'utiliser ces valeurs pour l'installation par script d'une version d'évaluation de Current Branch :

**SABranchOptions**

- **Nom de clé : SAActive**
  - Valeurs : 0 ou 1.
  - Détails : 0 installe une édition d'évaluation sans licence de Current Branch et 1 installe une édition sous licence.
- **CurrentBranch**
  - Valeurs : 0 ou 1.
  - Détails : 0 installe Long-Term Servicing Branch et 1 installe Current Branch.

Par exemple, pour installer une édition de Current Branch sous licence, vous utiliseriez :

**Nom de clé : SABranchOptions**

- **SSActive = 1**
- **CurrentBranch = 1**

> **IMPORTANT**
>
> **SABranchOptions** ne fonctionne qu'avec le programme d'installation à partir du support de la base de référence. Cette option ne s'applique pas quand vous exécutez le programme d'installation à partir du dossier CD.Latest d'un site vous avez précédemment installé à l'aide du support de la base de référence de la version 1606.
>
> **SABranchOptions** ne s'applique pas aux mises à niveau par script de System Center 2012 Configuration Manager et donne toujours Current Branch.

Pour plus d'informations, consultez Utiliser une ligne de commande pour installer des sites System Center Configuration Manager.

## Installer un nouveau site

Quand vous utilisez le support de la base de référence 1606 pour installer un nouveau site de l'une des deux branches, utilisez les procédures de planification, préparation et installation de sites décrites dans la rubrique Installation de sites System Center Configuration Manager en tenant également compte des points suivants :

- Pendant l'installation, vous devez choisir la branche de Configuration Manager à installer et vous pouvez spécifier les détails de votre contrat Software Assurance.
- Tous les sites d'une même hiérarchie doivent exécuter la même branche. Une hiérarchie ne peut pas comporter un mélange de LTSB et Current Branch sur des sites différents.
- Nouvelle installation par script. Pour plus d'informations, consultez « Nouvelles options d'installation par script », plus haut dans cet article.

## Étendre un site principal autonome

Vous pouvez développer un site principal autonome qui exécute LTSB. Le processus n'est pas différent de celui utilisé pour un site Current Branch avec tout de même une particularité :

- Quand vous installez le nouveau site d'administration centrale, vous devez utiliser le programme d'installation disponible à partir du support de source d'installation d'origine que vous avez utilisé pour installer le site LTSB. L'exécution du programme d'installation à partir du dossier CD.Latest n'est pas prise en charge pour ce scénario.

Pour plus d'informations sur l'extension d'un site, consultez « Étendre un site principal autonome » dans Installer un site à l'aide de l'Assistant Installation.

## Mettre à niveau à partir de System Center 2012 Configuration Manager

Quand vous effectuez une mise à niveau à partir de System Center 2012 Configuration Manager, utilisez les procédures de planification, de préparation et d'installation de site décrites dans la rubrique Mettre à niveau vers System Center Configuration Manager, en tenant compte des changements suivants :

**Mise à niveau vers Current Branch :**

- Pendant l'installation, vous devez choisir Current Branch et vous pouvez spécifier les détails de votre contrat Software Assurance.
- Nouvelle installation par script. Pour plus d'informations, consultez « Nouvelles options d'installation par script », plus haut dans cet article.

**Mise à niveau vers LTSB :**

- Autres étapes à suivre incluses dans la liste de vérification préalable à la mise à niveau.
- Pendant l'installation, vous devez choisir la branche LTSB et vous pouvez spécifier les détails de votre contrat

Software Assurance.

- Vous pouvez uniquement mettre à niveau un site qui exécute System Center 2012 Configuration Manager avec Service Pack 1 ou Service Pack 2, ou System Center 2012 R2 Configuration Manager avec Service Pack 1 ou sans Service Pack.

**Chemins de mise à niveau sur place pour le support de la base de référence 1606**

Vous pouvez utiliser le support de la base de référence 1606 pour mettre à niveau les produits suivants vers une édition sous licence de System Center Configuration Manager :

- System Center 2012 R2 Configuration Manager avec Service Pack 1
- System Center 2012 R2 Configuration Manager sans service Pack (requiert l'utilisation de médias de référence pour la version 1606 republiée le 15 décembre 2016)
- System Center 2012 Configuration Manager avec Service Pack 2
- System Center 2012 Configuration Manager avec Service Pack 1 (utilisation exigée du support de base de référence pour la version 1606 qui a été republiée le 15 décembre 2016)

Vous pouvez également utiliser ce support pour mettre à niveau une édition d'évaluation sans licence de Current Branch vers une version sous licence complète de Current Branch.

Ce média ne prend pas en charge la mise à niveau des produits suivants :

- Autres versions de System Center 2012 Configuration Manager.
- Configuration Manager 2007 ou version antérieure.
- Une installation de la version RC de System Center Configuration Manager.

## À propos du dossier CD.Latest et de LTSB

Voici les limitations relatives à l'utilisation du média que Configuration Manager crée dans le dossier CD.Latest sur le serveur de site. Ces limitations s'appliquent aux sites qui exécutent LTSB :

Le média fourni dans le dossier CD.Latest est pris en charge pour les opérations suivantes :

- Récupération de site.
- Maintenance de site.
- Installation de sites principaux enfants supplémentaires.

Le support inclus dans le dossier CD.Latest n'est pas pris en charge pour les éléments suivants :

- Installation d'un site d'administration centrale dans le cadre d'un scénario de développement de site

Pour plus d'informations, consultez Dossier CD.Latest.

## Sauvegarde, récupération et maintenance de site pour LTSB

Pour sauvegarder ou récupérer un site qui exécute LTSB, ou en effectuer la maintenance, suivez les instructions et procédures décrites dans Sauvegarde et récupération pour System Center Configuration Manager.

Utilisez le programme d'installation de Configuration Manager à partir du dossier CD.Latest de la sauvegarde de votre site LTSB.

# Gérer Long-Term Servicing Branch dans Configuration Manager

22/06/2018 • 5 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Long-Term Servicing Branch)*

Lorsque vous utilisez Long-Term Servicing Branch (LTSB) dans System Center Configuration Manager, les éléments suivants peuvent vous aider à comprendre les importantes modifications qui affectent la façon dont vous gérez votre infrastructure.

Étant donné que LTSB équivaut à la version 1606 de Current Branch (avec quelques exceptions comme l'intégration d'Intune et certaines fonctionnalités cloud), la plupart des tâches que vous utilisez pour la planification, le déploiement, la configuration et la gestion quotidienne sont identiques.

Par exemple, LTSB prend en charge les mêmes nombre de sites, types de site, clients et infrastructure générale que Current Branch. Ainsi, vous utilisez les instructions figurant dans les rubriques sur la planification et la conception de sites et de hiérarchies pour Current Branch. De même, pour les fonctionnalités LTSB prises en charge par les deux branches, comme les mises à jour logicielles ou le déploiement de système d'exploitation, utilisez les instructions figurant dans les sections de la documentation Current Branch en tenant compte des mises en garde liées au non-accès aux modifications de fonctionnalités introduites après la version 1606 de Current Branch.

Les sections suivantes fournissent des informations sur la gestion de tâches qui ne sont pas similaires.

## Mises à jour et maintenance

Seules les mises à jour de sécurité critiques sont disponibles en tant que mises à jour dans la console dans LTSB.

Les informations sur les mises à jour régulières des versions Current Branch ultérieures sont visibles dans la console, mais elles ne sont pas disponibles dans LTSB. Elles ne sont pas téléchargées et ne peuvent pas être installées.

Pour prendre en charge les mises à jour dans la console pour les correctifs de sécurité critiques, un site LTSB a besoin d'utiliser le point de connexion de service. Vous pouvez configurer ce rôle de système de site en mode hors connexion ou en ligne, comme pour Current Branch. LTSB collecte et envoie les mêmes données de télémétrie et d'utilisation que Current Branch.

LTSB prend en charge l'utilisation du programme d'installation de correctif logiciel et de l'outil Inscription de la mise à jour, comme indiqué pour Current Branch.

Pour obtenir des informations générales sur les mises à jour et la maintenance, consultez Mises à jour pour Configuration Manager.

## Modifications liées au développement de site et au dossier CD.Latest

Quand vous exécutez LTSB et que vous développez un site principal autonome en installant un nouveau site d'administration centrale, vous devez utiliser le programme d'installation et les fichiers sources du support de la base de référence de la version 1606. Pour Current Branch, vous exécutez le programme d'installation et vous utilisez les fichiers sources du dossier CD.Latest.

Bien que vous n'exécutiez pas le programme d'installation pour le développement de site à partir du dossier CD.Latest, vous continuez d'utiliser ce dossier pour la récupération de site et pour installer un nouveau site principal enfant si votre premier site LTSB était un site d'administration centrale.

Pour plus d'informations sur le développement d'un site, consultez Développement d'un site principal autonome. Pour plus d'informations sur le dossier CD.Latest, consultez Dossier CD.Latest.

## Récupération

Lorsque vous récupérez un site, vous devez restaurer le site ou la base de données de site dans sa branche d'origine. Vous ne pouvez pas récupérer une base de données de site Current Branch sur une installation LTSB, et vice versa.

# Mettre à niveau Long-Term Servicing Branch vers Current Branch

22/06/2018 • 4 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Long-Term Servicing Branch)*

Cette rubrique est destinée à vous apprendre à mettre à niveau (convertir) un site et une hiérarchie qui exécutent une installation Long-Term Servicing Branch (LTSB) de Configuration Manager vers la version Current Branch.

Si vous avez souscrit un contrat Software Assurance (ou des droits de licence similaires) qui vous donnent le droit d'utiliser Current Branch, vous pouvez convertir votre installation LTSB en version Current Branch. Il s'agit d'une conversion unidirectionnelle, car la conversion d'un site Current Branch en LTSB n'est pas prise en charge.

Si vous avez plusieurs sites, il vous suffit de convertir le site de niveau supérieur de votre hiérarchie. Dès lors que le site de niveau supérieur est converti :

- les sites principaux enfants sont convertis automatiquement ;
- vous devez procéder à une mise à jour manuelle des sites secondaires dans la console Configuration Manager.

## Exécuter le programme d'installation pour convertir Long-Term Servicing Branch

Sur le site de niveau supérieur de votre hiérarchie, vous pouvez exécuter le programme d'installation de Configuration Manager à partir du media de base de référence éligible et sélectionner **Maintenance de site**. Ensuite, une fois dans la page de licence, sélectionnez l'option Current Branch, puis terminez l'Assistant.

Une fois votre site converti en version Current Branch, vous avez accès à des fonctions et fonctionnalités qui n'étaient pas disponibles auparavant.

> **NOTE**
> Le média de ligne de base éligible est un média qui contient une version équivalente ou postérieure à votre installation LTSB.

Par exemple, sachant que LTSB est basé sur la version 1606, vous ne pouvez pas utiliser le média de ligne de base 1511 pour une conversion vers Current Branch. Vous devez exécuter le programme d'installation du média de base de référence de la version 1606 dont vous vous êtes servi pour installer le site LTSB, puis choisir l'option de licence correspondant à Current Branch. Autrement, si une base de référence ultérieure de Current Branch a été publiée, vous pouvez exécuter le programme d'installation à partir de ce média de base de référence.

Pour obtenir la liste des versions de ligne de base, consultez **Versions de base et de mise à jour** dans Mises à jour pour Configuration Manager.

## Utiliser la console Configuration Manager pour convertir Long-Term Servicing Branch

Si votre site s'exécute LTSB, vous pouvez utiliser l'option suivante dans la console Configuration Manager pour convertir Current Branch :

1. Dans la console, accédez à **Administration** > **Configuration du site** > **Sites**, puis ouvrez **Paramètres de hiérarchie**.

2. Sélectionnez l'option de conversion vers Current Branch, puis choisissez **Appliquer**.

Une fois votre site converti en version Current Branch, vous avez accès à des fonctions et fonctionnalités qui n'étaient pas disponibles auparavant.

# Quelle branche de Configuration Manager dois-je utiliser ?

10/07/2018 • 18 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch, Long-Term Servicing Branch et Technical Preview)*

Il existe trois branches pour System Center Configuration Manager : Current Branch, Long-Term Servicing Branch et Technical Preview. Utilisez cette rubrique pour mieux choisir la branche qui vous convient.

> **TIP**
> Tous les sites d'une hiérarchie doivent exécuter la même branche. Il est impossible de prendre en charge une hiérarchie avec des branches différentes sur des sites distincts.

## Current Branch

Cette branche est concédée sous licence pour une utilisation dans un environnement de production. Utilisez cette branche pour obtenir les dernières fonctionnalités. Si vous avez l'une des licences suivantes, vous pouvez utiliser cette branche :

- System Center Datacenter
- System Center Standard
- System Center Configuration Manager
- Droits d'abonnement équivalents

Pour plus d'informations sur la Software Assurance et les options de licence, consultez Licences et branches pour System Center Configuration Manager, ainsi que Questions fréquentes (FAQ) sur les branches et la gestion des licences de Configuration Manager.

Microsoft prévoit de publier des mises à jour de System Center Configuration Manager Current Branch plusieurs fois par an. Pour les versions de Configuration Manager publiées avant la version 1710, la prise en charge dure 12 mois. À compter de la version 1710, chaque version de mise à jour reste prise en charge pendant 18 mois suivant sa date de disponibilité générale (GA). Un support technique est assuré pendant toute la période de prise en charge. Toutefois, notre structure de prise en charge est dynamique et évolue en deux phases de maintenance distinctes qui dépendent de la disponibilité de la dernière version Current Branch. (Pour plus d'informations, consultez la rubrique intitulée Prise en charge des versions Current Branch de System Center Configuration Manager. Les mises à jour vers des versions plus récentes sont proposées sous forme de mises à jour dans la console.

Pour installer Current Branch en tant que nouveau site, utilisez le support de la base de référence. Utilisez également le support de la base de référence pour mettre à niveau System Center 2012 Configuration Manager avec Service Pack 2, ou System Center 2012 R2 Configuration Manager avec Service Pack 1. L'accès à ce support dépend de la manière dont votre organisation a acquis la licence de System Center Configuration Manager.

Vous pouvez également utiliser le support de la base de référence pour installer un nouveau site en tant qu'édition d'évaluation de Current Branch. L'édition d'évaluation ne nécessite aucune licence. Vous pouvez utiliser l'édition d'évaluation pendant 180 jours. Elle prend en charge la mise à niveau vers une édition sous licence de Current Branch. Pour installer uniquement une édition d'évaluation, accédez au site TechNet Evaluation Center.

> **NOTE**
>
> Utilisez uniquement le média de référence pour installer des sites pour une nouvelle hiérarchie Configuration Manager. Si vous avez installé une version de base de référence, utilisez les mises à jour dans la console pour mettre à jour vos sites vers une nouvelle version.
>
> Les sites mis à jour à l'aide de mises à jour dans la console sont équivalents au nouveau site installé à l'aide du média de référence.
>
> Pour plus d'informations, consultez Mises à jour pour System Center Configuration Manager.

**Fonctionnalités de la branche Current Branch**

- Elle reçoit des mises à jour dans la console qui mettent à votre disposition de nouvelles fonctionnalités.
- Elle reçoit des mises à jour dans la console qui offrent des correctifs de sécurité et de qualité aux fonctionnalités existantes.
- Elle prend en charge les mises à jour hors bande lorsque cela est nécessaire. Pour plus d'informations, consultez Utiliser l'outil Inscription de la mise à jour ou Utiliser le programme d'installation de correctif logiciel.
- Elle s'intègre à Microsoft Intune et d'autres services cloud.
- Elle prend en charge la migration des données vers et à partir d'autres installations de Configuration Manager.
- Elle prend en charge la mise à niveau à partir de versions précédentes de Configuration Manager.
- Elle prend en charge l'installation en tant qu'édition d'évaluation, à partir de laquelle vous pourrez ultérieurement effectuer une mise à niveau vers une installation sous licence.

La version 1511 était la version initiale de Current Branch. Les mises à jour ultérieures incluent les versions 1602, 1606, etc. Chaque version est prise en charge pendant un an et Microsoft vous recommande d'effectuer la mise à jour vers la dernière version peu après sa publication. Vous pouvez attendre jusqu'à une année avant d'effectuer la mise à jour vers une version plus récente et vous pouvez également ignorer une mise à jour pour installer la dernière version disponible. Dans la mesure où chaque version est cumulative, si vous ignorez une mise à jour et installez la version la plus récente, vous bénéficiez tout de même de l'ensemble des fonctionnalités et améliorations apportées par les versions précédentes.

Pour plus d'informations, consultez Prise en charge des versions Current Branch.

**Options de mise à jour**

- Avec la Software Assurance active, vous pouvez installer des mises à jour dans la console pour les versions Current Branch.
- Il n'existe aucune option permettant de convertir Current Branch en Technical Preview. Les branches Technical Preview sont des installations distinctes qui ne nécessitent pas de licence.
- Il n'existe aucune option permettant de convertir Current Branch en LTSB (Long-Term Servicing Branch). Vous devez désinstaller Current Branch, puis installer LTSB en tant que nouvelle installation.

## Long-Term Servicing Branch

Il s'agit d'une branche sous licence à utiliser en production pour les clients Configuration Manager qui utilisent Current Branch et ont autorisé Configuration Manager SA (Software Assurance) ou des droits d'abonnement équivalents à expirer après le 1er octobre 2016. Pour plus d'informations sur la Software Assurance et les options de licence, consultez Licences et branches pour System Center Configuration Manager, ainsi que Questions fréquentes (FAQ) sur les branches et la gestion des licences de Configuration Manager.

La branche LTSB est basée sur la version 1606. Cette branche ne reçoit pas les mises à jour dans la console, qui fournissent de nouvelles fonctionnalités ou mettent à jour des fonctionnalités existantes. Toutefois, des correctifs de sécurité critiques sont fournis. Pour installer la branche LTSB, vous devez utiliser le support de la base de référence de la version 1606 fourni avec System Center 2016. Les versions de base de référence ultérieures ne

prennent pas en charge l'installation de LTSB.

Pour installer la branche LTSB en tant que nouveau site ou en tant que mise à niveau d'un site Configuration Manager 2012 pris en charge, utilisez le support de la base de référence de la version 1606 fourni avec System Center 2016. Vous pouvez utiliser le support de la base de référence pour installer un nouveau site qui exécute la version 1606 de Current Branch, ou un nouveau site qui exécute Long-Term Servicing Branch.

> **TIP**
> Pour en savoir plus sur System Center 2016, consultez la documentation de System Center 2016. Cette documentation indique également comment obtenir System Center 2016, qui requiert un contrat de licence Microsoft ou des droits similaires.
>
> Pour trouver la version 1606 de System Center Configuration Manager dans le VLSC (Centre de gestion des licences en volume), accédez à l'onglet **Téléchargements et clés** du VLSC, recherchez `System Center 2016`, puis sélectionnez **System Center 2016 Datacenter** ou **System Center 2016 Standard**.
>
> Vous pouvez également obtenir une version d'évaluation de System Center 2016 à partir du site TechNet Evaluation Center.

**Fonctionnalités de la branche LTSB**

- Elle reçoit des mises à jour dans la console qui fournissent des correctifs de sécurité critiques.
- Elle fournit une option d'installation lorsque votre contrat SA ou vos droits équivalents sur Configuration Manager ont expiré.
- Elle prend en charge la mise à niveau (conversion) vers Current Branch quand vous avez un contrat SA ou des droits équivalents sur Configuration Manager.

**Limitations**

La branche LTSB est basée sur la version 1606 de Current Branch et présente les limitations suivantes :

- Vous bénéficiez pendant 10 ans de mises à jour de sécurité critiques pour LTSB après sa disponibilité générale (octobre 2016), après quoi la prise en charge de cette branche expire. Pour plus d'informations sur la politique de support, consultez la page Politique de support Microsoft.
- Elle prend en charge une liste limitée de systèmes d'exploitation serveur et client et les technologies associées, telles que les versions de SQL Server. Pour plus d'informations sur ce qui est pris en charge avec cette branche, consultez Configurations prises en charge pour Long-Term Servicing Branch.
- Elle ne reçoit pas de mises à jour pour les nouvelles fonctionnalités.
- Elle ne prend pas en charge fonctionnalités suivantes :
  - Ajout d'un abonnement Microsoft Intune, ce qui vous empêche d'utiliser :
    - Intune dans une configuration de gestion des appareils mobiles hybride ;
    - Gestion des appareils mobiles locale
  - Tableau de bord de maintenance de Windows 10, plans de maintenance ou canal semi-annuel Windows 10
  - Versions futures de Windows 10 LTSB et Windows Server
  - Asset Intelligence
  - Points de distribution cloud
  - Exchange Online en tant que connecteur Exchange
  - Fonctionnalités de préversion

**Options de mise à jour**

- Vous pouvez convertir votre installation LTSB en installation Current Branch. La conversion en On-premises MDM est prise en charge avant ou après l'expiration du support de la branche LTSB.

  Pour effectuer la conversion, vous devez disposer d'un contrat Software Assurance actif avec Microsoft.

Pour plus d'informations, suivez les liens ci-dessous :

- Mettre à niveau Long-Term Servicing Branch vers Current Branch
- Licences et branches pour System Center Configuration Manager
- Versions de base et de mise à jour

- Il n'existe aucune option permettant de convertir LTSB en branche Technical Preview. Les branches Technical Preview sont des installations distinctes qui ne nécessitent pas de licence.
- Vous ne pouvez pas mettre à niveau une édition d'évaluation de Current Branch vers une installation LTSB.

## Branche Technical Preview

La branche Technical Preview est destinée à un environnement lab. Découvrez et testez les dernières fonctionnalités développées pour Configuration Manager. Il n'est pas pris en charge dans un environnement de production et ne nécessite pas de contrat de licence Software Assurance.

Pour installer un nouveau site qui exécute la branche Technical Preview, utilisez le dernier support de la base de référence pour la branche Technical Preview. Une fois que vous avez installé la branche Technical Preview, de nouvelles versions sont disponibles chaque mois sous forme de mises à jour dans la console.

**Fonctionnalités de la branche Technical Preview**

- Elle est basée sur les versions de base de référence récentes de Current Branch
- Elle reçoit des mises à jour dans la console pour mettre à jour votre installation vers la dernière version de la branche Technical Preview
- Elle inclut de nouvelles fonctionnalités en cours de développement, pour lesquelles Microsoft souhaite recevoir vos commentaires
- Elle reçoit des mises à jour qui s'appliquent uniquement à la branche Technical Preview

**Limitations**

- La prise en charge est limitée, avec seulement un site principal et jusqu'à 10 clients.
- Elle ne peut pas être mise à niveau vers une branche Current Branch ou LTSB.
- Elle ne prend pas en charge les comportements suivants :
  - Utilisation de la migration pour importer ou exporter des données vers une autre installation de Configuration Manager
  - Mise à niveau à partir d'une version antérieure de Configuration Manager
  - Installation en tant qu'édition d'évaluation

Les fonctionnalités introduites initialement dans une branche Technical Preview sont souvent ajoutées à Current Branch au cours d'une mise à jour ultérieure. Chaque nouvelle version de branche Technical Preview inclut les fonctionnalités des branches Technical Preview précédentes, même après l'ajout de ces fonctionnalités à Current Branch.

Pour plus d'informations, consultez Technical Preview pour System Center Configuration Manager.

**Options de mise à jour**

- Vous pouvez installer n'importe quelle mise à jour dans la console pour une nouvelle version de branche Technical Preview.
- Il n'existe aucune option permettant de convertir une branche Technical Preview en branche Current Branch ou LTSB.

## Identifier votre version et votre branche

**Version**

Pour vérifier la version de votre site, en haut à gauche de la console, accédez à **À propos de System Center**

**Configuration Manager**. Cette boîte de dialogue affiche la **version du site**. Pour obtenir la liste des versions de site, consultez Versions de base et de mise à jour.

**Branche**

Pour vérifier la branche de votre site, dans la console, accédez à **Administration** > **Configuration du site** > **Sites**, puis ouvrez **Paramètres de hiérarchie**. Si vous voyez une option de conversion en Current Branch et si elle est active, cela signifie que le site exécute la version LTSB. Quand le site exécute Current Branch, cette option est grisée.

Pour plus d'informations sur les différentes versions de Configuration Manager, consultez Versions de base et de mise à jour.

# Configuration Manager et Windows as a Service

10/07/2018 • 4 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

System Center Configuration Manager offre un contrôle total sur les mises à jour des fonctionnalités de Windows 10. Pour adopter le modèle Windows as a service dans son entier, vous devez également adopter le modèle Configuration Manager Current Branch. Pour rester à jour avec Windows 10, vous devez rester à jour avec Configuration Manager pour une expérience optimale. En effet, vous devez disposer des nouvelles versions de Configuration Manager pour profiter pleinement des nouvelles fonctionnalités d'entreprise de Windows 10. Cet article est destiné à être une page d'accueil d'articles phares que vous devez consulter pour adopter Configuration Manager Current Branch. Configuration Manager Current Branch vous mène tout droit à Windows as a service.

## Articles importants sur l'adoption de Configuration Manager Current Branch

| ARTICLE | DESCRIPTION |
|---|---|
| Vue d'ensemble de Configuration Manager Current Branch | Fournit un bref résumé des points clés du nouveau modèle de maintenance pour Configuration Manager (Current Branch) |
| Cycle de vie du support | Explique le nouveau modèle de support et de maintenance. |
| Éléments supprimés et dépréciés | Annonce les changements à venir qui pourraient affecter votre utilisation de Configuration Manager. |
| Mises à jour vers Configuration Manager Current Branch | Explique la méthode simple pour appliquer des mises à jour de fonctionnalités à Configuration Manager dans la console. |
| Obtenir les mises à jour disponibles | Explique les deux modes disponibles pour obtenir les mises à jour de fonctionnalités de Configuration Manager. |
| Liste de contrôle des mises à jour | Fournit des listes de contrôle spécifiques aux versions des mises à jour (le cas échéant). |
| Installer les nouvelles mises à jour de fonctionnalités de Configuration Manager | Explique la procédure d'installation simple pour les mises à jour de fonctionnalités. |
| Prise en charge pour Windows 10 | Fournit une matrice de la prise en charge des versions de Windows 10 (et d'ADK). |
| Technical Preview pour Configuration Manager | Fournit des informations sur le programme d'évaluation technique de ConfigMgr. |

## Rubriques importantes sur l'adoption de Windows as a service

| ARTICLE | DESCRIPTION |
|---|---|
| Gérer Windows en tant que service | Explique comment utiliser des plans de maintenance pour déployer des mises à jour de fonctionnalités de Windows 10. |

| ARTICLE | DESCRIPTION |
| --- | --- |
| Mettre à niveau Windows 10 via une séquence de tâches | Détails de la création d'une séquence de tâches pour mettre à niveau Windows 10 avec des recommandations supplémentaires. |
| Déploiements par phases | Les déploiements par phases automatisent le lancement coordonné et séquencé d'une séquence de tâches sur plusieurs regroupements. |
| Optimiser la distribution des mises à jour Windows 10 | Utilisez Configuration Manager pour gérer le contenu de mise à jour pour rester à jour avec Windows 10. |
| Intégrer avec Upgrade Readiness | Upgrade Readiness vous permet d'évaluer et d'analyser l'état de préparation des appareils de votre environnement en vue d'une mise à niveau vers Windows 10. |
| Intégration de Windows Update pour Entreprise (facultatif) | Explique comment définir et déployer des stratégies Windows Update pour Entreprise avec Configuration Manager. |
| Utiliser la cogestion avec Microsoft Intune et Windows Update pour Entreprise (facultatif) | Fournit une vue d'ensemble de la cogestion. |

## Articles connexes

- Mise à niveau sur place avec System Center Configuration Manager (Current Branch) à partir de ConfigMgr 2012
- Planifier la migration vers System Center Configuration Manager (Current Branch) à partir de ConfigMgr 2007

# Utiliser le logiciel client Gestionnaire de configuration pour l'interopérabilité étendue avec les futures versions d'un site Current Branch

22/06/2018 • 5 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les exigences de l'entreprise risquent de ne pas vous autoriser à mettre à jour régulièrement le client Configuration Manager sur certains appareils. Par exemple, vous devrez peut-être respecter des stratégies de gestion des changements ; de même, l'appareil peut être critique pour la mission. Contournez-les en installant un nouveau client pour une utilisation à long terme, appelé client d'interopérabilité étendue (EIC). Utilisez le client EIC uniquement sur des appareils spécifiques qui ne peuvent pas être mis à jour fréquemment, comme des bornes ou des appareils de point de vente. Continuez à utiliser la mise à niveau automatique des clients sur la plupart de vos clients.

## Fonctionnement du scénario

En règle générale, quand vous installez une nouvelle mise à jour dans la console pour Configuration Manager, les clients mettent automatiquement à jour leur logiciel client pour pouvoir utiliser ces nouvelles fonctionnalités. Avec ce scénario, vous effectuez quand même la mise à jour vers la branche CB qui reçoit les nouvelles fonctionnalités et mises à jour. La plupart des appareils mettent à jour le logiciel client Configuration Manager avec chaque mise à jour de version que vous installez. Toutefois, sur un sous-ensemble de systèmes critiques qui ne doivent pas recevoir les mises à jour du logiciel client, vous installez le client d'interopérabilité étendue. Ces clients n'installent pas de nouveau logiciel client tant que vous n'y avez pas explicitement déployé de nouvelle version du logiciel client.

## Versions prises en charge

Le tableau suivant liste les versions du client Configuration Manager qui sont prises en charge pour ce scénario :

| VERSION | DATE DE DISPONIBILITÉ | DATE DE FIN DU SUPPORT |
|---|---|---|
| 1802<br>5.00.8634 | 1er mai 2018 | Pas avant le 1er mai 2020 |
| 1606<br>5.00.8412 | 18 novembre 2016 | 1er mai 2019 |

**TIP**

Le client EIC est pris en charge pendant au moins deux ans à partir de la date de sortie. Pour plus d'informations sur les dates de sortie, consultez Prise en charge des versions Current Branch de System Center Configuration Manager).

Envisagez de mettre à jour le client d'interopérabilité étendue sur les appareils que vous gérez avec Current Branch avant que la prise en charge du client n'arrive à expiration. Pour cela, téléchargez une nouvelle version du client auprès de Microsoft, puis déployez ce logiciel client mis à jour sur vos appareils qui utilisent le client d'interopérabilité étendue actuel.

## Utilisation du client d'interopérabilité étendue

1. Obtenez une version prise en charge du client EIC dans le dossier `\SMSSETUP\Client` du support d'installation des mises à jour de Configuration Manager. Veillez à copier tout le contenu du dossier.
2. Installez manuellement le client d'interopérabilité étendue sur ces appareils. Pour plus d'informations, consultez Installer manuellement le client.

   > **IMPORTANT**
   > Lors de la mise à niveau des clients de la version 1606 vers la version 1802, utilisez l'option CCMSETUP **/AlwaysExcludeUpgrade:True**. Sinon, le client risque de recevoir la stratégie du point de gestion pour être automatiquement mis à niveau avant la stratégie d'exclusion.

3. Ajoutez ces appareils dans une collection et excluez cette collection des mises à niveau automatiques du client. Pour plus d'informations, consultez Utiliser la mise à niveau automatique du client.

> **TIP**
> Pour rechercher le support Configuration Manager dans le Centre de gestion des licences en volume (VLSC), accédez à l'onglet **Téléchargements et clés**, recherchez `System Center Config`, puis sélectionnez **System Center Config Mgr (current branch)**.

## Limitations du client d'interopérabilité étendue

- Les mises à jour du logiciel client d'interopérabilité étendue ne sont pas disponibles par le biais des mises à jour dans la console. Pour plus d'informations sur la façon de mettre à jour les clients EIC, consultez Comment utiliser le client EIC.
- Le client EIC prend uniquement en charge les fonctionnalités suivantes :
  - Mises à jour logicielles
  - Inventaire matériel et logiciel
  - Packages et programmes

## Étapes suivantes

Pour vérifier que les clients sont installés correctement sur les appareils que vous souhaitez, consultez Guide pratique pour surveiller les clients.

# Licences et branches pour System Center Configuration Manager

12/06/2018 • 12 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch), (Long-Term Servicing Branch)*

Utilisez cette rubrique pour en savoir plus sur les conditions de licence pour les options d'installation disponibles avec la version Release d'octobre 2016 de System Center Configuration Manager version 1606. Ces options d'installation incluent Current Branch version 1606, Long-Term Servicing Branch (LTSB) et l'installation d'évaluation de Current Branch version 1606.

**Vue d'ensemble des licences :**
Les clients dotés d'un contrat Software Assurance (SA) sur les licences de System Center Configuration Manager ou dotés de droits d'abonnement équivalents à compter du 1er octobre 2016 ont le droit d'utiliser la version 1606 d'octobre 2016 de System Center Configuration Manager. Les clients dotés de droits pour System Center Configuration Manager au 1er octobre 2016 ou après se voient proposer deux options de licence lors de l'installation : CB (Current Branch) et LTSB (Long-Term Servicing Branch).

**Spécificités des licences :**
Les conditions générales des produits que vous achetez par le biais des programmes de licence en volume Microsoft se trouvent ici.

## Branches sous licence de System Center Configuration Manager

Cette rubrique fait référence au contrat Software Assurance (ou à des droits d'abonnement équivalents) qui correspond aux contrats de licence Microsoft qui octroient des droits d'installation et d'utilisation de Configuration Manager.

| BRANCHE | LICENCES | DÉTAILS |
|---|---|---|
| Current Branch | Requiert un contrat Software Assurance actif (ou des droits équivalents) pour Configuration Manager.<br>Consultez Software Assurance et Current Branch dans cette rubrique. | Prise en charge dans les environnements de production qui veulent recevoir des mises à jour de fonctionnalités et qualitatives régulières de Microsoft.<br>Cette branche donne accès à l'utilisation de toutes les fonctionnalités et améliorations.<br><br>Pour les versions de Configuration Manager publiées avant la version 1710, la prise en charge dure 12 mois. À compter de la version 1710, chaque version de mise à jour reste prise en charge pendant 18 mois suivant sa date de disponibilité générale. Pour plus d'informations, consultez Prise en charge des versions Current Branch de System Center Configuration Manager. |

| BRANCHE | LICENCES | DÉTAILS |
| --- | --- | --- |
| Long-Term Servicing Branch (LTSB) | Requiert un contrat Software Assurance actif avec Microsoft au moment de la publication (1er octobre 2016).<br>Consultez Software Assurance et LTSB dans cette rubrique. | Prise en charge dans les environnements de production. Utilisation prévue pour les clients qui ont laissé leur contrat Software Assurance (SA) ou leurs droits d'abonnement équivalents pour Configuration Manager expirer après le 1er octobre 2016.<br>Cette branche est limitée par rapport à Current Branch.<br><br>Les mises à jour de sécurité critiques pour Configuration Manager sont disponibles pour cette branche, mais aucune nouvelle fonctionnalité n'est disponible. |
| Installation d'évaluation de Current Branch | Ne requiert pas de contrat Software Assurance avec Microsoft. | Une installation d'évaluation correspond toujours à Current Branch et est utilisable pendant 180 jours. L'installation d'évaluation peut être mise à niveau vers une installation complète de Current Branch. Vous ne pouvez pas mettre à niveau une installation d'évaluation vers Long-Term Servicing Branch. |

En plus de Current Branch, LTSB et l'installation d'évaluation de Current Branch, une préversion technique de System Center Configuration Manager est également disponible. Il s'agit d'une build limitée de Configuration Manager qui vous permet d'essayer de nouvelles fonctionnalités susceptibles d'être ajoutées à Current Branch dans une prochaine mise à jour. Vous installez la préversion technique à l'aide d'un autre support que celui des versions sous licence. Pour plus d'informations, consultez la documentation de la préversion technique.

## Branches sous licence

Les clients dotés d'un contrat Software Assurance (SA) sur les licences de System Center Configuration Manager ou dotés de droits d'abonnement équivalents à compter du 1er octobre 2016 ont le droit d'utiliser la version 1606 d'octobre 2016 de System Center Configuration Manager. Les clients dotés de droits sur System Center Configuration Manager version 1606 à la date du ou après le 1er octobre 2016 se voient proposer deux options de licence lors de l'installation :

- **Current Branch**
- **Long-Term Servicing Branch (LTSB)**

Consultez le tableau de la section précédente pour plus d'informations.

## Contrats Software Assurance et System Center Configuration Manager

L'état du contrat Software Assurance sur vos licences System Center Configuration Manager ou vos droits d'abonnement équivalents, à la date du 1er octobre 2016 ou après cette date, déterminent la branche que vous pouvez installer et utiliser.

**Software Assurance et Current Branch**

Des droits d'utilisation sur System Center Configuration Manager Current Branch peuvent être octroyés par :

- **System Center :** les clients dotés d'un contrat SA actif sur des licences System Center Standard ou Datacenter peuvent installer et utiliser l'option Current Branch de System Center Configuration Manager.
- **System Center Configuration Manager :** les clients dotés d'un contrat SA actif sur des licences System Center Configuration Manager, ou dotés de droits d'abonnement équivalents, peuvent installer et utiliser l'option Current Branch de System Center Configuration Manager.

Si vous disposez d'un contrat SA actif sur des licences System Center Configuration Manager (ou des droits d'abonnement équivalents) à la date du ou après le 1er octobre 2016 :

- Vous pouvez installer et utiliser Current Branch.
- Si vous laissez votre contrat SA ou votre abonnement expirer, vous devez désinstaller Current Branch.

**Software Assurance et LTSB**

Si vous disposez d'un contrat SA actif sur des licences System Center Configuration Manager (ou des droits d'abonnement équivalents) à la date du ou après le 1er octobre 2016 :

- Vous pouvez installer et utiliser LTSB. Les clients dotés de droits perpétuels sur System Center Configuration Manager, ou qui laissent leur contrat SA ou leur abonnement expirer, peuvent installer la version LTSB de System Center Configuration Manager qui est en vigueur au moment de l'expiration.

LTSB est basé sur Current Branch version 1606 et présente les limitations suivantes :

- Il n'existe aucune prise en charge pour passer de Current Branch à LTSB. Si vous disposez actuellement d'un site Current Branch, vous devez installer LTSB en tant que nouveau site.
- LTSB ne prend pas en charge toutes les fonctionnalités de Current Branch. Les limitations sont décrites dans Présentation de Long-Term Servicing Branch et la documentation connexe. Ces limitations incluent un ensemble limité de fonctionnalités, des options de mise à niveau limitées et un cycle de vie du support produit distinct.

**Date d'expiration de Software Assurance**

À partir de la version d'octobre 2016 du support de la base de référence de la version 1606 de System Center Configuration Manager, vous pouvez spécifier la date d'expiration de votre contrat Software Assurance. La **date d'expiration de Software Assurance** est une valeur facultative que vous pouvez spécifier à titre de rappel pratique quand vous exécutez le programme d'installation de Configuration Manager ou ultérieurement à partir de la console Configuration Manager.

> **NOTE**
> Microsoft ne valide pas la date d'expiration spécifiée et ne l'utilise pas pour la validation de la licence. Vous pouvez ainsi l'utiliser en guise de rappel de votre date d'expiration. Ce rappel est pratique, car Configuration Manager vérifie régulièrement les nouvelles mises à jour logicielles proposées en ligne, et l'état de votre licence Software Assurance doit être actualisé pour être autorisé à utiliser ces mises à jour supplémentaires.

**Pour spécifier la date :**

- Quand vous exécutez le programme d'installation à partir du support de base de référence de System Center Configuration Manager version 1606, vous pouvez spécifier cette valeur dans la page **Clé de produit** de l'Assistant Installation.
- Dans la console Configuration Manager, dans **Propriétés des paramètres de hiérarchie**, vous pouvez également spécifier cette valeur sous l'onglet **Licences**.

Pour plus d'informations sur la licence Software Assurance et la branche Current Branch de System Center Configuration Manager, consultez Licences et branches pour System Center Configuration Manager.

# Ressources pour les informations de licence

Utilisez les liens suivants pour en savoir plus sur les licences de produit.

**Liens du Centre de gestion des licences en volume Microsoft (VLSC) :**

- Vue d'ensemble de VLSC : https://www.microsoft.com/en-us/Licensing/existing-customer/vlsc-training-and-resources.aspx .
- Termes des contrats de licence en volume Microsoft : http://go.microsoft.com/fwlink/?LinkId=800052.
- Les clients de licence en volume peuvent obtenir un résumé de leurs licences ici : https://www.microsoft.com/Licensing/servicecenter/default.aspx .
  Accédez au menu **Licences**, puis cliquez sur **Résumé des licences** pour obtenir une vue d'ensemble des licences.

**Vidéos VLSC :**

- Vidéos de formation sur le fonctionnement de VLSC : https://www.microsoft.com/en-us/Licensing/existing-customer/vlsc-training-and-resources.aspx#tab=2.
- Où rechercher votre contrat Software Assurance actif (à 43 secondes du début) : https://www.microsoft.com/showcase/video.aspx?uuid=fe1846cb-1d26-49fc-b064-57b25dcc31a0.
- Comment obtenir des autorisations pour VLSC : https://www.microsoft.com/showcase/video.aspx?uuid=ac4ed1ca-d0a9-43cd-89fa-74ccb555dec4. Vous pouvez déléguer des autorisations de lecture et d'écriture VLSC à d'autres personnes de votre organisation.

# Utiliser des services cloud avec System Center Configuration Manager

22/06/2018 • 8 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

System Center Configuration Manager prend en charge plusieurs options de cloud. Celles-ci peuvent compléter votre infrastructure locale et vous aider à résoudre certains problèmes d'entreprise comme :

- Gérer les appareils BYOD (en utilisant Intune pour gérer les appareils mobiles).
- Fournir des ressources de contenu à des clients isolés ou des ressources de l'intranet à l'extérieur de votre pare-feu d'entreprise (en utilisant des points de distribution cloud).
- Monter en charge l'infrastructure quand le matériel physique n'est pas disponible ou n'est pas placé de façon logique pour répondre à vos besoins (en utilisant des machines virtuelles Microsoft Azure).

La configuration de ressources cloud n'est pas indispensable avant de déployer Configuration Manager, mais il peut être utile de comprendre ces options avant d'aller plus en avant dans un plan de conception de hiérarchie. L'utilisation de ressources cloud peut vous faire gagner du temps et économiser de l'argent, mais aussi résoudre des problèmes qu'une infrastructure locale ne peut pas résoudre.

## Ressources cloud que vous pouvez utiliser avec Configuration Manager

Chaque option présente des conditions d'utilisation différentes. Vous devez donc étudier plus en détail les conditions préalables, les limitations et les coûts supplémentaires possibles selon le niveau d'utilisation pour chacune des options.

- Pour plus d'informations sur les points de distribution cloud, voir Installer des points de distribution cloud.
- Pour plus d'informations sur Azure, consultez Azure dans la bibliothèque MSDN.

**Machines virtuelles Azure (pour infrastructure cloud)**

Configuration Manager prend en charge l'utilisation d'ordinateurs qui s'exécutent en tant que machines virtuelles Azure, de la même manière que les ordinateurs qui s'exécutent localement dans votre réseau physique d'entreprise. Vous pouvez utiliser des machines virtuelles Azure dans les scénarios suivants :

- **Scénario 1** : vous pouvez exécuter Configuration Manager sur une machine virtuelle et l'utiliser pour gérer des clients installés sur d'autres machines virtuelles.
- **Scénario 2** : vous pouvez exécuter Configuration Manager sur une machine virtuelle et l'utiliser pour gérer des clients qui ne s'exécutent pas dans Azure.
- **Scénario 3** : vous pouvez exécuter différents rôles de système de site Configuration Manager sur des machines virtuelles, tout en exécutant d'autres rôles sur votre réseau physique d'entreprise (avec une connectivité réseau appropriée pour les communications).

Les exigences en matière de réseaux, de systèmes d'exploitation et de matériel qui s'appliquent à l'installation de Configuration Manager sur votre réseau physique d'entreprise s'appliquent également à l'installation de Configuration Manager dans Azure.

Un abonnement Azure est requis pour utiliser les machines virtuelles Azure. Vous occasionnez des frais en fonction du nombre et de la configuration de vos machines virtuelles, et du niveau d'utilisation des ressources cloud.

En outre, les sites et les clients Configuration Manager qui s'exécutent sur des machines virtuelles Azure sont soumis aux mêmes exigences de licence que les installations locales.

**Services Azure (pour les points de distribution cloud)**

Vous pouvez utiliser un service Azure pour héberger un point de distribution Configuration Manager, appelé point de distribution cloud. Vous pouvez utiliser un point de distribution cloud avec System Center Configuration Manager en même temps que des points de distribution locaux et des points de distribution déployés sur des machines virtuelles Azure.

Cela diffère de l'utilisation d'une machine virtuelle Azure sur laquelle vous déployez un rôle de système de site. Points de distribution cloud :

- Ils s'exécutent en tant que service dans Azure, et non sur une machine virtuelle.
- Ils sont mis automatiquement à l'échelle pour répondre à l'augmentation des demandes de contenu des clients.
- Ils prennent en charge les clients sur Internet et l'intranet.

Un abonnement Azure est requis pour utiliser Azure afin d'héberger des points de distribution. Les frais dépendent de la quantité de données qui circule vers et depuis le service.

**Microsoft Intune (pour gestion des appareils mobiles)**

Vous pouvez intégrer votre abonnement Microsoft Intune avec Configuration Manager pour permettre la gestion des appareils à l'aide du service Intune. Cette intégration présente les caractéristiques suivantes :

- Il s'agit d'une configuration hybride qui étend Configuration Manager (ou Intune selon votre perspective) pour prendre en charge une grande variété d'appareils.
- Elle requiert le rôle de système de site Connecteur Microsoft Intune.
- Elle nécessite que vous disposiez d'un abonnement Intune distinct avec des licences suffisantes pour les appareils que vous voulez gérer avec Intune.

Même si Intune utilise Azure, vous n'êtes pas tenu de configurer Azure de façon indépendante, et vous ne vous exposez pas à des coûts en supplément de ceux de l'abonnement Intune.

**Fonctionnalités supplémentaires de Configuration Manager**

Certaines fonctionnalités de Configuration Manager peuvent se connecter à des services cloud, par exemple :

- Windows Server Update Services (WSUS).
- Le service cloud Configuration Manager, pour télécharger les mises à jour de Configuration Manager.

Ces fonctions supplémentaires ne nécessitent pas d'avoir un abonnement Azure. Vous n'êtes pas tenu de configurer des connexions, des certificats ou des services spécifiques dans le cloud. En effet, ces fonctionnalités sont automatiquement gérées par Configuration Manager à votre place. Vous devez seulement veiller à ce que les systèmes de site et les appareils puissent accéder aux URL Internet.

## Sécurité des services cloud

Configuration Manager utilise des certificats pour configurer votre contenu dans Azure et y accéder, et pour gérer les services que vous utilisez. Configuration Manager chiffre les données que vous stockez dans Microsoft Azure, mais n'introduit pas de contrôles de données ou de sécurité en plus de ceux fournis par Microsoft Azure.

Pour plus d'informations, consultez les détails des différents scénarios de ressources cloud. Vous pouvez également consulter les rubriques suivantes sur la sécurité dans Azure :

- Azure : Présentation de la gestion des comptes de sécurité dans Azure

- Azure Security Overview (Présentation des fonctionnalités de sécurité Azure)
- Get Past the Security Crossroads in Your Cloud Migration (Franchir les barrières de sécurité dans le cadre d'une migration vers le cloud)
- La sécurité des données avec Azure - partie 1 sur 2

# Configuration Manager dans Azure – Forum Aux Questions

22/06/2018 • 23 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les questions et réponses suivantes peuvent vous aider à comprendre quand utiliser et comment configurer Configuration Manager dans Microsoft Azure.

## Questions générales

**Mon entreprise tente de déplacer autant de serveurs physiques que possible vers Microsoft Azure. Puis-je déplacer les serveurs Configuration Manager vers Azure ?**

Absolument, ce scénario est pris en charge. Consultez Prise en charge des environnements de virtualisation pour System Center Configuration Manager.

**Très bien ! Mon environnement requiert plusieurs sites. Tous les sites principaux enfants doivent-ils être dans Azure avec le site d'administration centrale ou locale ? Qu'en est-il des sites secondaires ?**

Les communications de site à site (réplication de base de données et basée sur les fichiers) tirent parti de la proximité de l'hébergement dans Azure. Toutefois, tout le trafic associé aux clients serait distant des serveurs de site et des systèmes de site. Si vous utilisez une connexion réseau rapide et fiable entre Azure et votre intranet avec un plan de données illimité, l'hébergement de toute votre infrastructure dans Azure est une option.

Toutefois, si vous utilisez un plan de données contrôlé et la bande passante disponible ou si le coût est un problème, ou si la connexion réseau entre Azure et votre intranet n'est pas rapide ou peut ne pas être fiable, envisagez de placer des sites spécifiques (et les systèmes de site) localement, puis d'utiliser les contrôles de bande passante intégrés dans Configuration Manager.

**Le fait d'avoir Configuration Manager dans Azure est-il un scénario SaaS (logiciel en tant que service) ?**

Non, il s'agit d'un IaaS (infrastructure en tant que service), car vous hébergez vos serveurs d'infrastructure Configuration Manager sur des machines virtuelles Azure.

**À quelles zones dois-je faire attention lorsque j'envisage un déplacement de mon infrastructure Configuration Manager vers Azure ?**

Excellente question. Voici les zones les plus importantes quand vous prenez cette décision. Chacune est explorée dans une section distincte de cette rubrique :

1. Mise en réseau
2. Disponibilité
3. Performances
4. Coût
5. Expérience utilisateur

## Mise en réseau

**Qu'en est-il de la configuration réseau requise ? Dois-je utiliser ExpressRoute ou une passerelle VPN Azure ?**

La mise en réseau est une décision très importante. Les vitesses et la latence des réseaux peuvent affecter les fonctionnalités entre le serveur de site et les systèmes de site distants, ainsi que les communications des clients vers les systèmes de site. Nous vous recommandons d'utiliser ExpressRoute. Toutefois, Configuration Manager ne présente aucune limitation pour vous empêcher d'utiliser la passerelle VPN Azure. Vous devez examiner

attentivement vos besoins (performances, correctifs, distribution de logiciels, déploiement de système d'exploitation) à partir de cette infrastructure, puis prendre votre décision. Voici quelques points à prendre en compte pour chaque solution :

- **ExpressRoute** (recommandé)
  - Extension naturelle de votre centre de données (peut relier plusieurs centres de données)
  - Connexions privées entre des centres de données Azure et votre infrastructure
  - Ne parvient pas jusqu'à l'Internet public
  - Offre une fiabilité, des vitesses élevées, une latence plus faible, une haute sécurité
  - Offre des vitesses pouvant atteindre 10 Gbits/s et des options de plan de données illimitées
- **Passerelle VPN**
  - Réseaux VPN de site à site/point à site
  - Le trafic parvient jusqu'à l'Internet public
  - Utilise la sécurité du protocole Internet (IPsec) et Internet Key Exchange (IKE)

**ExpressRoute dispose de nombreuses options différentes telles que différentes options de vitesse, illimitées et contrôlées, ainsi qu'un module complémentaire premium. Laquelle choisir ?**

Les options que vous sélectionnez dépendent du scénario que vous mettez en œuvre et du volume de données que vous envisagez de distribuer. Le transfert de données de Configuration Manager peut être contrôlé entre les serveurs de site et les points de distribution, mais la communication de serveur de site à serveur de site ne peut pas être contrôlée. Lorsque vous utilisez un plan de données contrôlé, le placement de sites spécifiques (et de systèmes de site) localement et l'utilisation de contrôles de bande passante intégrés à Configuration Manager permettent de mieux contrôler le coût d'utilisation d'Azure.

**Qu'en est-il des exigences d'installation telles que les domaines Active Directory ? Ai-je encore besoin de joindre mes serveurs de site à un domaine Active Directory ?**

Oui. Quand vous passez à Azure, les configurations prises en charge restent les mêmes, notamment les exigences d'Active Directory pour l'installation de Configuration Manager.

**Je comprends le besoin de joindre mes serveurs de site à un domaine Active Directory, mais puis-je utiliser Azure Active Directory ?**

Non, Azure Active Directory n'est pas pris en charge à ce stade. Vos serveurs de site doivent cependant être membres d'un domaine Windows Active Directory.

## Disponibilité

**L'une des raisons pour lesquelles je déplace l'infrastructure vers Azure est la promesse d'une haute disponibilité. Puis-je tirer parti des options de haute disponibilité, telles que les ensembles de disponibilité des machines virtuelles Azure, pour les machines virtuelles que j'utiliserai pour Configuration Manager ?**

Oui ! Des ensembles de disponibilité de machines virtuelles Azure peuvent être utilisés pour des rôles de système de site redondants, tels que les points de distribution ou les points de gestion.

Vous pouvez également les utiliser pour les serveurs de site Configuration Manager. Par exemple, les sites d'administration centrale et les sites principaux peuvent tous être dans le même ensemble de disponibilité, ce qui peut vous aider à vous assurer qu'ils ne sont pas redémarrés en même temps.

**Comment puis-je rendre ma base de données hautement disponible ? Puis-je utiliser Base de données SQL Azure ? Ou dois-je utiliser Microsoft SQL Server sur une machine virtuelle ?**

Vous devez utiliser Microsoft SQL Server sur une machine virtuelle. Configuration Manager ne prend pas en charge Azure SQL Server à ce stade. Mais vous pouvez utiliser des fonctionnalités telles que les groupes de disponibilité AlwaysOn pour votre serveur SQL Server. Les groupes de disponibilité AlwaysOn sont recommandés et sont officiellement pris en charge depuis la version 1602 de Configuration Manager.

**Puis-je utiliser des équilibreurs de charge Azure avec des rôles de système de site tels que les points de gestion**

**ou les points de mise à jour logicielle ?**

Configuration Manager n'a pas été testé avec les équilibreurs de charge Azure, mais si la fonctionnalité est transparente pour l'application, elle ne doit pas avoir d'effets négatifs sur les opérations normales.

## Performances

**Quels facteurs affectent les performances dans ce scénario ?**

La taille et le type des machines virtuelles Azure, les disques des machines virtuelles Azure (un stockage premium est recommandé, en particulier pour SQL Server), la latence de mise en réseau et la vitesse sont les domaines les plus importants.

**Spécifiez donc plus d'informations sur les machines virtuelles Azure ; quelle taille de machines virtuelles dois-je utiliser ?**

En règle générale, votre puissance de calcul (UC et mémoire) doit correspondre au matériel recommandé pour System Center Configuration Manager. Toutefois, il existe certaines différences entre le matériel informatique standard et les machines virtuelles Azure, notamment en ce qui concerne les disques que ces machines virtuelles utilisent. La taille des machines virtuelles que vous utilisez dépend de la taille de votre environnement. Voici quelques recommandations :

- Pour les déploiements en production d'une taille importante, nous recommandons des machines virtuelles Azure de classe « **S** ». Cela tient au fait qu'elles peuvent tirer parti des disques de stockage Premium. Les machines virtuelles de classe autre que « S » utilisent le stockage d'objets blob et, en général, ne respectent pas les exigences de performances nécessaires pour un environnement de production acceptable.
- Plusieurs disques de stockage Premium doivent être utilisés pour une échelle supérieure et agrégés par bandes dans la console Windows Disk Management pour un nombre maximal d'E/S par seconde.
- Nous vous recommandons d'utiliser de meilleurs disques premium ou plusieurs disques premium pendant votre déploiement initial de site (comme P30 à la place de P20, et 2xP30 dans un volume agrégé par bandes à la place de 1xP30). Ensuite, si votre site a besoin d'augmenter ultérieurement la taille des machines virtuelles en raison d'une charge supplémentaire, vous pouvez tirer parti de l'UC et de la mémoire supplémentaires qu'une plus grande taille de machine virtuelle fournit. Vous aurez également des disques déjà en place, susceptibles de tirer parti du débit d'E/S par seconde supplémentaire que permet la plus grande taille de machine virtuelle.

Les tableaux suivants répertorient les nombres de disques suggérés initiaux à utiliser sur les sites principaux et d'administration centrale pour des installations de différentes tailles :

**Base de données de site colocalisé** : site d'administration centrale ou site principal avec la base de données de site sur le serveur de site :

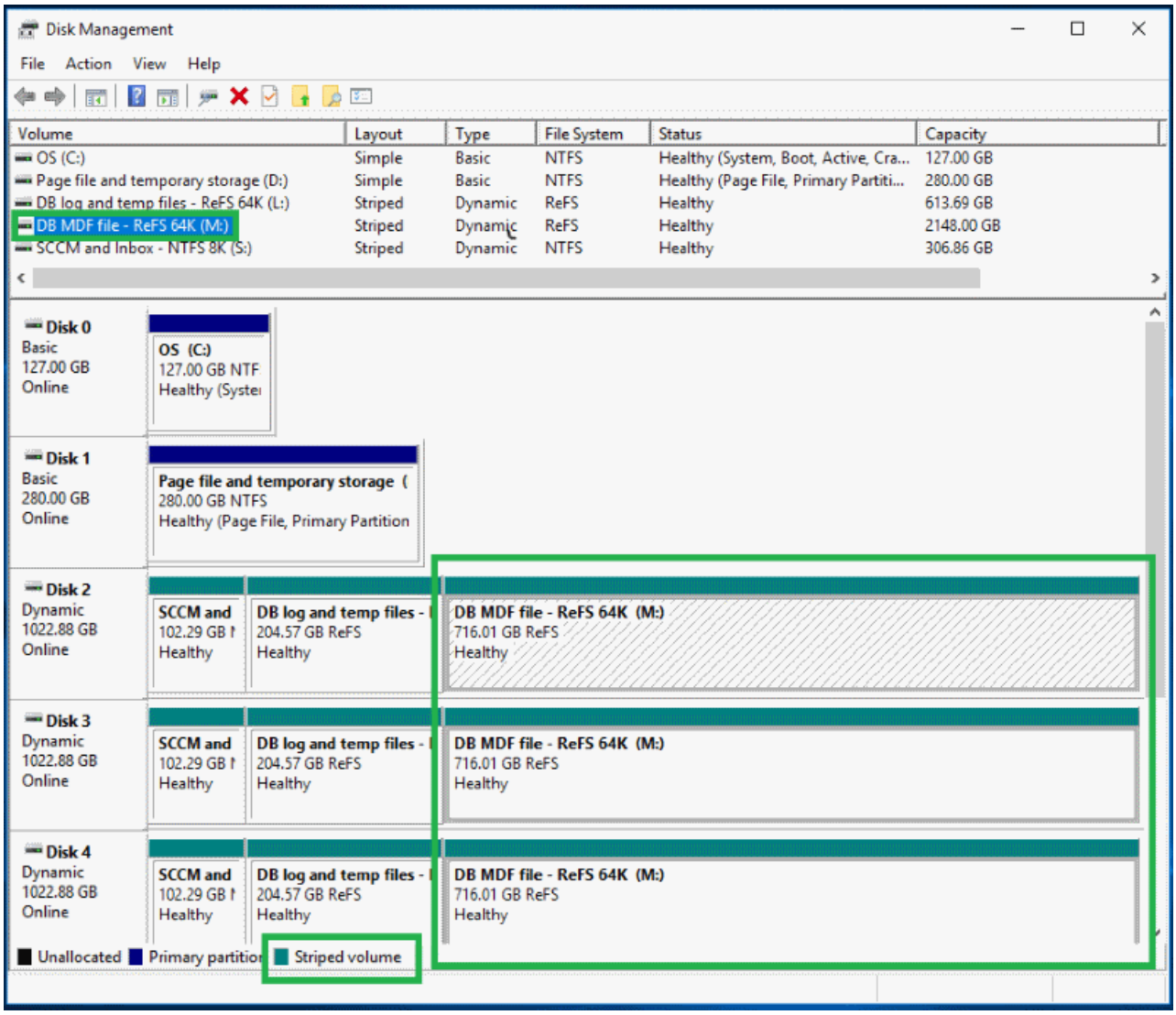
| CLIENTS BUREAU | TAILLE DE MACHINE VIRTUELLE RECOMMANDÉE | DISQUES RECOMMANDÉS |
|---|---|---|
| **Jusqu'à 25 000** | DS4_V2 | 2xP30 (agrégé par bandes) |
| **de 25 000 à 50 000** | DS13_V2 | 2xP30 (agrégé par bandes) |
| **de 50 000 à 100 000** | DS14_V2 | 3xP30 (agrégé par bandes) |

**Base de données de site distant** : site d'administration centrale ou site principal avec la base de données de site sur le serveur de site :

| CLIENTS BUREAU | TAILLE DE MACHINE VIRTUELLE RECOMMANDÉE | DISQUES RECOMMANDÉS |
|---|---|---|

| CLIENTS BUREAU | TAILLE DE MACHINE VIRTUELLE RECOMMANDÉE | DISQUES RECOMMANDÉS |
|---|---|---|
| **Jusqu'à 25 000** | Serveur de site : F4S<br>Serveur de base de données : DS12_V2 | Serveur de site : 1xP30<br>Serveur de base de données : 2xP30 (agrégé par bandes) |
| **de 25 000 à 50 000** | Serveur de site : F4S<br>Serveur de base de données : DS13_V2 | Serveur de site : 1xP30<br>Serveur de base de données : 2xP30 (agrégé par bandes) |
| **de 50 000 à 100 000** | Serveur de site : F8S<br>Serveur de base de données : DS14_V2 | Serveur de site : 2xP30 (agrégé par bandes)<br>Serveur de base de données : 3xP30 (agrégé par bandes) |

Voici un exemple de configuration pour 50 000 à 100 000 clients sur DS14_V2 avec 3 disques P30 dans un volume agrégé par bandes avec des volumes logiques distincts pour les fichiers d'installation de Configuration Manager et les fichiers de base de données :




## Expérience utilisateur

**Vous indiquez que l'expérience utilisateur est l'un des principaux domaines d'importance, pourquoi ?**

Les décisions que vous prenez quant à la mise en réseau, la disponibilité, les performances et l'emplacement où vous placez vos serveurs de site Configuration Manager peuvent directement affecter vos utilisateurs. Nous pensons qu'un déplacement vers Azure doit être transparent pour vos utilisateurs afin qu'ils ne rencontrent aucune

modification de leurs interactions quotidiennes avec Configuration Manager.

**Je comprends. J'envisage d'installer un site principal autonome unique sur une machine virtuelle Azure et je veux m'assurer que les coûts seront faibles. Dois-je placer les systèmes de site (distants) (tels que des points de gestion, des points de distribution et des points de mise à jour logicielle) sur des machines virtuelles Azure aussi ou localement ?**

À l'exception des communications depuis le serveur de site vers un point de distribution, des communications de serveur à serveur dans un site peuvent avoir lieu à tout moment et n'utilisent aucun mécanisme pour contrôler l'utilisation de la bande passante réseau. Étant donné que vous ne pouvez pas contrôler les communications entre les systèmes de site, tous les coûts associés à ces communications doivent être pris en compte.

Les vitesses et la latence des réseaux sont d'autres facteurs à prendre en compte également. Des réseaux lents et non fiables peuvent affecter les fonctionnalités entre le serveur de site et les systèmes de site distants, ainsi que les communications des clients vers les systèmes de site. Le nombre de clients managés qui utilisent un système de site donné, ainsi que les fonctionnalités que vous utilisez activement doivent également être pris en compte. En général, vous pouvez exploiter les conseils normaux en ce qui concerne les liaisons WAN et les systèmes de site, comme point de départ. Dans l'idéal, le débit réseau que vous sélectionnez et recevez entre Azure et votre intranet est cohérent avec un réseau WAN correctement connecté à un réseau rapide.

**Qu'en est-il de la distribution de contenu et de la gestion de contenu ? Les points de distribution standard doivent-ils être dans Azure ou localement, et dois-je utiliser BranchCache ou des points de distribution d'extraction localement ? Ou faut-il que j'effectue un usage exclusif des points de distribution cloud ?**

L'approche de la gestion de contenu est très similaire à celui pour les serveurs de site et les systèmes de site.

- Si vous utilisez une connexion réseau rapide et fiable entre Azure et votre intranet avec un plan de données illimité, l'hébergement de points de distribution standard dans Azure pourrait être une option.
- Si vous utilisez un plan de données contrôlé et que le coût de la bande passante est un problème ou que la connexion réseau entre Azure et votre intranet n'est pas rapide ou peut ne pas être fiable, vous pouvez envisager d'autres approches. Elles incluent le positionnement des points de distribution d'extraction ou standard localement, ainsi que l'utilisation de BranchCache. L'utilisation des points de distribution cloud est également une option, mais il existe certaines limites sur les types de contenu pris en charge (par exemple, aucune prise en charge pour les packages de mises à jour logicielles).

> **NOTE**
> Si la prise en charge PXE est requise, vous devez utiliser des points de distribution locaux (standard ou d'extraction) pour répondre aux demandes de démarrage. WDS n'est actuellement pas pris en charge pour s'exécuter sur les machines virtuelles Azure.

**Les limitations des points de distribution cloud ne me posent pas de problème, mais je ne souhaite pas placer mon point de gestion dans une zone DMZ, même si cela est nécessaire pour prendre en charge mes clients basés sur Internet. Y a-t-il d'autres options à ma disposition ?**

Oui ! Dans Configuration Manager version 1610, nous avons introduit la fonctionnalité de préversion Passerelle de gestion cloud. (Cette fonctionnalité a d'abord été proposée dans la version Technical Preview 1606 sous le nom Service de proxy cloud.)

La fonctionnalité **Passerelle de gestion cloud** fournit un moyen simple de gérer les clients Configuration Manager sur Internet. Ce service, qui est déployé sur Microsoft Azure et nécessite un abonnement Azure, se connecte à votre infrastructure Configuration Manager locale à l'aide d'un nouveau rôle appelé « point de connexion de passerelle de gestion cloud ». Après son déploiement et sa configuration, les clients peuvent accéder aux rôles de système de site Configuration Manager locaux, qu'ils soient connectés au réseau privé interne ou à Internet.

Vous pouvez commencer à utiliser la passerelle de gestion cloud dans votre environnement et nous envoyer vos commentaires pour nous aider à améliorer cette fonctionnalité. Pour plus d'informations sur les fonctionnalités de

préversions, consultez Utiliser des fonctionnalités de préversions de mises à jour.

**J'ai également entendu que vous avez introduit une nouvelle fonctionnalité, appelée Cache d'homologue, comme fonctionnalité préliminaire dans la version 1610. Est-elle différente de BranchCache ? Laquelle choisir ?**

Oui, totalement différente. La fonctionnalité Cache d'homologue est une technologie 100 % native de Configuration Manager, alors que BranchCache est une fonctionnalité de Windows. Les deux peuvent vous être utiles. BranchCache utilise une diffusion pour rechercher le contenu requis alors que le cache d'homologue utilise les paramètres de groupe de limites et de flux de travail de distribution standard de Configuration Manager.

Vous pouvez configurer n'importe quel client comme source de mise en cache d'homologue. Ensuite, lorsque les points de gestion fournissent aux clients des informations sur les emplacements sources de contenu, ils fournissent des détails sur les points de distribution et toutes les sources de mise en cache d'homologue qui disposent du contenu que le client requiert.

## Coût

**Donnez-moi des informations sur le coût. Cette solution sera-t-elle à faible coût ?**

Cela est difficile à dire puisque chaque environnement est différent. La meilleure chose à faire est d'estimer le coût de votre environnement à l'aide de la calculatrice de prix de Microsoft Azure : https://azure.microsoft.com/pricing/calculator/

## Ressources supplémentaires

**Principes de base :** http://azure.microsoft.com/documentation/articles/fundamentals-introduction-to-azure/

**Types de machines virtuelles Azure :**

- Tailles de machine virtuelle : https://azure.microsoft.com/documentation/articles/virtual-machines-size-specs/
- Prix des machines virtuelles : http://azure.microsoft.com/pricing/details/virtual-machines/
- Prix du stockage : http://azure.microsoft.com/pricing/details/storage/

**Considérations sur les performances de disque :**

- Introduction aux disques Premium : http://azure.microsoft.com/blog/2014/12/11/introducing-premium-storage-high-performance-storage-for-azure-virtual-machine-workloads/
- Informations approfondies sur les disques Premium : http://azure.microsoft.com/documentation/articles/storage-premium-storage-preview-portal/
- Collection pratique de graphiques pour les tailles maximales et les objectifs de performance du stockage : https://azure.microsoft.com/documentation/articles/storage-scalability-targets/
- Autre introduction + données utiles pour les passionnés d'informatique sur le fonctionnement du stockage Premium en coulisse : http://azure.microsoft.com/blog/2015/04/16/azure-premium-storage-now-generally-available-2/

**Disponibilité :**

- Temps de disponibilité dans les contrats SLA Azure IaaS : https://azure.microsoft.com/support/legal/sla/virtual-machines/v1_0/
- Définition des groupes à haute disponibilité : https://azure.microsoft.com/documentation/articles/virtual-machines-manage-availability/

**Connectivité :**

- ExpressRoute ou Azure VPN : http://azure.microsoft.com/blog/2014/06/10/expressroute-or-virtual-network-vpn-whats-right-for-me/
- Prix d'Express Route : http://azure.microsoft.com/pricing/details/expressroute/

- Plus sur Express Route : http://azure.microsoft.com/documentation/articles/expressroute-introduction/

# Foire aux questions sur les branches et la gestion des licences de Configuration Manager

22/06/2018 • 14 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch), System Center Configuration Manager (Long-Term Servicing Branch)*

## Résumé

Cette FAQ répond à des questions courantes sur la gestion des licences des versions System Center Configuration Manager Current Branch et Long Term Servicing Branch (LTSB), disponibles par le biais des programmes de gestion des licences en volume Microsoft. Cet article n'a qu'une fonction informative. Il ne remplace ni n'annule aucune documentation sur la gestion des licences de System Center Configuration Manager. Pour plus d'informations, consultez la gestion des licences des produits System Center 2016 et les Conditions des produits. Les Conditions des Produits décrivent les conditions d'utilisation de tous les produits Microsoft dans la gestion des licences en volume.

Pour plus d'informations sur les fonctionnalités de System Center Configuration Manager, consultez la page produit.

## FAQ sur les produits et la gestion des licences

**Qu'est-ce que Current Branch ?**

Il s'agit de la build prête pour la production de System Center Configuration Manager qui fournit un modèle de maintenance actif. Ce modèle de maintenance ressemble à l'expérience avec Windows 10 ou l'option d'installation de Windows Server 2016 Nano Server. Cette approche convient aux clients qui évoluent à une « cadence cloud » et souhaitent innover plus rapidement. Avec le modèle de maintenance Current Branch, les clients System Center Configuration Manager continuent de recevoir de nouvelles fonctionnalités. C'est pourquoi seuls les clients avec une Software Assurance active dans leurs licences System Center Configuration Manager, ou des droits d'abonnement équivalents, peuvent installer et utiliser l'option Current Branch de System Center Configuration Manager.

**Qu'est-ce que Long Term Servicing Branch (LTSB) ?**

Long-Term Servicing Branch est une version de production de System Center Configuration Manager. Elle est conçue pour les clients qui autorisent l'expiration de leur Software Assurance ou de leurs droits d'abonnements équivalents. Par rapport à Current Branch, LTSB a des fonctionnalités réduites. Les clients qui autorisent l'expiration de Software Assurance ou des droits d'abonnement équivalents doivent désinstaller Current Branch de System Center Configuration Manager. Les clients dotés de droits de licence perpétuels sur System Center Configuration Manager peuvent ensuite installer et utiliser la build LTSB de la version de System Center Configuration Manager qui est en vigueur au moment de l'expiration.

**J'ai vu les termes SA et L&SA dans le texte sur les licences. Que veulent dire ces acronymes dans System Center Configuration Manager ?**

SA (Software Assurance) et L&SA (Licence et Software Assurance) sont des options de licence qui accordent des droits d'utilisation de System Center Configuration Manager. SA est une option qui s'adresse à un client qui renouvelle la SA suite à un contrat précédent. L&SA est une option qui s'adresse à un client qui achète une nouvelle licence et la SA.

- **Software Assurance (SA)** : Les clients doivent avoir une SA active dans leurs licences System Center

Configuration Manager, ou des droits d'abonnement équivalents, pour pouvoir installer et utiliser l'option Current Branch de System Center Configuration Manager.

  - Même si la SA est facultative pour certains produits Microsoft, la seule façon d'obtenir les droits d'utiliser System Center Configuration Manager Current Branch est avec la SA *(ou des droits d'abonnement équivalents)*. Pour plus d'informations, consultez les questions fréquentes (FAQ) sur la Software Assurance.
- **Microsoft License and Software Assurance (L&SA)** : Les clients qui achètent de nouvelles licences pour System Center Configuration Manager doivent acquérir une L&SA (Licence et SA).
  - La SA accorde les droits d'utilisation de Current Branch.
  - Si votre SA expire et que vous avez toujours une licence System Center Configuration Manager, vous ne pourrez plus utiliser Current Branch. Pour plus d'informations, consultez la question Si ma SA expire et que j'avais une L&SA, que se passe-t-il ?

Pour plus d'informations sur les offres de licences, consultez Comment acheter et Termes du contrat de licence du produit.

**J'ai rencontré le terme « abonnement équivalent », de quels programmes est-il question ?**

Les abonnements équivalents font référence à des programmes comme Enterprise Mobility + Security (EMS) ou Microsoft 365 Entreprise. Il peut y en avoir d'autres, mais ceux-ci sont les plus courants. Ils sont considérés dans les conditions des produits de gestion des licences en volume Microsoft comme des licences équivalentes à des licences de gestion.

**J'ai Enterprise Mobility + Security mais il a expiré, que dois-je faire ?**

EMS accorde les droits d'utilisation de System Center Configuration Manager (Current Branch et Long Term Servicing Branch). Après expiration de ces droits, vous n'aurez plus le droit d'utiliser de branches et devrez procéder à une désinstallation.

**Si ma SA expire et que j'avais une L&SA, que se passe-t-il ?**

Si votre SA a expiré après le 1er octobre 2016, selon le programme dans le cadre duquel vous avez acquis la L&SA, vous pouvez conserver une licence perpétuelle pour utiliser LTSB (Long Term Servicing Branch). Si vous utilisez la version Current Branch, vous devez la désinstaller, puis installer LTSB. Il n'existe aucune prise en charge de la migration ni de la conversion vers LTSB à partir de Current Branch.

Si votre SA a expiré avant le 1er octobre 2016 et que vous avez conservé une licence perpétuelle pour System Center Configuration Manager, votre seule option pour continuer à l'utiliser consiste à installer et utiliser System Center 2012 R2 Configuration Manager et ses Service Packs disponibles. Vous deviez désinstaller Current Branch lors de l'expiration de votre SA et réinstaller cette version antérieure du produit. Il n'existe aucune prise en charge de la migration ni du passage à une version antérieure depuis System Center Configuration Manager Current Branch vers des versions précédentes de Configuration Manager.

**Suis-je « propriétaire » de Current Branch ?**

Non. Vous bénéficiez d'une licence pour utiliser Current Branch pendant que vous avez une SA active. Par exemple, avec *L&SA*, quand la *SA* arrive à expiration, il ne vous reste plus que les droits *L (Licence)*, ce qui n'inclut pas les droits d'utilisation de Current Branch. Si votre L (Licence) fournit des droits perpétuels, vous pouvez utiliser LTSB (Long Term Servicing Branch) de System Center Configuration Manager (ou System Center 2012 R2 Configuration Manager si votre SA a expiré avant le 1er octobre 2016) à la place de Current Branch.

**Puis-je acheter System Center Configuration Manager autonome sans SA ?**

Non. La seule façon d'obtenir les droits d'utiliser System Center Configuration Manager est d'acquérir une licence avec SA ou via un abonnement équivalent. Il existe des programmes pour développeurs (comme MSDN) où System Center Configuration Manager est proposé à des fins de développement et de test, mais pas pour une utilisation en production.

**Je vois des mises à jour pour System Center Configuration Manager proposées depuis ma console, comme la version 1610. Ai-je le droit de les installer ?**

Si vous avez une *SA* active, vous pouvez. Si vous n'avez pas de SA active, vous devez désinstaller Current Branch, puis installer LTSB de System Center Configuration Manager. LTSB ne reçoit pas de mises à jour pour les versions incrémentielles de System Center Configuration Manager, mais reçoit les mises à jour de sécurité selon le cycle de vie de prise en charge.

**J'ai acheté EMS ou Microsoft 365 via un fournisseur de solutions cloud (CSP), ai-je les droits pour utiliser System Center Configuration Manager ?**

Oui, vous disposez des droits d'utilisation de System Center Configuration Manager pour gérer les clients couverts par la licence EMS. Commencez par télécharger et installer le logiciel d'évaluation. Contactez le support Microsoft pour obtenir la clé de licence.

**Est-ce que la date de fin de mon abonnement est pareille qu'une date d'expiration d'une SA ?**

Si la *SA* ou votre abonnement est actif, vous disposez des droits d'utilisation pour System Center Configuration Manager Current Branch. Un abonnement actif équivaut à une *SA* active, mais pas à une *licence (« L »)* perpétuelle. Une fois votre abonnement terminé, vous devez désinstaller Current Branch et vous n'avez pas le droit d'utiliser LTSB.

**Quels sont les droits d'utilisation associés à la technologie SQL fournie avec System Center Configuration Manager ?**

Tous les produits System Center englobent la technologie SQL Server. Les conditions de gestion des licences Microsoft pour ces produits autorisent le client à utiliser la technologie SQL Server uniquement pour prendre en charge les composants de System Center. Les licences d'accès client SQL Server ne sont pas requises dans cet usage.

Voici quelques exemples de droits d'utilisation approuvés pour les fonctionnalités SQL avec System Center Configuration Manager :

- Rôle de base de données de site
- Windows Server Update Services (WSUS) pour le rôle de point de mise à jour logicielle
- SQL Server Reporting Services (SSRS) pour le rôle de point de rapport
- Rôle de point de service de l'entrepôt de données
- Réplicas de base de données pour les rôles de points de gestion
- SQL Server AlwaysOn

La licence SQL Server incluse avec System Center Configuration Manager prend en charge chacune des instances de SQL Server qui seront installées afin d'héberger une base de données pour Configuration Manager. Cependant, avec cette licence, seules les bases de données de Configuration Manager figurant dans la liste précédente peuvent s'exécuter sur ce serveur SQL Server. Si une base de données d'un autre produit Microsoft ou tiers partage le serveur SQL Server, il vous faudra une licence distincte pour cette instance de SQL Server.

# Questions fréquemment posées sur les données d'utilisation et de diagnostic pour System Center Configuration Manager

22/06/2018 • 6 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cet article fournit les réponses aux questions fréquemment posées sur les données de diagnostic et d'utilisation dans Configuration Manager.

## FAQ

**Comment désactiver la télémétrie ?**

La télémétrie ne peut pas être désactivée. Toutefois, vous pouvez choisir le niveau des données de télémétrie collectées. Pour définir le moment auquel les données de télémétrie sont envoyées, utilisez le point de connexion de service en mode hors connexion.

La version Current Branch de Configuration Manager doit être mise à jour régulièrement pour pouvoir prendre en charge les nouvelles versions de Windows 10 et de Microsoft Intune. Microsoft nécessite au moins des données de base pour le diagnostic et l'utilisation. Ces données sont utilisées pour conserver le produit à jour et améliorer l'expérience de mise à jour, ainsi que la qualité et la sécurité du produit.

**Quelle est la période de rétention des données ?**

Les données d'utilisation et de diagnostic sont conservées un an.

**Des données d'utilisation et de diagnostic sont-elles envoyées lors de l'installation ou de la mise à jour du produit ?**

Non. Des données d'utilisation et de diagnostic sont envoyées uniquement une fois le site installé et opérationnel.

**À quelle fréquence les données sont-elles envoyées ?**

Les procédures stockées SQL s'exécutent tous les sept jours, à partir de la date d'installation du site. En mode en ligne, le point de connexion de service est configuré pour charger les données après l'exécution de requêtes. En mode hors connexion, l'administrateur utilise l'outil de connexion de service pour charger les données. Pour utiliser les données hors connexion, vous devez attendre sept jours après l'installation du site.

**Les données peuvent-elles être utilisées pour former un mappage réseau ?**

Comme indiqué dans la description des niveaux de données d'utilisation et de diagnostic, les détails du site incluent les informations de fuseau horaire de chaque site. Celles-ci peuvent fournir des insights concernant la géolocalisation large et la dispersion globale des sites dans une hiérarchie. Ces données ne contiennent aucune information relative au réseau, comme des adresses IP ou des informations géographiques plus détaillées. Pour plus d'informations, consultez la liste des articles sur les données d'utilisation et de diagnostic, puis recherchez les niveaux de collecte des données de diagnostic et d'utilisation correspondant à la version que vous utilisez.

**Pouvez-vous voir les données figurant dans des tables personnalisées ?**

Non. Configuration Manager collecte des données de diagnostic et d'utilisation au moyen de procédures stockées SQL. Ces procédures stockées s'exécutent sur les tables de produit par défaut de la base de données. Toutes ces tables SQL ont le préfixe **TEL**_. Dans le cadre de la requête de détection de schéma SQL, tous les noms de tables sont hachés à des fins de comparaison avec les valeurs par défaut connues. Ce comportement détermine l'existence de tables personnalisées dans la base de données. La présence de tables personnalisées indique que le

schéma de la base de données par défaut a été étendu. Il n'inclut pas les données stockées dans ces tables.

**Pouvez-vous voir les noms d'autres bases de données, ou des données dans d'autres bases de données ?**

Non. Les procédures stockées pour la collecte des données sont limités à la base de données du site.

**Configuration Manager est-il soumis au règlement général sur la protection des données (RGPD) ?**

Non. Configuration Manager n'est pas soumis au règlement général sur la protection des données. Il s'agit d'un produit installé en local que vous déployez, gérez et exécutez directement. Les données d'utilisation et de diagnostic collectées par Microsoft sont destinées à améliorer l'expérience d'installation, ainsi que la qualité et la sécurité des futures versions. Ces données sont soumises au règlement général sur la protection des données. Aucune information d'identification de l'utilisateur final et aucun identificateur de pseudonyme de l'utilisateur final ne sont collectés et transmis à Microsoft. Pour plus d'informations sur le règlement général sur la protection des données, consultez le Centre de confidentialité Microsoft sur le règlement général sur la protection des données. Pour plus d'informations sur les données Configuration Manager, consultez Données d'utilisation et de diagnostic.

## Voir aussi

Données de diagnostic et d'utilisation

# Se préparer pour System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez les informations données dans les rubriques suivantes quand vous êtes prêt à planifier votre déploiement de System Center Configuration Manager :

- Concevoir une hiérarchie de sites pour System Center Configuration Manager
- Principes de base de l'administration basée sur des rôles pour System Center Configuration Manager
- Concepts fondamentaux de la gestion de contenu dans System Center Configuration Manager
- Comprendre comment les clients recherchent des services et des ressources de site pour System Center Configuration Manager
- Préparer votre environnement réseau à System Center Configuration Manager
- Configurations prises en charge pour System Center Configuration Manager

# Fonctions et fonctionnalités de System Center Configuration Manager

22/06/2018 • 9 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les principales fonctionnalités de gestion de System Center Configuration Manager sont exposées ci-après. Chaque fonctionnalité possède ses propres prérequis, et les fonctionnalités que vous souhaitez utiliser peuvent influencer la conception et l'implémentation de votre hiérarchie Configuration Manager. Par exemple, si vous souhaitez déployer des logiciels sur des appareils de votre hiérarchie, vous devez installer le rôle de système de site du point de distribution.

Pour plus d'informations sur la planification et l'installation de Configuration Manager pour prendre en charge ces fonctionnalités de gestion dans votre environnement, consultez Se préparer pour System Center Configuration Manager.

**Gestion des applications**

Fournit un ensemble d'outils et de ressources qui peuvent vous aider à créer, gérer, déployer et surveiller les applications sur les différents types d'appareils que vous gérez. Par ailleurs, Configuration Manager met à votre disposition des outils qui vous aident à protéger les données de votre entreprise contenues dans les applications des utilisateurs. Consultez Introduction à la gestion des applications.

**Accès aux ressources d'entreprise**

Fournit un ensemble d'outils et de ressources qui permettent aux utilisateurs de votre organisation d'accéder à des données et des applications à partir d'emplacements distants. Ces outils incluent les profils Wi-Fi, les profils VPN, les profils de certificat et l'accès conditionnel à Exchange et SharePoint Online. Consultez Protéger les données et l'infrastructure des sites avec System Center Configuration Manager et Gérer l'accès aux services dans System Center Configuration Manager.

**Paramètres de compatibilité**

Fournit un ensemble d'outils et de ressources susceptibles de vous aider à évaluer, suivre et corriger la compatibilité de la configuration des appareils clients de l'entreprise. De plus, vous pouvez utiliser les paramètres de compatibilité pour configurer tout un éventail de fonctionnalités et de paramètres de sécurité sur les appareils que vous gérez. Consultez Garantir la conformité des appareils avec System Center Configuration Manager.

**Endpoint Protection**

Propose une gestion de la sécurité, des logiciels anti-programme malveillant et du Pare-feu Windows pour les ordinateurs de votre entreprise. Consultez Endpoint Protection dans System Center Configuration Manager.

**Inventaire**

Fournit un ensemble d'outils pour aider à identifier et surveiller les actifs :

- **Inventaire matériel**: collecte des informations détaillées sur le matériel des appareils de votre entreprise. Consultez Présentation de l'inventaire matériel dans System Center Configuration Manager.
- **Inventaire logiciel**: collecte et rapporte des informations sur les fichiers qui sont stockés sur des ordinateurs clients de votre organisation. Consultez Présentation de l'inventaire logiciel dans System Center Configuration Manager.

- **Asset Intelligence**: fournit des outils pour collecter les données d'inventaire et surveiller l'utilisation des licences de logiciels dans votre entreprise. Consultez Présentation d'Asset Intelligence dans System Center Configuration Manager.

**Gestion des appareils mobiles avec Microsoft Intune**

Vous pouvez utiliser Configuration Manager pour gérer des appareils iOS, Android (dont Samsung KNOX Standard), Windows Phone et Windows à l'aide du service Microsoft Intune sur Internet.

Même si vous utilisez le service Intune, les tâches de gestion s'effectuent à l'aide du rôle de système de site de point de connexion de service, disponible via la console Configuration Manager. Consultez Gestion des appareils mobiles (MDM) hybride avec System Center Configuration Manager et Microsoft Intune.

**Gestion des appareils mobiles locale**

Inscrit et gère les PC et les appareils mobiles en utilisant l'infrastructure Configuration Manager locale et les fonctionnalités de gestion intégrées aux plateformes d'appareils (au lieu d'utiliser un client Configuration Manager installé séparément). Prend actuellement en charge la gestion des appareils Windows 10 Entreprise et Windows 10 Mobile. Consultez Gérer des appareils mobiles avec une infrastructure locale dans System Center Configuration Manager.

**Déploiement de systèmes d'exploitation**

Fournit un outil pour créer des images de système d'exploitation. Vous pouvez ensuite utiliser ces images pour déployer les systèmes d'exploitation sur des ordinateurs, à l'aide du démarrage PXE ou d'un média de démarrage, tel qu'un jeu de CD, un DVD ou des lecteurs flash USB. Notez que cela s'applique aux ordinateurs qui sont gérés par Configuration Manager ainsi qu'aux ordinateurs non gérés. Consultez Introduction au déploiement de système d'exploitation dans System Center Configuration Manager.

**Gestion de l'alimentation**

Fournit un ensemble d'outils et de ressources que vous pouvez utiliser pour gérer et surveiller la consommation d'énergie des ordinateurs clients dans l'entreprise. Consultez Présentation de la gestion de l'alimentation dans System Center Configuration Manager.

**Requêtes**

Fournit un outil pour récupérer des informations sur les ressources de votre hiérarchie et des informations sur les données d'inventaire et les messages d'état. Vous pouvez ensuite utiliser ces informations pour établir des rapports ou pour définir des regroupements d'appareils ou d'utilisateurs pour les paramètres de déploiement et de configuration de logiciels. Consultez Présentation des requêtes dans System Center Configuration Manager.

**Profils de connexion à distance**

Fournit un ensemble d'outils et de ressources pour vous aider à créer, déployer et surveiller les paramètres de connexion à distance vers des appareils de votre organisation. En déployant ces paramètres, vous réduisez l'effort fourni par les utilisateurs pour se connecter à leurs ordinateurs sur le réseau d'entreprise. Consultez Utilisation de profils de connexion à distance dans System Center Configuration Manager.

**Éléments de configuration des données et profils utilisateur**

Les éléments de configuration des données et profils utilisateur dans Configuration Manager contiennent des paramètres permettant de gérer la redirection de dossiers, les fichiers hors connexion et les profils itinérants sur des ordinateurs qui exécutent Windows 8 et versions ultérieures pour les utilisateurs de votre hiérarchie. Consultez Utilisation d'éléments de configuration des données et profils utilisateur dans System Center Configuration Manager.

**Contrôle à distance**

Fournit des outils pour administrer des ordinateurs clients à distance, à partir de la console Configuration Manager. Consultez Présentation du contrôle à distance dans System Center Configuration Manager.

**Rapports**

Fournissent un ensemble d'outils et de ressources vous permettant d'utiliser les fonctionnalités de création de rapport avancées de SQL Server Reporting Services à partir de la console Configuration Manager. Consultez Présentation des rapports dans System Center Configuration Manager.

**Contrôle de logiciel**

Fournit des outils pour surveiller et collecter les données d'utilisation des logiciels à partir de clients Configuration Manager. Consultez Surveiller l'utilisation des applications avec le contrôle de logiciel dans System Center Configuration Manager.

**Mises à jour logicielles**

Fournit un ensemble d'outils et de ressources qui peuvent vous aider à gérer, déployer et surveiller les mises à jour logicielles dans l'entreprise. Consultez Présentation des mises à jour logicielles dans System Center Configuration Manager.

# Changements dans System Center Configuration Manager par rapport à System Center 2012 Configuration Manager

22/06/2018 • 21 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Current Branch de System Center Configuration Manager présente des changements importants par rapport à System Center 2012 Configuration Manager. Cette rubrique identifie les changements importants et les nouvelles fonctionnalités dans la version de base de référence 1511 de System Center Configuration Manager. Pour en savoir plus sur les changements introduits dans les mises à jour suivantes pour System Center Configuration Manager, consultez Nouveautés dans les versions incrémentielles de System Center Configuration Manager.

La version de décembre 2015 de System Center Configuration Manager (version 1511) était la version initiale du produit Configuration Manager actuel de Microsoft. Elle est généralement désignée sous le nom de « Current Branch » de System Center Configuration Manager. La mention *Current Branch* indique qu'il s'agit d'une version qui prend en charge les mises à jour incrémentielles du produit. Elle représente également un moyen de faire la distinction entre cette version et les versions précédentes de Configuration Manager.

System Center Configuration Manager :

- N'utilise pas d'identificateur d'année ni de produit dans le nom du produit, comme c'était le cas dans les versions précédentes telles que Configuration Manager 2007 ou System Center 2012 Configuration Manager.
- Prend en charge les mises à jour incrémentielles dans le produit, aussi appelées versions de mise à jour. La version initiale était la version 1511. Les versions suivantes sont publiées plusieurs fois par an sous la forme de mises à jour dans la console, comme la version 1710.
- Est installé à l'aide d'une version de base. La version 1511 était la version de base initiale, mais de nouvelles versions de base sont également publiées de temps à autre, comme la version 1802. Les versions de base peuvent être utilisées pour installer un nouveau site System Center Configuration Manager et sa hiérarchie ou pour mettre à niveau à partir d'une version prise en charge de Configuration Manager 2012.

## Mises à jour dans la console pour Configuration Manager

System Center Configuration Manager utilise une méthode de service dans la console appelée **Mises à jour et maintenance** qui facilite la localisation et l'installation des mises à jour recommandées.

Certaines versions disponibles uniquement comme mises à jour pour des sites existants (à partir de la console Configuration Manager) ne peuvent pas être utilisées pour installer de nouveaux sites Configuration Manager. Par exemple, la mise à jour 1710 est disponible uniquement à partir de la console Configuration Manager. Elle est utilisée pour mettre à jour un site qui exécute déjà une version de System Center Configuration Manager.

Une version de mise à jour est également publiée régulièrement sous la forme d'une nouvelle version de base (par exemple, la mise à jour 1802). Ce type de mise à jour peut être utilisée pour installer une nouvelle hiérarchie sans avoir à démarrer avec une ancienne version de base de référence (comme 1511) et à effectuer une mise à niveau vers la version la plus récente.

Pour plus d'informations sur l'utilisation des mises à jour, consultez Mises à jour pour System Center Configuration Manager.

Pour plus d'informations sur les versions de base, consultez Versions de base et de mise à jour.

## Nouveau rôle de système de site : point de connexion de service

Le **connecteur Microsoft Intune** est remplacé par un nouveau rôle de système de site qui offre des fonctionnalités supplémentaires, à savoir le **point de connexion de service**. Le point de connexion de service :

- remplace le connecteur Microsoft Intune quand vous intégrez Intune à la gestion des appareils mobiles locale System Center Configuration Manager.
- est utilisé comme point de contact pour les appareils que vous gérez.
- charge des données d'utilisation relatives à votre déploiement sur le service cloud Microsoft.
- met des mises à jour qui s'appliquent à votre déploiement à disposition à partir de la console Configuration Manager.

Ce rôle de système de site prend en charge à la fois un mode en ligne et hors connexion de fonctionnement. Pour plus d'informations, voir À propos du point de connexion de service dans System Center Configuration Manager.

## Collecte des données d'utilisation

System Center Configuration Manager collecte des données d'utilisation sur vos sites et votre infrastructure. Ces informations sont compilées et transmises au service cloud Microsoft par le point de connexion de service. Configuration Manager en a besoin pour télécharger les mises à jour applicables à la version de Configuration Manager que vous utilisez pour votre déploiement. Au moment de configurer le point de connexion de service, vous pouvez définir le niveau des données collectées et si celles-ci sont envoyées automatiquement (mode en ligne) ou manuellement (mode hors connexion).

Pour plus d'informations, consultez Paramètres et niveaux de données d'utilisation.

## Prise en charge de la technologie Intel AMT (Active Management Technology)

Avec System Center Configuration Manager, la prise en charge native des ordinateurs AMT à partir de la console Configuration Manager est supprimée. Les ordinateurs AMT restent entièrement gérés quand vous utilisez le module complémentaire Intel SCS pour Microsoft System Center Configuration Manager. Ce module complémentaire vous permet d'accéder aux dernières fonctionnalités permettant de gérer AMT tout en supprimant les limitations introduites jusqu'à ce que Configuration Manager puisse intégrer ces changements.

La suppression de la technologie AMT intégrée pour System Center Configuration Manager inclut la gestion hors bande. Le rôle de système de site de point de gestion hors bande n'est plus utilisé, ni disponible.

Notez que la gestion hors bande dans System Center 2012 Configuration Manager n'est pas affectée par cette modification.

## Fonctionnalités déconseillées

Certaines fonctionnalités, telles que la prise en charge de la technologie Intel AMT (Active Management Technology), sont retirées de la console Configuration Manager. D'autres comme la protection d'accès réseau sont entièrement retirées. Par ailleurs, certains produits Microsoft plus anciens comme Windows Vista, Windows Server 2008 et SQL Server 2008 ne sont plus pris en charge.

Pour obtenir la liste des fonctionnalités dépréciées, consultez Éléments supprimés et dépréciés dans System Center Configuration Manager.

Pour plus d'informations sur les produits, les systèmes d'exploitation et les configurations pris en charge,

consultez Configurations prises en charge pour System Center Configuration Manager.

## Déploiement des clients

System Center Configuration Manager inaugure une nouvelle fonctionnalité visant à tester les nouvelles versions du client Configuration Manager avant la mise à niveau du reste du site avec le nouveau logiciel. Vous pouvez configurer un regroupement de préproduction dans lequel piloter un nouveau client. Dès lors que vous êtes satisfait du nouveau logiciel client en préproduction, vous pouvez le promouvoir pour mettre automatiquement à niveau le reste du site avec la nouvelle version.

Pour plus d'informations sur le test des clients, consultez Comment tester les mises à niveau du client dans un regroupement de préproduction dans System Center Configuration Manager.

## Déploiement du système d'exploitation

Tenez compte des modifications suivantes apportées au déploiement du système d'exploitation :

- Dans l'Assistant Création d'une séquence de tâches, un nouveau type de séquence de tâches est disponible, à savoir **Mettre à niveau un système d'exploitation à partir du package de mise à niveau**. Cette séquence permet de créer la procédure de mise à niveau des ordinateurs Windows 7, Windows 8 ou Windows 8.1 vers Windows 10. Pour plus d'informations, voir Upgrade Windows to the latest version with System Center Configuration Manager.

- Le cache d'homologue Windows PE est désormais disponible pendant le déploiement de systèmes d'exploitation. Les ordinateurs qui exécutent une séquence de tâches pour le déploiement d'un système d'exploitation peuvent utiliser le cache d'homologue Windows PE pour obtenir le contenu d'un homologue local (source de cache d'homologue) au lieu de télécharger du contenu auprès d'un point de distribution. Cela permet de réduire le trafic du réseau étendu dans les scénarios de succursale où il n'existe aucun point de distribution local. Pour plus d'informations, voir Prepare Windows PE peer cache to reduce WAN traffic in System Center Configuration Manager.

- Vous pouvez désormais afficher l'état de Windows sous forme de service dans votre environnement. Vous pouvez également créer des plans de maintenance pour former des anneaux de déploiement et vérifier que les ordinateurs Windows 10 Current Branch sont tenus à jour quand de nouvelles versions sont publiées. Par ailleurs, vous pouvez être alerté quand la prise en charge de la build CB (Current Branch) ou CBB (Current Branch for Business) des clients Windows 10 touche à sa fin. Pour plus d'informations, voir Gérer Windows as a Service (WaaS) à l'aide de System Center Configuration Manager.

## Gestion des applications

Tenez compte des modifications suivantes apportées à la gestion des applications :

- System Center Configuration Manager vous permet de déployer des applications de la plateforme Windows universelle pour les appareils exécutant Windows 10 et des versions ultérieures. Consultez Création d'applications Windows avec System Center Configuration Manager.

- Le Centre logiciel a été modernisé. Les applications qui figuraient uniquement dans le catalogue d'applications (applications accessibles à l'utilisateur) apparaissent désormais dans le Centre logiciel sous l'onglet Applications. Ces déploiements sont ainsi plus identifiables pour les utilisateurs qui n'ont plus besoin d'utiliser le catalogue d'applications. De plus, un navigateur Silverlight n'est plus nécessaire. Consultez Planifier et configurer la gestion des applications dans System Center Configuration Manager.

- Par l'intermédiaire du type d'application MDM, le nouveau Windows Installer vous permet de créer et déployer des applications Windows Installer sur les PC inscrits qui exécutent Windows 10. Consultez Création d'applications Windows avec System Center Configuration Manager.

- Quand vous créez une application pour une application iOS interne, vous devez seulement spécifier le fichier d'installation (.ipa) de l'application. Vous n'avez plus besoin de spécifier de fichier de liste de propriétés (.plist) correspondant. Consultez Création d'applications iOS avec System Center Configuration Manager.
- Dans Configuration Manager 2012, pour spécifier un lien vers une application du Windows Store, vous pouviez soit spécifier directement le lien, soit accéder à un ordinateur distant sur lequel l'application était installée. Dans System Center Configuration Manager, vous pouvez toujours entrer directement le lien mais, au lieu d'accéder à un ordinateur de référence, vous pouvez rechercher l'application directement dans le Store à partir de la console Configuration Manager.

## Mises à jour logicielles

Tenez compte des modifications suivantes apportées aux mises à jour logicielles :

- System Center Configuration Manager peut désormais faire la distinction entre les différentes méthodes de gestion des mises à jour logicielles pour les ordinateurs. Plus précisément, il peut faire la différence entre un ordinateur Windows 10 qui se connecte à WUfB (Windows Update for Business) pour la gestion des mises à jour logicielles et un ordinateur connecté à WSUS à cette même fin. **UseWUServer** est un nouvel attribut qui indique si l'ordinateur est géré avec WUfB. Vous pouvez utiliser ce paramètre dans un regroupement pour retirer ces ordinateurs de la gestion des mises à jour logicielles. Pour plus d'informations, voir Intégration avec Windows Update for Business dans Windows 10.
- Vous pouvez maintenant planifier et exécuter la tâche de nettoyage WSUS à partir de la console Configuration Manager. Dans les propriétés du **composant du point de mise à jour logicielle**, quand vous choisissez d'exécuter la tâche de nettoyage WSUS, elle s'exécute à la prochaine synchronisation des mises à jour logicielles. Les mises à jour logicielles qui ont expiré présentent un état refusé sur le serveur WSUS et l'Agent Windows Update ne les analyse plus. Pour plus d'informations, voir Schedule and run the WSUS clean up task.

## Paramètres de conformité

Tenez compte des modifications suivantes apportées aux paramètres de compatibilité :

- System Center Configuration Manager améliore le flux de travail pour créer les éléments de configuration. Désormais, quand vous créez un élément de configuration et que vous sélectionnez une plateforme prise en charge, seuls les paramètres correspondant à cette plateforme vous sont proposés. Consultez Prise en main des paramètres de compatibilité dans System Center Configuration Manager.
- L'Assistant **Création d'élément de configuration** vous permet désormais de choisir plus facilement le type d'élément de configuration à créer. De plus, les éléments de configuration nouveaux et mis à jour sont disponibles pour :
  - les appareils Windows 10 gérés avec le client Configuration Manager ;
  - les appareils Mac OS X gérés avec le client Configuration Manager ;
  - les ordinateurs de bureau et serveur Windows gérés avec le client Configuration Manager ;
  - les appareils Windows 8.1 et Windows 10 gérés sans le client Configuration Manager ;
  - les appareils Windows Phone gérés sans le client Configuration Manager ;
  - les appareils iOS et Mac OS X gérés sans le client Configuration Manager ;
  - les appareils Samsung KNOX Standard et Android gérés sans le client Configuration Manager.

  Consultez Comment créer des éléments de configuration dans System Center Configuration Manager.

- Prise en charge de la gestion des paramètres sur les ordinateurs Mac OS X inscrits avec Microsoft Intune ou gérés à l'aide du client Configuration Manager. Consultez Comment créer des éléments de configuration pour des appareils iOS et Mac OS X gérés sans le client System Center Configuration Manager.

## Protéger l'infrastructure de site et les données

System Center Configuration Manager permet d'intégrer Windows Hello Entreprise (anciennement Microsoft Passport pour Windows). Windows Hello Entreprise constitue une méthode de connexion alternative qui utilise Active Directory ou un compte Azure Active Directory en remplacement d'un mot de passe, d'une carte à puce ou d'une carte à puce virtuelle sur les appareils exécutant Windows 10. Consultez Paramètres Windows Hello Entreprise dans System Center Configuration Manager.

## Gestion des appareils mobiles avec Microsoft Intune

System Center Configuration Manager propose des améliorations en matière de gestion des appareils mobiles, avec notamment :

- une limitation du nombre d'appareils qu'un utilisateur peut inscrire ;
- la possibilité de spécifier des conditions générales que les utilisateurs du portail d'entreprise doivent accepter avant de pouvoir inscrire ou utiliser l'application ;
- l'ajout d'un rôle de gestionnaire d'inscription d'appareil pour faciliter la gestion d'un grand nombre d'appareils.

Pour plus d'informations sur les fonctionnalités de gestion des appareils mobiles avec Configuration Manager et Intune, consultez Gestion des appareils mobiles (MDM) hybride avec System Center Configuration Manager et Microsoft Intune.

## Gestion des appareils mobiles (MDM) locale

Vous pouvez désormais gérer les appareils mobiles au moyen d'une infrastructure Configuration Manager locale. La gestion des appareils et les données associées sont traitées localement et ne font pas partie de Microsoft Intune ni d'autres services cloud. Ce type de gestion d'appareils ne fait appel à aucun logiciel client. Configuration Manager gère les appareils avec des fonctionnalités qui sont intégrées aux systèmes d'exploitation des appareils.

Pour en savoir plus, consultez Gérer des appareils mobiles avec une infrastructure locale dans System Center Configuration Manager.

# Nouveautés des versions incrémentielles de System Center Configuration Manager

02/07/2018 • 3 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Configuration Manager utilise un processus de mise à jour et de maintenance dans la console. Ce processus facilite la découverte et l'installation des mises à jour Configuration Manager. Vous n'avez plus à gérer ni à installer les Services Packs ou les versions de mise à jour cumulative. Vous n'avez plus à rechercher le téléchargement de la version ou de la mise à jour la plus récente.

Pour mettre à jour le produit avec une nouvelle version de Current Branch, utilisez la console Configuration Manager pour rechercher puis installer les mises à jour dans la console. Plusieurs fois par an, Microsoft publie de nouvelles versions qui incluent des mises à jour du produit. Chaque version contient également de nouvelles fonctionnalités. Quand vous installez une mise à jour avec de nouvelles fonctionnalités, vous pouvez choisir d'utiliser ces fonctionnalités.

Les versions des mises à jour sont identifiées par un numéro composé de l'année et du mois. Par exemple, la version 1511 indique « Novembre 2015 » (mois auquel Configuration Manager Current Branch est sorti en version RTM). Les versions suivantes portent des noms tels que 1802, lequel indique que la mise à jour a été créée en février 2018. Ces versions de mise à jour sont essentielles pour identifier la version incrémentielle de votre installation Configuration Manager et les fonctionnalités que vous pouvez activer dans votre environnement.

## Versions prises en charge

Utilisez les liens suivants pour découvrir les nouveautés propres à chaque version prise en charge :

- Nouveautés de la version 1802
- Nouveautés dans la version 1710
- Nouveautés dans la version 1706

Pour les versions de Configuration Manager publiées avant la version 1710, la prise en charge dure 12 mois. À compter de la version 1710, chaque version de mise à jour reste prise en charge pendant 18 mois suivant sa date de disponibilité générale (GA). Pour rester à jour, utilisez la version la plus récente de la mise à jour. Pour plus d'informations, consultez Prise en charge des versions Current Branch de Configuration Manager.

## Voir aussi

Notes de publication

# Nouveautés de la version 1802 de System Center Configuration Manager

26/07/2018 • 31 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

La mise à jour 1802 pour la Current Branch de Configuration Manager est disponible en tant que mise à jour dans la console. Appliquez cette mise à jour sur les sites qui exécutent la version 1702, 1706 ou 1710. Lors de l'installation d'un nouveau site, elle est également disponible sous la forme d'une version de base de référence.

En plus des nouvelles fonctionnalités, cette version inclut également des modifications supplémentaires comme des corrections de bogues. Pour plus d'informations, consultez Récapitulatif des modifications dans Current Branch de System Center Configuration Manager version 1802.

Les mises à jour supplémentaires suivantes pour cette version sont également disponibles :

- Correctif cumulatif pour Current Branch de System Center Configuration Manager, version 1802

> **TIP**
> Pour installer un nouveau site, vous devez utiliser une version de base de Configuration Manager.
>
> Informations supplémentaires :
>
> - Installation de nouveaux sites
> - Installation de mises à jour sur les sites
> - Versions de base et de mise à jour

Les sections suivantes fournissent des détails sur les modifications et les nouvelles fonctionnalités de la version 1802 de Configuration Manager.

## Infrastructure de site

**Réaffecter un point de distribution**

De nombreux clients ont de grandes infrastructures Configuration Manager et réduisent le nombre de sites principaux ou secondaires pour simplifier leur environnement. Ils doivent néanmoins toujours conserver des points de distribution aux emplacements des filiales pour délivrer du contenu aux clients gérés. Ces points de distribution contiennent souvent plusieurs téraoctets ou plus de contenus. Ce contenu est coûteux en termes de temps et de bande passante réseau pour le distribuer à ces serveurs distants. Cette fonctionnalité vous permet de réaffecter un point de distribution à un autre site principal sans redistribuer le contenu. Cette action met à jour l'affectation du système de site tout en conservant la totalité du contenu sur le serveur. Pour plus d'informations, consultez Réaffecter un point de distribution.

**Configurer l'Optimisation de la distribution de Windows de façon à utiliser des groupes de limites Configuration Manager**

Les groupes de limites Configuration Manager permettent de définir et de réguler la distribution de contenu sur le réseau de l'entreprise et dans les agences. L'Optimisation de la distribution de Windows est une technologie cloud pair à pair de partage de contenu entre appareils Windows 10. À partir de cette version, vous pourrez la configurer de façon à ce qu'elle utilise vos groupes de limites pour partager du contenu entre pairs. Un nouveau paramètre client s'applique à l'identificateur de groupe de limites sous la forme de l'identificateur de groupe d'Optimisation de la distribution sur le client. Lorsque le client communique avec le service de cloud d'Optimisation de la

distribution, il utilise cet identificateur pour localiser les pairs possédant le contenu souhaité. Pour plus d'informations, consultez Concepts fondamentaux de la gestion de contenu.

**Prise en charge des appareils Windows 10 ARM64**

À partir de cette version, le client Configuration Manager est pris en charge sur les appareils Windows 10 ARM64. Les fonctionnalités de gestion du client existantes devraient fonctionner avec ces nouveaux appareils, par exemple, l'inventaire matériel et logiciel, les mises à jour logicielles et la gestion des applications. Le déploiement de système d'exploitation n'est pas pris en charge pour le moment.

**Prise en charge améliorée des certificats CNG**

La version 1710 de Configuration Manager (Current Branch) prend en charge les certificats Cryptography : Next Generation (CNG). La version 1710 limite la prise en charge aux certificats clients dans plusieurs scénarios.

À compter de cette version, utilisez des certificats de passerelle de gestion cloud pour les rôles serveurs HTTPS suivants :

- Point de gestion
- Point de distribution
- Point de mise à jour logicielle
- Point de migration d'état

**Groupe de limites de secours pour les points de gestion**

Configurez des relations de secours pour les points de gestion entre les groupes de limites. Ce comportement offre un meilleur contrôle des points de gestion que les clients utilisent. Pour plus d'informations, consultez Configurer des groupes de limites.

**Affinité de site de point de distribution cloud**

Cette fonctionnalité profite aux clients qui ont une hiérarchie multisite, géographiquement dispersée, utilisant des points de distribution cloud. Quand un client Internet recherchait du contenu, il n'y avait aucun ordre dans la liste des points de distribution cloud reçus par le client. Ce comportement avait comme conséquence que les clients Internet pouvaient recevoir le contenu de points de distribution cloud géographiquement distants. Le téléchargement du contenu d'un serveur distant est généralement plus lent que celui d'un serveur plus proche.

Avec l'affinité de site de point de distribution cloud, un client Internet reçoit une liste ordonnée. Cette liste établit la priorité des points de distribution cloud à partir du site affecté au client. Ce comportement permet à l'administrateur de conserver le but de sa conception pour les téléchargements de contenu à partir des ressources de site.

# Management insights

Les insights de gestion dans System Center Configuration Manager fournissent des informations sur l'état actuel de votre environnement. Les informations sont basées sur l'analyse des données provenant de la base de données du site. Ces informations vous aident à mieux comprendre votre environnement et à prendre des mesures en fonction de ces renseignements. Pour plus d'informations, consultez Insights de gestion

Dans Configuration Manager 1802, les insights suivants sont disponibles :

- Applications :
  - Applications sans déploiements
- Services cloud :
  - Évaluer la préparation de la cogestion
  - Permettre à vos appareils d'être hybrides joints à Azure Active Directory
  - Moderniser votre infrastructure d'identité et d'accès
  - Mettre à niveau vos clients vers Windows 10, version 1709 ou ultérieure

- Regroupements :
  - Regroupements vides
- Gestion simplifiée :
  - Versions des clients obsolètes
- Centre logiciel :
  - Diriger les utilisateurs vers le Centre logiciel au lieu du catalogue d'applications
  - Utiliser la nouvelle version du Centre logiciel
- Windows 10 :
  - Configurer la télémétrie et la clé d'ID commercial de Windows
  - Connecter Configuration Manager à Upgrade Readiness

## Gestion des clients

**Prise en charge de la Passerelle de gestion cloud pour Azure Resource Manager**

Lors de la création d'une instance de Passerelle de gestion cloud (CMG), l'Assistant offre maintenant la possibilité de créer un **déploiement Azure Resource Manager**. Azure Resource Manager est une plateforme moderne permettant de gérer l'ensemble des ressources de la solution comme une seule entité, nommée groupe de ressources. Lors du déploiement d'une Passerelle CMG avec Azure Resource Manager, le site utilise Azure Active Directory (Azure AD) pour authentifier et créer les ressources cloud nécessaires. Le certificat de gestion Azure classique n'est pas nécessaire pour ce déploiement modernisé. Pour plus d'informations, consultez Conception de la topologie de passerelle de gestion cloud.

> **IMPORTANT**
> Cette fonctionnalité ne permet pas la prise en charge des fournisseurs de services cloud Azure. Le déploiement de la passerelle de gestion cloud avec Azure Resource Manager continue d'utiliser le service cloud classique, que le fournisseur de services cloud ne prend pas en charge. Pour plus d'informations, consultez Services Azure disponibles auprès du fournisseur de services cloud Azure.

**Améliorations apportées à la passerelle de gestion cloud**

- À compter de cette version, la **passerelle de gestion cloud** n'est plus une fonctionnalité en préversion.
- La documentation des fonctionnalités a été revue et améliorée. Pour plus d'informations, consultez les articles suivants :
  - Planifier la passerelle de gestion cloud
  - Taille et scalabilité de la passerelle de gestion cloud en chiffres
  - Sécurité et confidentialité de la passerelle de gestion cloud
  - Questions fréquentes (FAQ) sur la passerelle de gestion cloud
  - Certificats pour la passerelle de gestion cloud
  - Configurer la passerelle de gestion cloud

**Configurer l'inventaire matériel pour collecter les chaînes supérieures à 255 caractères**

Vous pouvez configurer la longueur des chaînes à une taille supérieure à 255 caractères pour les propriétés de l'inventaire matériel. Cette modification s'applique seulement aux classes nouvellement ajoutées et aux propriétés de l'inventaire matériel qui ne sont pas des clés. Pour plus d'informations, consultez l'article Étendre l'inventaire matériel.

**Annonce de la dépréciation de la prise en charge des clients Linux et Unix**

Microsoft prévoit de déprécier la prise en charge des clients Linux et UNIX dans System Center Configuration Manager d'ici un an environ, de sorte que les clients ne seront pas inclus dans SCCM version 1902 dans le

calendrier anticipé de 2019. Dans le dernier calendrier 2018, la version 1810 de Configuration Manager est la dernière version à inclure les clients Linux et UNIX qui seront pris en charge pour le cycle de vie complet de Configuration Manager 1810. Après Configuration Manager 1810, les clients peuvent envisager Operations Management Suite de Microsoft pour la gestion des serveurs Linux. OMS offre une prise en charge étendue de Linux qui, dans la plupart des cas, dépasse les fonctionnalités de Configuration Manager, notamment la gestion des correctifs de bout en bout pour Linux.

#### Tableau de bord des appareils Surface

Le tableau de bord des appareils Surface fournit des informations sur les appareils Surface trouvés dans votre environnement. Dans la console, accédez à **Surveillance** > **Appareils Surface**. Vous pouvez voir les éléments suivants :

- Le pourcentage d'appareils Surface
- Le pourcentage de modèles Surface
- Les cinq principales versions de microprogramme

Pour plus d'informations, consultez l'article Tableau de bord Surface.

#### Changement dans l'installation du client Configuration Manager

À compter de cette version, Silverlight n'est plus installé automatiquement sur les appareils clients. Pour plus d'informations, consultez Prérequis pour le déploiement de clients sur des ordinateurs Windows.

## Cogestion

#### Transférer la charge de travail Endpoint Protection vers Intune à l'aide de la cogestion

La charge de travail Endpoint Protection peut être transférée à Intune après activation de la cogestion. Pour cela, accédez à la page des propriétés de cogestion et déplacez le curseur de Configuration Manager sur **Pilote** ou **Tout**. Pour plus d'informations sur les charges de travail, consultez Charges de travail pouvant être transférées à Intune. Pour plus d'informations sur la cogestion, consultez Cogestion pour les appareils Windows 10.

#### Tableau de bord de cogestion dans System Center Configuration Manager

À compter de cette version, vous pouvez consulter un tableau de bord avec des informations sur la cogestion. Le tableau de bord vous permet d'examiner les machines qui sont cogérées dans votre environnement. Les graphes peuvent vous aider à identifier les appareils qui demandent une attention particulière. Pour plus d'informations, consultez l'article Tableau de bord de cogestion.

## Paramètres de conformité

#### Stratégies du navigateur Microsoft Edge

Pour les clients qui utilisent le navigateur web Microsoft Edge sur des clients Windows 10, créez une stratégie de paramètres de conformité Configuration Manager pour configurer plusieurs paramètres Microsoft Edge. Pour plus d'informations, consultez Créer un profil de navigateur Microsoft Edge.

## Gestion des applications

#### Autoriser l'interaction utilisateur lors de l'installation d'une application

Autorisez un utilisateur final à interagir avec l'installation d'une application pendant l'exécution de la séquence de tâches. Par exemple, exécutez un processus d'installation qui invite l'utilisateur final à choisir diverses options. Certains programmes d'installation d'application ne peuvent pas se passer d'invites utilisateur ou le processus d'installation nécessite des valeurs de configuration spécifiques que seul l'utilisateur connaît. Cette fonctionnalité vous permet de gérer ces scénarios d'installation. Pour plus d'informations, consultez Spécifier des options d'expérience utilisateur pour le type de déploiement.

#### Ne pas mettre automatiquement à niveau les applications remplacées

Configurez un déploiement d'application pour ne pas mettre à niveau automatiquement les versions remplacées. Désormais, quand vous créez le déploiement, dans la page **Paramètres du déploiement** de l'**Assistant Déploiement logiciel**, pour un objectif d'installation **Disponible**, vous pouvez activer ou désactiver l'option **Mettre automatiquement à niveau toutes les versions remplacées de cette application**. Pour plus d'informations, consultez Spécifier des paramètres de déploiement.

#### Approuver les demandes d'application pour les utilisateurs appareil par appareil

À compter de cette version, lorsqu'un utilisateur demande une application qui nécessite une approbation, le nom de l'appareil fait partie de la demande. Si l'administrateur approuve la demande, l'utilisateur ne pourra installer l'application que sur cet appareil. Il devra soumettre une autre demande pour installer l'application sur un autre appareil. Pour plus d'informations, consultez Spécifier des paramètres de déploiement.

> **NOTE**
> Cette fonctionnalité est facultative. Pour plus d'informations, consultez Activer les fonctionnalités facultatives des mises à jour.

#### Améliorations apportées à l'exécution de scripts

À compter de cette version, la fonctionnalité **Exécuter les scripts** n'est plus en préversion. La sortie du script est désormais retournée au format JSON. Pour plus d'informations, consultez Créer et exécuter des scripts PowerShell à partir de la console Configuration Manager.

## Déploiement du système d'exploitation

#### Séquence de tâches de mise à niveau sur place de Windows 10 via la Passerelle de gestion cloud

La séquence de tâches de mise à niveau sur place de Windows 10 prend maintenant en charge le déploiement vers des clients basés sur Internet et gérés par le biais de la Passerelle de gestion cloud. Cette capacité permet aux utilisateurs distants de passer plus facilement à Windows 10, sans avoir à se connecter au réseau d'entreprise. Pour plus d'informations, voir Déployer une séquence de tâches.

#### Améliorations apportées à la séquence de tâches de mise à niveau sur place de Windows 10

Le modèle de séquence de tâches par défaut pour la mise à niveau sur place de Windows 10 comprend maintenant des groupes supplémentaires, avec des actions recommandées à ajouter avant ou après le processus de mise à niveau. Ces actions sont communes à de nombreux clients qui parviennent à mettre à niveau des appareils sur Windows 10. Pour plus d'informations, consultez Créer une séquence de tâches pour mettre à niveau un système d'exploitation.

#### Améliorations apportées au déploiement des systèmes d'exploitation

Cette version inclut les améliorations suivantes pour le déploiement de système d'exploitation :

- Dans Windows PE, lors du lancement de cmtrace.exe, vous n'êtes plus invité à choisir s'il faut utiliser ce programme comme visionneuse par défaut pour les fichiers journaux.
- Ajoutez des images de démarrage à l'étape de séquence de tâches Télécharger le contenu du package.
- Améliorations apportées à l'étape Exécuter une séquence de tâches :
  - Prise en charge de tous les scénarios de déploiement de système d'exploitation à partir du Centre logiciel, de l'environnement PXE (Preboot Execution Environment) et de médias.
  - Améliorations apportées à des actions de console comme la copie, l'importation, l'exportation et l'avertissement lors de la suppression d'objets.
  - Prise en charge de l'Assistant Création d'un fichier de contenu préparé.
  - Intégration à la vérification du déploiement. Pour plus d'informations, consultez Déploiements de séquences de tâches à haut risque.
  - Vous pouvez désormais utiliser l'étape d'exécution de la séquence de tâches sur plusieurs niveaux de

séquences de tâches, et non uniquement sur une relation parent-enfant unique. Les relations multiniveaux ajoutent de la complexité, alors utilisez-les avec précaution. Les références circulaires sont toujours vérifiées dans ces relations.

#### Modèles de déploiement pour les séquences de tâches

L'Assistant Déploiement de séquences de tâches peut maintenant créer un modèle de déploiement. Celui-ci peut être enregistré et appliqué à une séquence de tâches existante ou nouvelle pour créer un déploiement.

#### Déploiements par phases pour des séquences de tâches

Les déploiements par phases sont une fonctionnalité en préversion. Les déploiements par phases automatisent le lancement coordonné et séquencé d'une séquence de tâches sur plusieurs regroupements. Vous pouvez créer des déploiements par phases avec deux phases par défaut ou configurer manuellement plusieurs phases. Le déploiement par phrases de séquences de tâches ne prend pas en charge l'installation PXE ou à partir d'un support.

## Centre logiciel

#### Installer plusieurs applications dans le Centre logiciel

Si un utilisateur final ou un technicien a besoin d'installer plusieurs applications sur un appareil, le Centre logiciel prend désormais en charge l'installation de plusieurs applications sélectionnées. Ce comportement permet à l'utilisateur de ne pas perdre de temps, car il n'est pas obligé d'attendre qu'une installation soit terminée pour commencer la suivante. Pour plus d'informations, consultez Installer plusieurs applications dans le guide utilisateur du nouveau Centre logiciel.

#### Utiliser le Centre logiciel pour parcourir et installer des applications accessibles aux utilisateurs sur des appareils joints à Azure AD

Les utilisateurs peuvent maintenant parcourir et installer les applications accessibles aux utilisateurs sur des appareils Azure Active Directory (Azure AD) en utilisant le Centre logiciel. Pour plus d'informations, consultez Déployer des applications disponibles pour l'utilisateur sur des appareils joints à Azure AD.

#### Masquer les applications installées dans le Centre logiciel

Il est maintenant possible de masquer les applications installées dans le Centre logiciel. Celles qui sont déjà installées ne s'affichent plus sous l'onglet Applications quand cette option est activée sous les paramètres clients. Cette option est définie par défaut quand vous installez ou mettez à niveau vers Configuration Manager 1802. Les applications installées sont toujours disponibles pour examen sous l'onglet de l'état d'installation. Masquer les applications installées dans le Centre logiciel contient des informations supplémentaires.

#### Masquer les applications non approuvées dans le Centre logiciel

Quand cette option est activée pour les clients, les applications disponibles pour l'utilisateur qui nécessitent une approbation sont masquées dans le Centre logiciel. Masquer les applications non approuvées dans le Centre logiciel contient des informations supplémentaires.

#### Le Centre logiciel affiche des informations de conformité supplémentaires de l'utilisateur

Lors de l'utilisation de l'état de l'attestation d'intégrité de l'appareil en tant que règle de stratégie de conformité pour l'accès conditionnel aux ressources d'entreprise, le Centre logiciel montre désormais à l'utilisateur le paramètre d'attestation d'intégrité de l'appareil qui n'est pas conforme.

## Mises à jour logicielles

#### Planifiez l'évaluation des règles de déploiement automatique pour la décaler à partir d'un jour de base.

Les règles de déploiement automatique peuvent être planifiées pour évaluer le décalage à partir d'un jour de base. Cela signifie que si le correctif Mardi tombe en fait un mercredi pour vous, vous pouvez définir le calendrier d'évaluation pour le deuxième mardi du mois avec un décalage d'un jour. Pour plus d'informations, consultez

Déployer automatiquement des mises à jour logicielles.

# Rapports

**Rapports pour le nombre de navigateurs par défaut**

Il existe maintenant un nouveau rapport qui affiche le nombre de clients ayant spécifié un certain navigateur web par défaut sous Windows. Consultez le rapport **Nombre de navigateurs par défaut** dans le groupe de rapports **Logiciel - Sociétés et produits**. Pour plus d'informations, consultez Liste des rapports.

**Générer un rapport sur les informations d'appareil Windows AutoPilot**

Windows AutoPilot est une solution permettant d'intégrer et de configurer de nouveaux appareils Windows 10 d'une manière moderne. Pour plus d'informations, consultez Vue d'ensemble de Windows AutoPilot. Pour inscrire un appareil existant auprès de Windows AutoPilot, vous pouvez charger les informations de l'appareil dans Microsoft Store pour Entreprises et Éducation : numéro de série, identificateur de produit Windows et identificateur matériel. Utilisez Configuration Manager pour collecter et communiquer ces informations sur les appareils avec le nouveau rapport, **Informations d'appareil Windows AutoPilot**, dans le nœud de rapports **Matériel - Général**. Pour plus d'informations, consultez Nouveaux appareils Windows 10 en préparation à la cogestion.

**Rapport sur les détails de la maintenance de Windows 10 pour un regroupement spécifique**

Le **rapport Détails de la maintenance de Windows 10 pour un regroupement spécifique** montre des informations générales sur la maintenance de Windows 10 pour un regroupement spécifique. Il affiche l'ID de la ressource, le nom NetBIOS, le nom du système d'exploitation et de sa version, la build, la branche du système d'exploitation et l'état du service de maintenance pour les appareils Windows 10. Pour plus d'informations, consultez Liste des rapports.

# Protéger les appareils

**Améliorations apportées aux stratégies de Configuration Manager pour Windows Defender Exploit Guard**

Des paramètres de stratégie supplémentaires pour les composants Réduction de la surface d'attaque et Accès contrôlé aux dossiers ont été ajoutés à Configuration Manager pour Windows Defender Exploit Guard.

**Nouveaux paramètres d'interaction d'hôte pour Windows Defender Application Guard**

Pour les appareils avec Windows 10 version 1709 et ultérieur, il existe deux nouveaux paramètres d'interaction d'hôte pour Windows Defender Application Guard :

- Vous pouvez autoriser les sites web à accéder au processeur graphique virtuel de l'hôte.
- Les fichiers téléchargés dans le conteneur peuvent être conservés sur l'hôte.

# Console Configuration Manager

**Améliorations apportées à la console Configuration Manager**

Cette version comprend les améliorations suivantes apportées à la console Configuration Manager.

- Les listes d'appareils sous Ressources et conformité, Appareils, affichent désormais l'utilisateur principal par défaut. Cette colonne s'affiche seulement dans le nœud Appareils. Le dernier utilisateur connecté peut également être ajouté en tant que colonne facultative. Activez les paramètres clients Affinité entre utilisateur et appareil pour le site, de façon à associer à un utilisateur principal à un appareil.
- Quand un regroupement est membre d'un autre regroupement et qu'il est renommé, le nouveau nom est mis à jour dans les règles d'adhésion.
- Lors de l'utilisation du contrôle à distance sur un client avec plusieurs moniteurs ayant une mise à l'échelle différente des ppp, le curseur de la souris est maintenant correctement mappé entre eux.
- Le tableau de bord Gestion des clients Office 365 affiche une liste des appareils concernés quand des sections

de graphe sont sélectionnées.

## Étapes suivantes

Quand vous êtes prêt à installer cette version, consultez Mises à jour pour Configuration Manager.

# Nouveautés de la version 1710 de System Center Configuration Manager

22/06/2018 • 16 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

La mise à jour 1710 de la version Current Branch de System Center Configuration Manager est une mise à jour dans la console des sites déjà installés qui exécutent la version 1610, 1702 ou 1706.

En plus des nouvelles fonctionnalités, cette version inclut également des modifications supplémentaires comme des corrections de bogues. Pour plus d'informations, consultez Récapitulatif des modifications dans Current Branch de System Center Configuration Manager version 1710.

Les mises à jour supplémentaires suivantes pour cette version sont également disponibles :

- Correctif cumulatif pour Current Branch de System Center Configuration Manager, version 1710
- Correctif cumulatif 2 pour Current Branch de System Center Configuration Manager, version 1710

> **TIP**
> Pour installer un nouveau site, vous devez utiliser une version de base de Configuration Manager.
> Informations supplémentaires :
>
> - Installation de nouveaux sites
> - Installation de mises à jour sur les sites
> - Versions de base et de mise à jour

Les sections suivantes fournissent des détails sur les modifications et les nouvelles fonctionnalités introduites dans la version 1710 de Configuration Manager.

## Infrastructure de site

**Mises à jour du Cache d'homologue**

À compter de cette version, le Cache d'homologue n'est plus une fonctionnalité en préversion. Aucune nouvelle modification n'est introduite pour le Cache d'homologue avec cette version. Pour plus d'informations, consultez Cache d'homologue pour les clients Configuration Manager.

**Prise en charge du point de distribution cloud pour le cloud Azure Government**

Vous pouvez maintenant utiliser des points de distribution cloud dans le cloud Azure Government.

**Révision de l'unité par défaut pour l'inventaire**

Les appareils étant désormais équipés de disques durs avec des tailles de plusieurs gigaoctets (Go), téraoctets (To) et plus, cette version utilise le Go (et non plus le mégaoctets (Mo)) comme unité par défaut (SMS_Units) dans de nombreux affichages. Par exemple, la valeur v_gs_LogicalDisk.FreeSpace est désormais exprimée en Go.

## Gestion des clients

**Cogestion pour les appareils Windows 10**

Dans les mises à jour précédentes de Windows 10, vous pouvez déjà joindre un appareil Windows 10 à Active Directory (AD) en local et à Azure AD sur le cloud (Azure AD hybride). À compter de Configuration Manager

version 1710, la cogestion tire parti de cette amélioration et vous permet de gérer simultanément plusieurs appareils Windows 10, version 1709 (également appelée Fall Creators Update) à l'aide de Configuration Manager et d'Intune. C'est une solution qui établit une passerelle entre la gestion classique et la gestion moderne tout en vous donnant la possibilité d'opérer cette transition selon une approche en plusieurs phases. Pour plus d'informations, consultez Cogestion pour les appareils Windows 10.

**Redémarrer les ordinateurs à partir de la console Configuration Manager**

À compter de cette version, vous pouvez utiliser la console Configuration Manager pour identifier les périphériques clients qui nécessitent un redémarrage, puis utiliser une action de notification de client pour les redémarrer.

Consultez Guide pratique pour gérer les clients dans System Center Configuration Manager

## Gestion des applications

**Améliorations de l'exécution de scripts**

Cette version apporte plusieurs améliorations à la fonctionnalité **Exécuter les scripts**, ce qui vous permet de déployer des scripts PowerShell à exécuter sur les appareils gérés. Cette fonctionnalité a été introduite dans la version 1706.

Les améliorations apportées incluent :

- Utilisation d'étendues de sécurité pour faciliter le contrôle des utilisateurs autorisés à exécuter des scripts
- Surveillance en temps réel des scripts que vous exécutez
- Paramètres d'affichage des scripts dans l'Assistant Création d'un script, validation prise en charge et identification comme étant obligatoires ou facultatifs.

Pour plus d'informations sur l'utilisation de la fonctionnalité Exécuter les scripts, consultez Créer et exécuter des scripts.

**Nouveaux paramètres de stratégie de gestion d'application mobile**

Les paramètres suivants ont été ajoutés aux paramètres de stratégie de gestion des applications mobiles :

- **Désactiver la synchronisation des contacts :** empêche l'application d'enregistrer des données sur l'application Contacts native de l'appareil.
- **Désactiver l'impression :** empêche l'application d'imprimer des données scolaires ou de travail.

**Le Centre logiciel ne déforme plus les grandes icônes aux dimensions supérieures à 250 x 250**

Avec cette version, le Centre logiciel ne déforme plus les icônes aux dimensions supérieures à 250 x 250. Auparavant, il rendait ces icônes floues. Désormais, vous pouvez définir une icône avec des dimensions maximales de 512 x 512 pixels et l'afficher sans déformation.

Pour ajouter une icône pour votre application dans le Centre logiciel, consultez Créer des applications.

## Déploiement du système d'exploitation

> **TIP**
> À compter de la version 1709 de Windows 10 (également appelée Fall Creators Update), Windows Media inclut plusieurs éditions. Quand vous configurez une séquence de tâches pour utiliser un package de mise à niveau de système d'exploitation ou une image de système d'exploitation, veillez à sélectionner une édition prise en charge par Configuration Manager.

**Ajouter des séquences de tâches enfants à une séquence de tâches**

Vous pouvez ajouter une nouvelle étape de séquence de tâches qui exécute une autre séquence de tâches, créant

ainsi une relation parent/enfant entre les séquences de tâches. Cela vous permet de créer et d'utiliser des séquences de tâches plus modulaires.

Pour plus d'informations sur la séquence de tâches enfant, consultez Séquence de tâches enfant.

## Personnalisation du Centre logiciel

Vous pouvez ajouter des éléments de personnalisation d'entreprise et spécifier la visibilité des onglets du Centre logiciel. Vous pouvez ajouter votre nom de société Centre logiciel spécifique, définir un modèle de couleurs de configuration Centre logiciel, un logo de société et les onglets visibles pour les périphériques clients.

Pour plus d'informations, consultez Planifier et configurer la gestion des applications dans System Center Configuration Manager.

## Mises à jour logicielles

**Mises à jour du pilote Surface**

À partir de cette version, la gestion des mises à jour du pilote Surface n'est plus une fonctionnalité en préversion.

## Rapports

**Limiter la télémétrie avancée dans Windows 10 pour envoyer uniquement les données pertinentes à Windows Analytics Device Health**

Vous pouvez désormais définir la collecte de données de télémétrie dans Windows 10 sur le niveau **Avancé (limité)**. Ce paramètre vous permet d'obtenir un insight actionnable sur les périphériques de votre environnement sans que ces derniers aient à envoyer toutes les données au niveau de télémétrie **Avancé** avec Windows 10 version 1709 ou ultérieure.

Pour plus d'informations, consultez Guide pratique pour configurer les paramètres client dans System Center Configuration Manager.

## Gestion des appareils mobiles

**Actions en cas de non-conformité**

Vous pouvez désormais configurer une séquence chronologique d'actions appliquées aux appareils qui ne sont pas conformes. Par exemple, vous pouvez notifier les utilisateurs d'appareils non conformes par e-mail ou marquer ces appareils comme non conformes. Pour plus d'informations, consultez Configurer des actions en cas de non-conformité.

**Prise en charge des appareils Windows 10 ARM64**

Les scénarios de gestion hybride des appareils mobiles seront pris en charge sur les appareils ARM64 exécutant Windows 10 quand ces appareils seront disponibles.

Ces scénarios sont les suivants :

- Inscrire des appareils
- Effectuer des actions de réinitialisation complète à distance et sélective
- Gérer des paramètres via des éléments de configuration et des lignes de base
- Gérer la stratégie de conformité et l'accès conditionnel
- Activer l'accès aux ressources de l'entreprise par le biais de :
  - Profils de certificat
  - Profils VPN
  - Profils Wi-Fi
  - Profils de messagerie

- Configurer une stratégie Windows Hello Entreprise
- Gérer les applications

> **NOTE**
> Le déploiement d'applications .appxbundle générées pour plusieurs architectures peuvent ne pas fonctionner sur ces appareils, et ce scénario n'est pas pris en charge pour l'instant.

**Expérience de profil VPN améliorée dans la console Configuration Manager**

Avec cette version, nous avons mis à jour l'Assistant Création d'un profil VPN et les pages de propriétés pour afficher uniquement les paramètres appropriés à la plateforme sélectionnée :

- Chaque plateforme a son propre flux de travail, ce qui signifie que les nouveaux profils VPN ne contiennent que les paramètres pris en charge par la plateforme.
- La page **Plateformes prises en charge** apparaît désormais après la page **Général**. Maintenant, vous choisissez la plateforme avant de définir les valeurs de propriété.
- Lorsque la plateforme est définie sur **Android**, **Android for Work** ou **Windows Phone 8.1**, la page **Plateformes prises en charge** est inutile et ne s'affiche pas.
- Le flux de travail du client Configuration Manager a été combiné aux flux de travail Windows 10 du client de l'appareil mobile hybride (MDM) ; ils prennent en charge les mêmes paramètres.
- Chaque flux de travail de plateforme inclut uniquement les paramètres appropriés à ce flux de travail. Par exemple, le flux de travail Android contient les paramètres propres à Android ; les paramètres appropriés pour iOS ou Windows 10 Mobile n'apparaissent donc plus dans le flux de travail Android.
- La page VPN automatique est obsolète et a été supprimée.

Ces modifications s'appliquent aux nouveaux profils VPN.

Pour réduire les problèmes de compatibilité, les profils VPN existants restent inchangés. Lorsque vous modifiez un profil existant, les paramètres s'affichent comme au moment de sa création.

Pour plus d'informations, consultez Profils VPN sur des appareils mobiles dans System Center Configuration Manager.

**Prise en charge limitée des certificats Cryptography : Next Generation (CNG)**

Configuration Manager prend en charge les certificats Cryptography : Next Generation (CNG) de manière limitée. Les clients Configuration Manager peuvent utiliser un certificat d'authentification client PKI avec une clé privée dans le fournisseur de stockage de clés (KSP) CNG. La prise en charge du KSP permet aux clients Configuration Manager de prendre en charge une clé privée matérielle, comme TPM KSP pour les certificats d'authentification client PKI.

Pour plus d'informations, consultez Vue d'ensemble des certificats CNG.

# Protéger les appareils

**Créer et déployer des stratégies Exploit Guard**

Vous pouvez créer et déployer des stratégies qui gèrent les quatre composants de Windows Defender Exploit Guard, à savoir la réduction de la surface d'attaque, l'accès contrôlé aux dossiers, Exploit Protection et la protection du réseau.

**Créer et déployer une stratégie Windows Defender Application Guard**

Vous pouvez créer et déployer des stratégies Windows Defender Application Guard à l'aide de la protection du point de terminaison Configuration Manager.

**Modifications des stratégies Device Guard**

Les trois modifications suivantes ont été apportées au niveau des stratégies Device Guard :

- Les stratégies Device Guard s'appellent désormais les stratégies Windows Defender Application Control. Ainsi, par exemple, l'**Assistant Créer une stratégie Device Guard** s'appelle désormais l'**Assistant Créer une stratégie Windows Defender Application Control**.
- Les appareils qui utilisent Fall Creators Update pour Windows version 1709 n'ont pas besoin de redémarrage pour appliquer les stratégies Windows Defender Application Control. Le redémarrage est toujours la valeur par défaut, mais vous pouvez désactiver les redémarrages.
- Vous pouvez définir les appareils pour qu'ils exécutent automatiquement les logiciels approuvés par Intelligent Security Graph.

## Étapes suivantes

Quand vous êtes prêt à installer cette version, consultez Mises à jour pour Configuration Manager.

# Nouveautés de la version 1706 de System Center Configuration Manager

22/06/2018 • 24 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

La mise à jour 1706 de la version Current Branch de System Center Configuration Manager est une mise à jour dans la console des sites déjà installés qui exécutent la version 1606, 1610 ou 1702.

> **TIP**
> Pour installer un nouveau site, vous devez utiliser une version de base de Configuration Manager.
> Informations supplémentaires :
>
> - Installation de nouveaux sites
> - Installation de mises à jour sur les sites
> - Versions de base et de mise à jour

Les sections suivantes fournissent des détails sur les nouvelles fonctionnalités et les changements introduits dans la version 1706 de Configuration Manager.

## Infrastructure de site

**Prise en charge du cache d'homologue client pour les fichiers d'installation rapide de Windows 10 et Office 365**

À partir de cette version, le cache d'homologue prend en charge la distribution des fichiers d'installation rapide de Windows 10 et des fichiers de mise à jour d'Office 365. Aucune configuration supplémentaire n'est nécessaire pour prendre en charge ce changement.

**Mises à jour de l'entrepôt de données**

L'entrepôt de données n'est plus une fonctionnalité en préversion. Nous avons également mis à jour les prérequis pour prendre en charge la base de données sur les groupes de disponibilité SQL Server Always On et les clusters de basculement. Pour en savoir plus, consultez la section relative au point de service de l'entrepôt de données.

**Améliorations d'accessibilité**

Des améliorations supplémentaires ont été apportées aux fonctionnalités d'accessibilité de la console Configuration Manager. Pour plus d'informations, consultez Fonctionnalités d'accessibilité.

**Améliorations pour les groupes de disponibilité Always On SQL Server**

Avec cette version, vous pouvez maintenant utiliser les réplicas avec validation asynchrone dans les groupes de disponibilité Always On SQL Server que vous utilisez avec Configuration Manager. Cela signifie que vous pouvez ajouter des réplicas supplémentaires à vos groupes de disponibilité à utiliser en tant que sauvegardes hors site (à distance) puis de les utiliser dans un scénario de récupération d'urgence.

- Configuration Manager prend en charge l'utilisation du réplica avec validation asynchrone pour récupérer votre réplica synchrone. Consultez les options de récupération de base de données de site dans la rubrique Sauvegarde et récupération pour plus d'informations sur la façon d'y parvenir.
- Cette version ne prend pas en charge le basculement pour utiliser le réplica avec validation asynchrone en tant que base de données de votre site. Pour plus d'informations, consultez Se préparer à l'utilisation de groupes de disponibilité SQL Server Always On.

**Outil de réinitialisation des mises à jour**

À compter de la version 1706, les sites d'administration centrale et les sites principaux Configuration Manager incluent l'outil de réinitialisation des mises à jour Configuration Manager (**CMUpdateReset.exe**). Utilisez cet outil avec n'importe quelle version de Current Branch prise en charge pour résoudre les problèmes de téléchargement ou de réplication des mises à jour dans la console. Pour plus d'informations, consultez Outil de réinitialisation des mises à jour.

**Prise en charge des consoles à résolution élevée**

Avec cette version, les problèmes liés à la façon dont la console Configuration Manager met à l'échelle et affiche les différentes parties de l'interface utilisateur lors de son affichage sur des appareils à résolution élevée (comme un livre) devraient être corrigés.

**Améliorations des groupes de limites pour les points de mise à jour logicielle**

Cette version inclut des améliorations pour le fonctionnement des points de mise à jour logicielle avec des groupes de limites. Voici qui résume le nouveau comportement de secours :

- L'action de secours pour les points de mise à jour logicielle utilise désormais un temps configurable pour le repli sur les groupes de limites voisins.
- Indépendamment de la configuration de secours, un client essaie d'atteindre le dernier point de mise à jour logicielle qu'il a utilisé pendant 120 minutes. Après l'échec de communication avec ce serveur pendant 120 minutes, le client vérifie ensuite son pool de points de mise à jour logicielle disponibles, afin d'en trouver un nouveau.
- Après avoir échoué pendant deux heures à atteindre le serveur d'origine, le client passe à un cycle plus court pour contacter un nouveau point de mise à jour logicielle. Cela signifie que si un client ne parvient pas à se connecter avec un nouveau serveur, il sélectionne rapidement le serveur suivant à partir de son pool de serveurs disponibles et tente de le contacter.

Pour plus d'informations, consultez la section Points de mise à jour logicielle dans la rubrique Groupes de limites pour Current Branch.

**Intégration d'Azure AD à Configuration Manager**

Dans cette version, nous avons amélioré l'intégration de Configuration Manager et d'Azure Active Directory (Azure AD). Ces améliorations simplifient non seulement la configuration des services Azure que vous utilisez avec Configuration Manager, mais aussi la gestion des clients et des utilisateurs qui s'authentifient par le biais d'Azure AD.

Grâce à l'intégration améliorée, les opérations suivantes sont possibles :

- Assistant Services Azure : cet Assistant propose une expérience de configuration commune qui remplace les différents flux de travail associés à la configuration des services Azure suivants que vous utilisez avec Configuration Manager.
  - **Gestion cloud** Donnez aux clients la possibilité de s'authentifier à l'aide d'Azure Active Directory (Azure AD). Vous pouvez également configurer la découverte des utilisateurs Azure AD.
  - **Connecteur OMS** Connectez-vous à Operations Manager Suite (OMS) et synchronisez les données telles que les collections à OMS Log Analytics.
  - **Upgrade Readiness** Connectez-vous à Upgrade Readiness et consultez les données de compatibilité de mise à niveau des clients.
  - **Microsoft Store pour Entreprises** Connectez-vous au Microsoft Store pour Entreprises et obtenez des applications pour votre organisation que vous pouvez déployer avec Configuration Manager.

Pour cela, une application web serveur Azure fournit les détails de l'abonnement et de la configuration, ce qui vous évite de les entrer chaque fois que vous configurez un nouveau service ou composant Configuration Manager avec Azure. Pour plus d'informations, consultez Assistant Services Azure.

- Utilisez Azure AD pour authentifier les clients sur Internet et leur permettre d'accéder à vos sites Configuration Manager. Azure AD élimine le besoin de configurer et d'utiliser des certificats d'authentification client. Vous devez pour cela utiliser le rôle de système de site Passerelle de gestion cloud. Pour plus d'informations, consultez Installer et attribuer des clients Configuration Manager à partir d'Internet à l'aide de l'authentification Azure AD.

- Installez et gérez le client Configuration Manager sur les ordinateurs qui se trouvent sur Internet. Vous devez pour cela utiliser le rôle de système de site Passerelle de gestion cloud. Pour plus d'informations, consultez Installer et attribuer des clients Configuration Manager à partir d'Internet à l'aide de l'authentification Azure AD.

- Configurer la découverte des utilisateurs Azure AD. Utilisez l'Assistant Services Azure pour configurer cette nouvelle méthode de découverte. Cette nouvelle méthode exécute une requête sur votre annuaire Azure AD pour extraire des données utilisateur que vous pouvez utiliser avec vos données de découverte traditionnelles. La synchronisation complète et la synchronisation delta sont prises en charge. Pour plus d'informations, consultez Découverte d'utilisateurs Azure AD.

#### Améliorations du cache d'homologue

Le cache d'homologue n'utilise plus le compte d'accès réseau pour authentifier les demandes de téléchargement à partir d'homologues. Cela pose problème quand les clients ont besoin de ce compte. Il est en effet exigé par les clients qui démarrent dans WinPE et qui accèdent ensuite au contenu à partir d'une source de cache d'homologue. Pour plus d'informations, consultez Exigences et considérations relatives au cache d'homologue.

## Paramètres de conformité

#### Nouveaux paramètres de configuration pour les appareils Windows 10 qui ne sont pas gérés avec le client Configuration Manager

Dans cette version, nous avons ajouté de nouveaux paramètres de configuration pour les appareils Windows 10 inscrits auprès d'Intune ou gérés localement par Configuration Manager. Ces paramètres sont les suivants :

- **Mot de passe**
  - Chiffrement de l'appareil
- **Appareil**
  - Modification des paramètres de région (Desktop uniquement)
  - Modification des paramètres d'alimentation et de mise en veille
  - Modification des paramètres de langue
  - Modification de l'heure du système
  - Modification du nom de l'appareil
- **Store**
  - Mettre à jour automatiquement les applications du store
  - Utiliser uniquement un store privé
  - Lancement des applications provenant du store
- **Microsoft Edge**
  - Bloquer l'accès à about:flags
  - Remplacement de l'invite SmartScreen
  - Remplacement de l'invite SmartScreen pour les fichiers
  - Adresse IP localhost WebRTC
  - Moteur de recherche par défaut
  - URL OpenSearch XML
  - Pages d'accueil (Desktop uniquement)

Pour plus de détails sur tous les paramètres de Windows 10, consultez Comment créer des éléments de

configuration pour des appareils Windows 8.1 et Windows 10 gérés sans le client System Center Configuration Manager.

**Nouvelles règles de stratégie de conformité d'appareil**

- **Type de mot de passe requis**. Spécifie si les utilisateurs doivent créer un mot de passe de type alphanumérique ou numérique. Pour les mots de passe alphanumériques, vous spécifiez également le nombre minimal de jeux de caractères que le mot de passe doit avoir. Les quatre jeux de caractères sont : lettres minuscules, lettres majuscules, symboles et chiffres.

  **Pris en charge sur :**

  - Windows Phone 8+
  - Windows 8.1+
  - iOS 6+
- **Bloquer le débogage USB sur l'appareil**. Vous n'avez pas à configurer ce paramètre, car le débogage USB est déjà désactivé pour les appareils Android for Work.

  **Pris en charge sur :**

  - Android 4.0+
  - Samsung KNOX Standard 4.0+
- **Bloquer les applications provenant de sources inconnues**. Exiger que les appareils interdisent l'installation des applications provenant de sources inconnues. Vous n'avez pas à configurer ce paramètre, car les appareils Android for Work limitent toujours l'installation à partir de sources inconnues.

  **Pris en charge sur :**

  - Android 4.0+
  - Samsung KNOX Standard 4.0+
- **Exiger l'analyse des menaces sur les applications**. Ce paramètre spécifie que la fonction Vérifier les applications est activée sur l'appareil.

  **Pris en charge sur :**

  - Android 4.2 à 4.4
  - Samsung KNOX Standard 4.0+

Pour essayer les nouvelles règles de conformité d'appareil, consultez Créer et déployer une stratégie de conformité d'appareil.

## Gestion des applications

**Exécuter des scripts PowerShell à partir de la console Configuration Manager**

Dans Configuration Manager, vous pouvez déployer des scripts sur des appareils clients à l'aide de packages et de programmes. Dans cette version, nous avons ajouté de nouvelles fonctionnalités qui vous permettent d'effectuer les actions suivantes :

- Importer des scripts PowerShell dans Configuration Manager
- Modifier les scripts à partir de la console Configuration Manager (pour les scripts non signés uniquement)
- Marquer les scripts comme Approuvés ou Refusés pour améliorer la sécurité
- Exécuter des scripts sur des collections d'ordinateurs clients Windows, et des ordinateurs Windows gérés localement. Vous ne pouvez pas déployer des scripts : ils sont exécutés en temps quasi réel sur les appareils clients.
- Examinez les résultats retournés par le script dans la console Configuration Manager.

Pour plus d'informations, consultez Créer et exécuter des scripts PowerShell à partir de la console Configuration Manager.

#### Nouveaux paramètres de stratégie de gestion d'application mobile

À partir de cette version, vous pouvez utiliser trois nouveaux paramètres de stratégie de gestion des applications mobiles (MAM) :

- **Bloquer la capture d'écran (appareils Android uniquement)** : spécifie que les fonctionnalités de capture d'écran de l'appareil sont bloquées lors de l'utilisation de cette application.

Consultez Protéger les applications à l'aide des stratégies de protection des applications de Configuration Manager pour essayer de nouveaux paramètres de stratégie de protection d'application.

## Déploiement du système d'exploitation

#### L'inventaire matériel collecte des informations sur le démarrage sécurisé

L'inventaire matériel collecte désormais des informations indiquant si le démarrage sécurisé est activé sur les clients. Ces informations sont stockées dans la classe **SMS_Firmware** (introduite dans la version 1702) et activées dans l'inventaire matériel par défaut. Pour plus d'informations sur l'inventaire matériel, consultez Guide pratique pour configurer l'inventaire matériel.

#### Groupes de séquences de tâches réductibles

Cette version permet de développer et réduire des groupes de séquences de tâches. Vous pouvez développer ou réduire des groupes individuels ou tous les groupes à la fois.

#### Recharger les images de démarrage avec la version actuelle de Windows PE

Lorsque vous exécutez l'option **Mise à jour des points de distribution** sur une image de démarrage sélectionnée, vous pouvez maintenant choisir de recharger la dernière version de Windows PE (depuis le répertoire d'installation de Windows ADK) dans l'image de démarrage. Pour plus d'informations, consultez Mettre à jour des points de distribution avec l'image de démarrage.

## Mises à jour logicielles

#### Amélioration de la durée de téléchargement des mises à jour rapides

Dans cette version, nous avons considérablement amélioré la durée de téléchargement des mises à jour rapides. Pour plus d'informations, consultez Gérer les fichiers d'installation rapide pour les mises à jour de Windows 10.

#### Gérer les mises à jour du pilote Microsoft Surface

Vous pouvez maintenant utiliser Configuration Manager pour gérer les mises à jour du pilote Microsoft Surface.

##### Prérequis

- Tous les points de mise à jour logicielle doivent exécuter Windows Server 2016.
- Il s'agit d'une fonctionnalité en préversion que vous devez activer pour pouvoir y accéder. Pour plus d'informations, consultez Utiliser des fonctionnalités de préversions de mises à jour.

##### Pour gérer les mises à jour du pilote Surface

1. Activer la synchronisation pour les pilotes Microsoft Surface. Utilisez la procédure décrite dans Configurer la classification et les produits et cochez la case **Inclure les mises à jour du microprogramme et des pilotes Microsoft Surface** sous l'onglet **Classifications** pour activer les pilotes Surface.
2. Synchroniser les pilotes Microsoft Surface.
3. Déployer des pilotes Microsoft Surface synchronisés

#### Configuration de Windows Update pour les stratégies d'entreprise de report d'entreprise

Vous pouvez maintenant configurer des stratégies de report pour les appareils Windows 10 avec mises à jour de

fonctionnalités ou de qualité gérés directement par Windows Update for Business. Vous pouvez gérer les stratégies de report du nouveau nœud **Stratégies Windows Update for Business** sous **Bibliothèque de logiciels** > **Maintenance de Windows 10**.

Pour plus d'informations, consultez Intégration à Windows Update for Business dans Windows 10.

#### Amélioration des notifications à l'utilisateur pour les mises à jour d'Office 365

Des améliorations ont été apportées pour tirer parti de l'expérience utilisateur « Cliquer pour exécuter » d'Office lorsqu'un client installe une mise à jour d'Office 365. Cela inclut des fenêtres contextuelles et des notifications dans l'application, ainsi qu'une expérience de compte à rebours. Pour plus d'informations, consultez Comportement de redémarrage et notifications des clients pour les mises à jour d'Office 365.

## Rapports

#### Utiliser Windows Analytics avec Configuration Manager

Windows Analytics est un ensemble de solutions qui s'exécutent sur Operations Management Suite. Les solutions vous permettent d'obtenir des insights sur l'état actuel de votre environnement. Les appareils de votre environnement envoient des données de télémétrie Windows. Ces données sont accessibles par le biais du portail web Operations Management Suite. Dans le cadre d'Upgrade Readiness, les données sont directement disponibles dans le nœud de surveillance de la console Configuration Manager.

Pour plus d'informations, consultez Utiliser Windows Analytics avec Configuration Manager.

## Gestion des appareils mobiles

#### Mises à jour apportées à la configuration de partage Android for Work

Dans cette version, les valeurs du paramètre **Autoriser le partage de données entre les profils professionnel et personnel** dans le groupe de paramètres **Profil professionnel** ont été mises à jour. Nous avons également ajouté un paramètre personnalisé pour bloquer les opérations copier-coller entre les profils professionnels et personnels.

Pour plus d'informations, consultez Éléments de configuration pour les appareils Android for Work.

#### Restrictions de l'inscription Android et iOS

Avec cette version, vous pouvez à présent spécifier que les utilisateurs ne peuvent pas inscrire des appareils Android ou iOS personnels. Les nouveaux paramètres de restriction des appareils permettent de limiter l'inscription des appareils Android aux appareils prédéclarés. Pour les appareils iOS, vous pouvez bloquer l'inscription de tous les appareils à l'exception de ceux qui sont inscrits auprès du Programme d'inscription des appareils d'Apple, d'Apple Configurator ou du compte du gestionnaire d'inscription des appareils Intune.

- Pour plus d'informations sur les restrictions d'inscription Android, consultez la page Configurer la gestion des appareils Android.
- Pour plus d'informations sur les restrictions d'inscription iOS, consultez la page Configurer des restrictions d'inscription iOS.

## Protéger les appareils

#### Inclure la confiance pour des fichiers et dossiers spécifiques dans une stratégie de protection des appareils

Dans cette version, nous avons ajouté des fonctionnalités supplémentaires à la gestion des stratégies Device Guard.

Vous pouvez éventuellement ajouter l'approbation pour des fichiers spécifiques pour les dossiers dans une stratégie Device Guard. Cela vous permet de :

- Résoudre les problèmes avec les comportements des programmes d'installation gérés

- Approuver les applications métier qui ne peuvent pas être déployées avec Configuration Manager
- Approuver des applications qui sont incluses dans une image de déploiement de système d'exploitation

Pour plus d'informations, consultez Gestion de Device Guard avec Configuration Manager.

# Éléments supprimés et dépréciés dans System Center Configuration Manager

22/06/2018 • 3 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cet article décrit comment utiliser les informations des fonctionnalités, produits et systèmes d'exploitation supprimés de la prise en charge dans System Center Configuration Manager, ou qui seront supprimés dans une prochaine mise à jour (dépréciés). Il annonce les changements à venir qui pourraient affecter votre utilisation de Configuration Manager.

Ces informations peuvent faire l'objet de modifications dans les futures versions et ne pas inclure chaque fonctionnalité, produit ou système d'exploitation déprécié.

## Utilisation de ces informations

Quand une fonctionnalité, un produit ou un système d'exploitation est répertorié pour la première fois comme étant déprécié, sa prise en charge dans Configuration Manager sera supprimée dans une version future de Configuration Manager. Ces informations sont fournies pour vous permettre de planifier des alternatives à l'utilisation de cette fonctionnalité ou de ce système d'exploitation. Cet article est mis à jour à la publication de la première version de Configuration Manager dans laquelle la prise en charge est supprimée.

Quand la prise en charge d'une fonctionnalité ou d'un système d'exploitation est supprimée, la fonctionnalité ou le système d'exploitation continuent d'être pris en charge dans les versions antérieures de Configuration Manager aussi longtemps que celles-ci restent prise en charge. Cependant, quand vous utilisez une version de Configuration Manager publiée après la date ou la version indiquée, cette version de Configuration Manager ne fournit pas de prise en charge.

Par exemple, si la suppression de la prise en charge d'une fonctionnalité a été planifiée dans la première mise à jour publiée après septembre 2016, la prise en charge de cette fonctionnalité n'est plus incluse dans la mise à jour 1610, publiée en octobre 2016.

- Avec la mise à jour 1610, la fonctionnalité ne serait ainsi plus prise en charge.
- Cet article serait mis à jour pour indiquer que la prise en charge a été supprimée avec la version 1610. Cependant, si vous continuez à utiliser une version antérieure qui prend en charge la fonctionnalité, comme la version 1602 ou 1606, vous pouvez continuer à utiliser cette fonctionnalité, jusqu'à ce que la version que vous utilisez supprime la prise en charge.

## Éléments supprimés et dépréciés dans Configuration Manager

Les éléments supprimés ou dépréciés sont répartis en trois catégories.

**Fonctionnalités Configuration Manager supprimées et dépréciées**

**Éléments supprimés et dépréciés pour les serveurs de site Configuration Manager**

**Éléments supprimés et dépréciés pour les clients Configuration Manager**

## Plus d'informations

Pour plus d'informations, voir :

- Le site web Politique de support Microsoft.
- Prise en charge des versions Current Branch de System Center Configuration Manager.

# Fonctionnalités supprimées et déconseillées dans System Center Configuration Manager

22/06/2018 • 6 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cet article liste les fonctionnalités dépréciées ou supprimées du support de Configuration Manager. Les fonctionnalités dépréciées seront supprimées dans une prochaine mise à jour. Ces futurs changements risquent d'affecter votre utilisation de Configuration Manager.

Ces informations sont susceptibles de changer dans les futures versions. Les fonctionnalités Configuration Manager dépréciées ne sont peut-être pas toutes listées ici.

## Fonctionnalités dépréciées

| FONCTIONNALITÉ | DÉPRÉCIATION ANNONCÉE | PRISE EN CHARGE SUPPRIMÉE |
|---|---|---|
| Les applications à la disposition des utilisateurs qui figuraient uniquement dans le catalogue d'applications apparaissent maintenant dans le nouveau Centre logiciel.<br>Par conséquent, l'expérience de catalogue d'applications web ne sera pas disponible dans les prochains mois. | 11 août 2017 | Fin de la prise en charge de l'expérience utilisateur du site web du catalogue d'applications avec la première mise à jour publiée après le 1er juin 2018 |
| Ancienne version du Centre logiciel.<br><br>Pour plus d'informations sur le nouveau Centre logiciel, consultez Planifier et configurer la gestion des applications. | 13 décembre 2016 | Version 1802 |
| Gestion de disques durs virtuels avec Configuration Manager.<br>Cette dépréciation inclut la suppression des options permettant de créer un nouveau disque dur virtuel ou de gérer un disque dur virtuel à l'aide d'une séquence de tâches, ainsi que la suppression du nœud Disques durs virtuels dans la console Configuration Manager.<br><br>Les disques durs virtuels existants ne sont pas supprimés, mais ne sont plus accessibles à partir de la console Configuration Manager. | 6 janvier 2017 | Version 1710 |
| Séquences de tâches :<br>- Convertir en disque dynamique<br>- Installer les outils de déploiement | 18 novembre 2016 | Version 1710 |

| FONCTIONNALITÉ | DÉPRÉCIATION ANNONCÉE | PRISE EN CHARGE SUPPRIMÉE |
|---|---|---|
| Outil d'évaluation de mise à niveau System Center Configuration Manager. L'outil d'évaluation de mise à niveau dépend à la fois de System Center Configuration Manager et des outils d'analyse de compatibilité des applications (ACT) 6.x. La dernière version d'ACT a été intégrée à Windows 10 v1511 ADK. Comme il n'y a plus aucune mise à jour d'ACT, la prise en charge de l'outil d'évaluation de mise à niveau prend fin.<br><br>L'outil d'évaluation de mise à niveau est remplacé par la fonctionnalité Disponibilité pour la mise à niveau. Une note de dépréciation a été ajoutée à la page de téléchargement UAT le 12 septembre 2016. | 12 septembre 2016 | 11 juillet 2017 |
| Séquences de tâches :<br>- OSDPreserveDriveLetter<br><br>Lors d'un déploiement de système d'exploitation, par défaut, le programme d'installation Windows détermine désormais la meilleure lettre de lecteur à utiliser (généralement C:). Si vous souhaitez spécifier un autre lecteur à utiliser, vous pouvez modifier l'emplacement dans l'étape de séquence de tâches Appliquer le système d'exploitation. Accédez au paramètre **Sélectionnez l'emplacement où vous souhaitez appliquer ce système d'exploitation**. Sélectionnez **Lettre de lecteur logique spécifique** et choisissez le lecteur que vous souhaitez utiliser. | 20 juin 2016 | Version 1606 |
| Protection d'accès réseau (NAP) : telle que dans System Center 2012 Configuration Manager | 10 juillet 2015 | Version 1511 |
| Gestion hors bande : telle que dans System Center 2012 Configuration Manager | 16 octobre 2015 | Version 1511 |

# Fonctionnalités supprimées dans la version 1511

Les sections suivantes contiennent des détails supplémentaires sur les fonctionnalités supprimées avec la version 1511 :

### Gestion hors bande

Avec Configuration Manager, la prise en charge native des ordinateurs AMT à partir de la console Configuration Manager est supprimée.

- Les ordinateurs AMT restent entièrement gérés quand vous utilisez le module complémentaire Intel SCS

pour Microsoft System Center Configuration Manager. Ce module complémentaire vous permet d'accéder aux dernières fonctionnalités permettant de gérer AMT tout en supprimant les limitations introduites jusqu'à ce que Configuration Manager puisse intégrer ces changements.

- La gestion hors bande dans System Center 2012 Configuration Manager n'est pas affectée par cette modification.

**Protection d'accès au réseau**

System Center Configuration Manager ne prend pas en charge la protection d'accès réseau. La fonctionnalité est dépréciée dans Windows Server 2012 R2 et a été supprimée dans Windows 10.

Pour les solutions de protection d'accès réseau, consultez la section *Fonctionnalités déconseillées* dans Vue d'ensemble des services de stratégie et d'accès réseau.

## Plus d'informations

Pour plus d'informations, voir :

- Supprimé et déprécié
- Politique de support Microsoft
- Prise en charge des versions Current Branch de System Center Configuration Manager.

# Supprimé et déprécié pour les serveurs de site System Center Configuration Manager

22/06/2018 • 4 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cet article décrit les produits et systèmes d'exploitation supprimés de la prise en charge dans les serveurs de site System Center Configuration Manager ou qui seront supprimés dans une prochaine mise à jour (dépréciés). Il annonce les changements à venir qui pourraient affecter votre utilisation de Configuration Manager.

Ces informations peuvent faire l'objet de modifications dans les futures versions et ne pas inclure chaque fonctionnalité, produit ou système d'exploitation déprécié.

## Systèmes d'exploitation serveur dépréciés

| SYSTÈMES D'EXPLOITATION | PREMIÈRE ANNONCE DE DÉPRÉCIATION | SUPPORT SUPPRIMÉ |
|---|---|---|
| Windows Server 2008 R2 | 10 juillet 2015 | Version 1702 (voir la remarque 1) |
| Windows Server 2008 | 10 juillet 2015 | Version 1511<br>Le support prend fin quand un système de site est supprimé (Voir la remarque 2). |

**NOTE**

- À compter de la version 1702, Windows Server 2008 R2 n'est pas pris en charge pour les serveurs de site ou la plupart des rôles de système de site. Toutefois, les versions antérieures à 1702 continuent de prendre en charge son utilisation. Ce système d'exploitation reste pris en charge pour le rôle de système de site de point de distribution (y compris les points de distribution d'extraction, ainsi que pour PXE et la multidiffusion) jusqu'à l'annonce de la dépréciation de cette prise en charge ou jusqu'à l'expiration du support étendu de ce système d'exploitation. À compter de la version 1602, vous pouvez mettre à niveau sur place le système d'exploitation d'un serveur de site de Windows Server 2008 R2 vers Windows Server 2012 R2.
- Pour plus d'informations sur la mise à niveau sur place d'un système d'exploitation de serveurs de site, consultez la section Mise à niveau sur place du système d'exploitation des serveurs de site qui exécutent Windows Server 2008 R2 dans Mettre à niveau l'infrastructure locale qui prend en charge System Center Configuration Manager.

**NOTE**

- Windows Server 2008 n'est pas pris en charge pour les serveurs de site ou les rôles de système de site, à l'exception du point de distribution et du point de distribution d'extraction. Vous pouvez continuer à utiliser ce système d'exploitation comme point de distribution jusqu'à l'annonce de la dépréciation de la prise en charge ou jusqu'à l'expiration du support étendu de ce système d'exploitation. Pour plus d'informations, consultez Échec de l'installation de System Center Configuration Manager CB et LTSB sur Windows Server 2008.

## Support déprécié pour les versions de SQL Server en tant que base de données de site

| VERSIONS DE SQL SERVER | PREMIÈRE ANNONCE DE DÉPRÉCIATION | SUPPORT SUPPRIMÉ |
|---|---|---|
| SQL Server 2008 R2 | 10 juillet 2015 | Version 1702 |
| SQL Server 2008 | 10 juillet 2015 | Version 1511 |

Si vous devez mettre à niveau votre version de SQL Server, nous vous recommandons les méthodes suivantes, de la plus simple à la plus complexe.

1. Mise à niveau de SQL Server sur place (recommandé).
2. Installez une nouvelle version de SQL Server sur un nouvel ordinateur. Ensuite, utilisez l'option de déplacement de la base de données du programme d'installation de Configuration Manager pour pointer votre serveur de site vers la nouvelle version de SQL Server.
3. Utilisez la sauvegarde et la récupération.

## Plus d'informations

Pour plus d'informations, voir :

- Supprimé et déprécié
- Le site web Politique de support Microsoft.
- Prise en charge des versions Current Branch de System Center Configuration Manager.

# Éléments supprimés et dépréciés pour les clients System Center Configuration Manager

22/06/2018 • 3 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cet article décrit les produits et systèmes d'exploitation supprimés de la prise en charge dans les clients System Center Configuration Manager ou qui seront supprimés dans une prochaine mise à jour (dépréciés). Il annonce les changements à venir qui pourraient affecter votre utilisation de Configuration Manager.

Ces informations peuvent faire l'objet de modifications dans les futures versions et ne pas inclure chaque fonctionnalité, produit ou système d'exploitation déprécié.

## Systèmes d'exploitation client dépréciés

Sauf indication contraire, chaque système d'exploitation pris en charge en tant que client Configuration Manager est pris en charge jusqu'à sa date de fin de support étendu. Pour plus d'informations sur les dates de fin du support étendu, consultez la Politique de support Microsoft. Si la prise en charge de Configuration Manager pour un système d'exploitation se termine avant la date de fin du support étendu, une date de dépréciation et une date de suppression de la prise en charge de ce système d'exploitation sont mentionnées ici.

| SYSTÈMES D'EXPLOITATION | PREMIÈRE ANNONCE DE DÉPRÉCIATION | SUPPORT SUPPRIMÉ |
|---|---|---|
| Linux et UNIX | 22 mars 2018 | |
| Windows 8 : Professionnel, Entreprise | 12 janvier 2018 | |
| Windows Embedded 8 Pro | 12 janvier 2018 | |
| Windows Embedded 8 Industry | 12 janvier 2018 | |
| Windows XP Embedded<br><br>Comprend tous les systèmes d'exploitation embarqués basés sur XP. | 10 juillet 2015 | Version 1702 |
| Windows Vista | 10 juillet 2015 | Version 1511 |
| Windows Server 2003 R2 | 10 juillet 2015 | Version 1511 |
| Windows Server 2003 | 10 juillet 2015 | Version 1511 |
| Windows XP | 10 juillet 2015 | Version 1511 |
| Mac OS X 10.6 - 10.8 | 10 juillet 2015 | Version 1511 |
| Windows Mobile 6.0 - 6.5 | 10 juillet 2015 | Version 1511 |
| Nokia Symbian Belle | 10 juillet 2015 | Version 1511 |

| SYSTÈMES D'EXPLOITATION | PREMIÈRE ANNONCE DE DÉPRÉCIATION | SUPPORT SUPPRIMÉ |
| --- | --- | --- |
| Windows CE 5.0 - 6.0 | 10 juillet 2015 | Version 1511 |

## Plus d'informations

Pour plus d'informations, voir :

- Supprimé et déprécié
- Le site web Politique de support Microsoft.
- Prise en charge des versions Current Branch de System Center Configuration Manager.

# Configurations prises en charge pour System Center Configuration Manager

22/06/2018 • 5 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Comme solution locale, System Center Configuration Manager utilise vos serveurs, clients, configurations réseau et autres produits tels que Microsoft Intune, SQL Server et Azure.

La présente rubrique et les rubriques suivantes fournissent des informations essentielles pour vous aider à déterminer les principales configurations, exigences et limitations à prendre en compte pour planifier, installer et gérer un déploiement de Configuration Manager pleinement opérationnel. Ces informations sont propres à l'infrastructure des sites, hiérarchies et appareils gérés de Configuration Manager.

Quand une fonctionnalité Configuration Manager nécessite des configurations particulières, ces informations sont fournies dans la documentation de la fonctionnalité, venant ainsi compléter les informations de configuration plus générales.

Les produits et les technologies qui sont décrits dans les rubriques suivantes sont pris en charge par Configuration Manager. Toutefois, leur inclusion dans ce contenu n'implique pas une extension de prise en charge des produits au-delà de leur cycle de vie individuel. L'utilisation de produits qui ont dépassé leur cycle de vie n'est pas prise en charge avec Configuration Manager. Pour plus d'informations sur les politiques de support Microsoft, consultez le site web Politique de support Microsoft .

> **NOTE**
> Pour plus d'informations sur la politique de support Microsoft, consultez le site web FAQ sur la politique de support Microsoft.

De plus, les produits et versions de produits non répertoriés dans les rubriques suivantes ne sont pas pris en charge avec System Center Configuration Manager, sauf s'ils ont été annoncés dans le blog Enterprise Mobility and Security. Parfois, le contenu de ce blog précède une mise à jour du corps de cette documentation.

- Taille et échelle en chiffres
  Découvrez combien de sites, de rôles de système de site par site et de clients ou d'appareils sont pris en charge dans les différentes conceptions de hiérarchie pour Configuration Manager.
- Prérequis des sites et systèmes de site
  Découvrez les configurations requises sur un ordinateur Windows Server pour prendre en charge les différents types de site et rôles de système de site.
- Systèmes d'exploitation pris en charge pour les serveurs de système de site
  Découvrez quels systèmes d'exploitation vous pouvez utiliser comme serveur de site ou serveur de système de site.
- Systèmes d'exploitation pris en charge pour les clients et appareils
  Découvrez quels systèmes d'exploitation vous pouvez gérer à l'aide de Configuration Manager, notamment Windows, Windows Embedded, Linux et UNIX, Mac, ainsi que les appareils mobiles.
- Systèmes d'exploitation pris en charge pour la console
  Découvrez quels systèmes d'exploitation peuvent héberger la console Configuration Manager pour

fournir un point d'accès permettant de gérer votre déploiement.

- Prise en charge des versions de SQL Server
  Découvrez quelles versions de SQL Server peuvent héberger la base de données de site et la base de données de création de rapports, et quelles configurations requises et facultatives vous pouvez utiliser.
- Options de haute disponibilité
  Découvrez les options que vous pouvez implémenter lors de la conception de votre environnement pour faciliter le maintien d'un haut niveau de service disponible pour votre déploiement Configuration Manager.
- Matériel recommandé
  Découvrez des conseils pour vous aider à déterminer les configurations et le matériel appropriés pour héberger vos sites et principaux services Configuration Manager.
- Prise en charge des domaines Active Directory
  Découvrez les configurations de domaine Active Directory prises en charge que Configuration Manager exige et prend en charge.
- Prise en charge des fonctionnalités et réseaux Windows
  Découvrez les technologies Windows (telles que la déduplication de données et BranchCache) prises en charge dans Configuration Manager, ainsi que les limitations de leur utilisation.
- Prise en charge des environnements de virtualisation
  Découvrez comment utiliser les technologies de machine virtuelle prises en charge.

# Taille et échelle de System Center Configuration Manager en chiffres

22/06/2018 • 19 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Chaque déploiement de Configuration Manager comporte un nombre maximal de sites, de rôles de système de site et d'appareils qu'il peut prendre en charge. Ces nombres varient selon votre structure hiérarchique, les types et nombres de sites que vous utilisez et les rôles de système de site que vous déployez. Les informations contenues dans cet article peuvent vous aider à déterminer le nombre de rôles de système de site et de sites dont vous avez besoin pour prendre en charge les appareils que vous envisagez de gérer.

Utilisez les informations de cette rubrique ainsi que celles contenues dans les articles suivants :

- Matériel recommandé
- Systèmes d'exploitation pris en charge pour les serveurs de système de site
- Systèmes d'exploitation pris en charge pour les clients et appareils
- Prérequis des sites et systèmes de site

Ces nombres sont basés sur l'utilisation du matériel recommandé pour Configuration Manager. Ils sont également basés sur les paramètres par défaut de toutes les fonctionnalités Configuration Manager disponibles. Quand vous n'utilisez pas le matériel recommandé ou que vous utilisez des paramètres personnalisés plus stricts, les performances des systèmes de site peuvent se dégrader. Les systèmes de site peuvent ne pas atteindre les niveaux de prise en charge indiqués. (Procéder à l'inventaire matériel ou logiciel plus d'une fois tous les 7 jours, ce qui est la valeur par défaut, constitue un exemple de paramètres clients plus stricts.)

## Types de sites

**Site d'administration centrale**

- Un site d'administration centrale peut prendre en charge jusqu'à 25 sites principaux enfants.

**Site principal**

- Chaque site principal prend en charge jusqu'à 250 sites secondaires.
- Le nombre de sites secondaires par site principal est basé sur des connexions réseau WAN continues et fiables. Pour les emplacements de moins de 500 clients, envisagez à un point de distribution au lieu d'un site secondaire.

  Pour plus d'informations sur le nombre de clients et d'appareils qu'un site principal peut prendre en charge, consultez Nombres de clients pour les hiérarchies et les sites.

**Site secondaire**

- Les sites secondaires ne prennent pas en charge les sites enfants.

## Rôles système de site

**Point de service web du catalogue des applications**

- Vous pouvez installer plusieurs instances du point de service web du catalogue d'applications sur des sites principaux.

> **TIP**
> Comme bonne pratique, installez le point du site web du catalogue d'applications et le point de service web du catalogue d'applications sur le même système de site lorsque ces points fournissent le service aux clients Intranet.

- Pour améliorer les performances, envisagez prendre en charge jusqu'à 50 000 clients par instance.
- Chaque instance de ce rôle de système de site prend en charge le nombre maximal de clients pris en charge par la hiérarchie.

**Point du site web du catalogue des applications**

- Vous pouvez installer plusieurs instances du point de site Web du catalogue d'applications sur des sites principaux.

> **TIP**
> Comme bonne pratique, installez le point du site web du catalogue d'applications et le point de service web du catalogue d'applications sur le même système de site lorsque ces points fournissent le service aux clients Intranet.

- Pour améliorer les performances, envisagez prendre en charge jusqu'à 50 000 clients par instance.
- Chaque instance de ce rôle de système de site prend en charge le nombre maximal de clients pris en charge par la hiérarchie.

**Passerelle de gestion cloud**

- Vous pouvez installer plusieurs instances de la passerelle de gestion cloud (CMG) sur des sites principaux ou sur le site d'administration centrale.

> **TIP**
> Dans une hiérarchie, créez la passerelle de gestion cloud sur le site d'administration centrale.

- Une passerelle de gestion cloud prend en charge de une à 16 instances de machine virtuelle dans le service cloud Azure.
- Chaque instance de machine virtuelle de la passerelle de gestion cloud prend en charge 6 000 connexions clientes simultanées. Quand la passerelle de gestion cloud subit une charge élevée en raison d'un dépassement du nombre de clients pris en charge, elle gère néanmoins les requêtes, mais des délais sont possibles.

Pour plus d'informations, consultez Performances et échelle de la passerelle de gestion cloud.

**Point de connexion de la passerelle de gestion cloud**

- Vous pouvez installer plusieurs instances du point de connexion CMG sur des sites principaux.
- Un point de connexion CMG peut prendre en charge une passerelle de gestion cloud avec jusqu'à quatre instances de machine virtuelle. Si la passerelle de gestion cloud compte plus de quatre instances de machine virtuelle, ajoutez un deuxième point de connexion CMG pour l'équilibrage de charge. Une passerelle de gestion cloud disposant de 16 instances de machine virtuelle doit être liée à quatre points de connexion CMG.

Pour plus d'informations, consultez Performances et échelle de la passerelle de gestion cloud.

**Point de distribution**

- Points de distribution par site :

- Chaque site principal et chaque site secondaire prend en charge jusqu'à 250 points de distribution.
- Chaque site principal et secondaire prend en charge jusqu'à 2 000 points de distribution supplémentaires configurés comme points de distribution d'extraction. **Par exemple**, un même site principal prend en charge 2 250 points de distribution quand 2 000 d'entre eux sont configurés comme points de distribution d'extraction.
- Chaque point de distribution prend en charge jusqu'à 4 000 connexions de clients.
- Un point de distribution d'extraction agit comme un client quand il accède au contenu d'un point de distribution source.

- Chaque site principal prend en charge un total combiné de 5 000 points de distribution maximum. Ce total inclut tous les points de distribution sur le site principal et tous les points de distribution qui appartiennent aux sites secondaires enfants du site principal.
- Chaque point de distribution prend en charge un total combiné allant jusqu'à 10 000 packages et applications.

> **WARNING**
> Le nombre réel de clients qu'un point de distribution peut prendre en charge dépend de la vitesse du réseau et de la configuration matérielle du serveur.
>
> De la même façon, le nombre de points de distribution d'extraction qu'un point de distribution source peut prendre en charge dépend de la vitesse du réseau et de la configuration matérielle du point de distribution source. Mais ce nombre est également affecté par la quantité de contenu que vous avez déployé. En effet, contrairement aux clients qui accèdent généralement au contenu à des moments différents pendant un déploiement, tous les points de distribution d'extraction demandent du contenu en même temps. Ces derniers peuvent demander tout le contenu disponible, et pas seulement le contenu qui leur est applicable. Quand vous placez une charge de traitement élevée sur un point de distribution source, des retards imprévus peuvent se produire dans la distribution du contenu aux points de distribution cibles.

**Point d'état de secours**

- Chaque point d'état de secours peut prendre en charge jusqu'à 100 000 clients.

**Point de gestion**

- Chaque site principal prend en charge jusqu'à 15 points de gestion.

  > **TIP**
  > N'installez pas de point de gestion sur des serveurs qui se trouvent sur une liaison lente à partir du serveur de site principal ou du serveur de bases de données du site.

- Chaque site secondaire prend en charge un seul point de gestion qui doit être installé sur le serveur de site secondaire.

  Pour plus d'informations sur le nombre de clients et d'appareils qu'un point de gestion peut prendre en charge, consultez la section Points de gestion.

**Point de mise à jour logicielle**

- Un point de mise à jour logicielle installé sur le serveur de site peut prendre en charge jusqu'à 25 000 clients.
- Un point de mise à jour logicielle distant du serveur de site peut prendre en charge jusqu'à 150 000 clients quand l'ordinateur distant répond à la configuration requise de WSUS (Windows Server Update Services) consistant à prendre en charge ce nombre de clients.

- Par défaut, Configuration Manager ne prend pas en charge la configuration de points de mise à jour logicielle comme clusters d'équilibrage de la charge réseau (NLB). Toutefois, vous pouvez utiliser le kit SDK Configuration Manager pour configurer jusqu'à quatre points de mise à jour logicielle sur un cluster NLB.

## Nombres de clients pour les hiérarchies et les sites

Utilisez les informations suivantes pour déterminer le nombre de clients et leurs types que vous pouvez prendre en charge sur un site ou dans une hiérarchie.

**Hiérarchie avec un site d'administration centrale**

Un site d'administration centrale prend en charge un nombre total d'appareils pouvant atteindre le nombre d'appareils répertoriés pour les trois groupes suivants :

- 700 000 ordinateurs de bureau (exécutant Windows, Linux et UNIX). Consultez également la prise en charge des appareils embarqués.
- 25 000 appareils exécutant Mac et Windows CE 7.0
- L'un des nombres suivants, selon la manière dont votre déploiement prend en charge la gestion des appareils mobiles :
  - 100 000 appareils que vous gérez à l'aide de la gestion MDM locale
  - 300 000 appareils cloud

  Par exemple, dans une hiérarchie, vous pouvez prendre en charge 700 000 ordinateurs de bureau, jusqu'à 25 000 appareils Mac et Windows CE 7.0, et jusqu'à 300 000 appareils cloud quand vous intégrez Microsoft Intune. Cette hiérarchie prend en charge un total de 1 025 000 appareils. Si vous prenez en charge des appareils gérés par la gestion MDM locale, cette hiérarchie totalise 825 000 appareils.

> **IMPORTANT**
> Une hiérarchie où le site d'administration centrale utilise une édition Standard de SQL Server prend en charge un maximum de 50 000 ordinateurs de bureau et appareils. Pour prendre en charge plus de 50 000 postes de travail et appareils, vous devez utiliser une édition Entreprise de SQL Server. Cette exigence s'applique uniquement à un site d'administration centrale. Elle ne s'applique pas à un site principal autonome ou à un site principal enfant. L'édition de SQL Server que vous utilisez pour un site principal ne limite pas sa capacité pour prendre en charge le nombre indiqué de clients.

L'édition de SQL Server utilisée sur un site principal autonome ne limite pas la capacité du site consistant à prendre en charge au maximum le nombre indiqué de clients.

**Site principal enfant**

Chaque site principal enfant d'une hiérarchie disposant d'un site d'administration centrale prend en charge le nombre de clients suivant :

- Un total de 150 000 clients et appareils, non limités à un groupe ou à un type spécifiques, à condition que la prise en charge ne dépasse pas le nombre pris en charge par la hiérarchie. Consultez également la prise en charge des appareils embarqués.

Par exemple, un site principal prend en charge 25 000 appareils Mac et Windows CE 7.0. Ce nombre est la limite d'une hiérarchie. Ce site principal peut alors prendre en charge 125 000 ordinateurs de bureau supplémentaires. Le nombre total d'appareils pris en charge pour le site principal enfant est la limite maximale de 150 000 prise en charge.

**Site principal autonome**

Un site principal autonome prend en charge le nombre suivant d'appareils :

- Total de 175 000 clients et appareils, sans dépasser :
  - 150 000 ordinateurs de bureau (exécutant Windows, Linux et UNIX). Consultez également la prise en charge des appareils embarqués.
  - 25 000 appareils exécutant Mac et Windows CE 7.0
  - L'un des nombres d'éléments suivants, selon la manière dont votre déploiement prend en charge la gestion des appareils mobiles :
    - 50 000 appareils que vous gérez à l'aide de la gestion MDM locale
    - 150 000 appareils cloud

Par exemple, un site principal autonome prenant en charge 150 000 ordinateurs de bureau et 10 000 clients Mac ou Windows CE 7.0 ne peut prendre en charge que 15 000 appareils supplémentaires. Ces appareils peuvent être basés sur le cloud ou gérés à l'aide de la gestion MDM locale.

**Sites principaux et appareils Windows Embedded**

Les sites principaux prennent en charge les appareils embarqués Windows Embedded où les filtres d'écriture basés sur des fichiers (FBWF) sont activés. Quand des appareils embarqués ne disposent pas de filtres d'écriture activés, un site principal peut prendre en charge un nombre d'appareils embarqués pouvant atteindre le nombre autorisé d'appareils pour ce site. Du nombre total des appareils qu'un site principal prend en charge, un maximum de 10 000 de ceux-ci peuvent être des appareils Windows Embedded. Ces appareils doivent être configurés pour les exceptions listées dans la Remarque importante se trouvant dans Planification du déploiement de clients sur des appareils Windows Embedded. Un site principal prend en charge seulement 3 000 appareils Windows Embedded où EWF est activé et qui ne sont pas configurés pour les exceptions.

**Sites secondaires**

Les sites secondaires prennent en charge le nombre suivant d'appareils :

- 15 000 ordinateurs de bureau (exécutant Windows, Linux et UNIX)

**Points de gestion**

Chaque point de gestion peut prendre en charge le nombre suivant d'appareils :

- Total de 25 000 clients et appareils, sans dépasser :
  - 25 000 ordinateurs de bureau (exécutant Windows, Linux et UNIX)
  - L'un des nombres d'éléments suivants (pas les deux) :
    - 10 000 appareils que vous gérez à l'aide de la gestion MDM locale
    - 10 000 appareils exécutant des clients Mac et Windows CE 7.0

# Prérequis des sites et systèmes de site pour System Center Configuration Manager

22/06/2018 • 41 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les ordinateurs Windows nécessitent des configurations spécifiques pour pouvoir être utilisés comme serveurs de système de site System Center Configuration Manager.

Dans certains cas, par exemple Windows Server Update Services (WSUS) pour le point de mise à jour logicielle, vous devez vous référer à la documentation du produit pour connaître les prérequis et limitations supplémentaires liés à l'utilisation. Cet article porte uniquement sur les configurations qui s'appliquent directement à l'utilisation de Configuration Manager.

> **NOTE**
> Depuis janvier 2016, le support n'est plus assuré pour .NET Framework 4.0, 4.5 et 4.5.1. Pour plus d'informations, consultez Forum Aux Questions sur la politique de support - Microsoft .NET Framework à l'adresse support.microsoft.com.

## Configuration requise et limitations générales du serveur de site

**Ce qui suit s'applique à tous les serveurs de système de site :**

- Chaque serveur de système de site doit utiliser un système d'exploitation 64 bits. La seule exception est le rôle de système de site du point de distribution, que vous pouvez installer sur certains systèmes d'exploitation 32 bits.
- Les systèmes de site ne sont pas pris en charge sur des installations minimales pour les systèmes d'exploitation suivants : Une exception est que les installations minimales sont prises en charge pour le rôle de système de site du point de distribution, sans prise en charge de PXE ou de la multidiffusion.
- Une fois que vous avez installé un serveur de système de site, vous ne pouvez plus modifier les éléments suivants :
  - Le nom du domaine où se trouve l'ordinateur du système de site (également appelé **changement de nom de domaine**).
  - L'appartenance de l'ordinateur au domaine.
  - Nom de l'ordinateur.

  Si vous devez modifier ces éléments, vous devez d'abord supprimer le rôle système de site sur l'ordinateur, puis réinstaller les rôles une fois la modification effectuée. Concernant les modifications affectant l'ordinateur du serveur de site, vous devez désinstaller le site, puis le réinstaller une fois la modification effectuée.
- Les rôles de système de site ne sont pas pris en charge sur une instance de cluster Windows Server. La seule exception est le serveur de base de données de site.
- Vous ne pouvez pas modifier le type de démarrage ou les paramètres d'ouverture de session pour un service Configuration Manager. Dans ce cas, vous risquez d'empêcher des services clés de s'exécuter correctement.

# Conditions préalables pour les systèmes d'exploitation Windows Server 2012 et versions ultérieures

**Serveur de site : site d'administration centrale et site principal**

**Rôles et fonctionnalités Windows Server :**

- .NET Framework 3.5 SP1 (ou version ultérieure)
- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1
  - Pour plus d'informations sur les versions du .Net Framework, consultez Versions et dépendances du .NET Framework.
- Compression différentielle à distance

**Windows ADK :**

- Avant d'installer ou de mettre à niveau un site d'administration centrale ou un site principal, vous devez installer la version du Kit de déploiement et d'évaluation Windows (ADK) nécessaire pour la version de Configuration Manager que vous installez ou vers laquelle vous effectuez une mise à niveau. Consultez Windows 10 ADK dans l'article Prise en charge pour Windows 10 comme client.
- Pour plus d'informations sur cette configuration requise, consultez Configuration requise de l'infrastructure pour le déploiement de système d'exploitation.

**Redistribuable Visual C++ :**

- Configuration Manager installe Microsoft Visual C++ 2013 Redistributable Package sur chaque ordinateur sur lequel est installé un serveur de site.
- Les sites d'administration centrale et les sites principaux requièrent à la fois les versions x86 et x64 du fichier redistribuable applicable.

**Serveur de site : site secondaire**

**Rôles et fonctionnalités Windows Server :**

- .NET Framework 3.5 SP1 (ou version ultérieure)
- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1
  - Pour plus d'informations sur les versions du .Net Framework, consultez Versions et dépendances du .NET Framework.
- Compression différentielle à distance

**Redistribuable Visual C++ :**

- Configuration Manager installe Microsoft Visual C++ 2013 Redistributable Package sur chaque ordinateur sur lequel est installé un serveur de site.
- Les sites secondaires requièrent seulement la version x64.

**Rôles de système de site par défaut :**

- Par défaut, un site secondaire installe un **point de gestion** et un **point de distribution**.
- Assurez-vous que le serveur de site secondaire remplit les conditions préalables pour ces rôles de système de site.

**Serveur de base de données**

**Service d'accès à distance au Registre :**

- Durant l'installation du site Configuration Manager, vous devez activer le service d'accès à distance au Registre sur l'ordinateur qui hébergera la base de données du site.

**SQL Server :**

- Avant d'installer un site d'administration centrale ou un site principal, vous devez installer une version prise en charge de SQL Server pour héberger la base de données du site.
- Avant d'installer un site secondaire, vous pouvez installer une version prise en charge de SQL Server.
- Si vous souhaitez que Configuration Manager installe SQL Server Express en même temps que le site secondaire, vérifiez que l'ordinateur présente la configuration requise pour exécuter SQL Server Express.

**Serveur de fournisseur SMS**

**Windows ADK :**

- L'ordinateur sur lequel vous installez une instance du fournisseur SMS doit disposer de la version de Windows ADK nécessaire à la version de Configuration Manager que vous installez ou vers laquelle vous effectuez une mise à niveau. Consultez Windows 10 ADK dans l'article Prise en charge pour Windows 10 comme client.
- Pour plus d'informations sur cette configuration requise, consultez Configuration requise de l'infrastructure pour le déploiement de système d'exploitation.

**Point du site web du catalogue des applications**

**Rôles et fonctionnalités Windows Server :**

- .NET Framework 3.5 SP1 (ou version ultérieure)
- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1
  - ASP.NET 4.5
  - Pour plus d'informations sur les versions du .Net Framework, consultez Versions et dépendances du .NET Framework.

**Configuration IIS :**

- Fonctionnalités HTTP communes :
  - Document par défaut
  - Contenu statique
- Développement d'applications :
  - ASP.NET 3.5 (et les options sélectionnées automatiquement)
  - ASP.NET 4.5 (et les options sélectionnées automatiquement)
  - Extensibilité .NET 3.5
  - Extensibilité .NET 4.5
- Sécurité :
  - Authentification Windows
- Compatibilité avec la gestion IIS 6 :
  - Compatibilité avec la métabase de données IIS 6

**Point de service web du catalogue des applications**

**Rôles et fonctionnalités Windows Server :**

- .NET Framework 3.5 SP1 (ou version ultérieure)
- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1 :
  - ASP.NET 4.5 :
    - Activation de HTTP (et des options sélectionnées automatiquement)

**Configuration IIS :**

- Fonctionnalités HTTP communes :
  - Document par défaut
- Compatibilité avec la gestion IIS 6 :
  - Compatibilité avec la métabase de données IIS 6
- Développement d'applications :
  - ASP.NET 3.5 (et les options sélectionnées automatiquement)
  - Extensibilité .NET 3.5
  - ASP.NET 4.5 (et les options sélectionnées automatiquement)
  - Extensibilité .NET 4.5

**Mémoire de l'ordinateur :**

- L'ordinateur hébergeant ce rôle de système de site doit avoir au moins 5 % de mémoire disponible pour permettre au rôle de système de site de traiter les demandes.
- Quand ce rôle de système de site coexiste avec un autre rôle de système de site qui a cette même exigence, la quantité de mémoire disponible requise pour l'ordinateur n'augmente pas, mais elle reste à un minimum de 5 %.

**Point de synchronisation Asset Intelligence**

**Rôles et fonctionnalités Windows Server :**

- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1

**Point d'enregistrement de certificat**

**Rôles et fonctionnalités Windows Server :**

- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1 :
  - Activation HTTP

**Configuration IIS :**

- Développement d'applications :
  - ASP.NET 3.5 (et les options sélectionnées automatiquement)
  - ASP.NET 4.5 (et les options sélectionnées automatiquement)
- Compatibilité avec la gestion IIS 6 :
  - Compatibilité avec la métabase de données IIS 6
  - Compatibilité WMI d'IIS 6

**Point de distribution**

**Rôles et fonctionnalités Windows Server :**

- Compression différentielle à distance

**Configuration IIS :**

- Développement d'applications :
  - Extensions ISAPI
- Sécurité :
  - Authentification Windows
- Compatibilité avec la gestion IIS 6 :
  - Compatibilité avec la métabase de données IIS 6
  - Compatibilité WMI d'IIS 6

**PowerShell :**

- Sur Windows Server 2012 et les versions ultérieures, PowerShell 3.0 ou 4.0 est nécessaire pour pouvoir installer le point de distribution.

**Redistribuable Visual C++ :**

- Configuration Manager installe Microsoft Visual C++ 2013 Redistributable Package sur chaque ordinateur hébergeant un point de distribution.
- La version installée dépend de la plateforme de l'ordinateur (x86 ou x64).

**Microsoft Azure :**

- Pour héberger un point de distribution, vous pouvez utiliser un service cloud dans Microsoft Azure.

**Pour prendre en charge PXE ou la multidiffusion :**

- Installez et configurez le rôle WDS (Windows Deployment Services) de Windows Server.

> **NOTE**
> WDS s'installe et se configure automatiquement quand vous configurez un point de distribution pour prendre en charge PXE ou la multidiffusion sur un serveur exécutant Windows Server 2012 ou une version ultérieure.

> **NOTE**
> Lorsque le point de distribution transfère du contenu, il le fait à l'aide du **Service de transfert intelligent en arrière-plan** (BITS) intégré au système d'exploitation Windows. Le rôle du point de distribution ne requiert pas que la fonctionnalité BITS IIS Server Extension facultative soit installée car le client n'y charge pas d'informations.

**Point Endpoint Protection**

**Rôles et fonctionnalités Windows Server :**

- .NET Framework 3.5 SP1 (ou version ultérieure)

**Point d'inscription**

**Rôles et fonctionnalités Windows Server :**

- .NET Framework 3.5 (ou version ultérieure).

- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1 :

  Pendant l'installation de ce rôle de système de site, Configuration Manager installe automatiquement .NET Framework 4.5.2. Cette installation peut placer le serveur dans un état d'attente redémarrage. Si un redémarrage est en attente pour .NET Framework, il est possible que les applications .NET ne puissent pas s'exécuter tant que le serveur n'a pas redémarré et que l'installation n'est pas terminée.

  - Activation de HTTP (et des options sélectionnées automatiquement)
  - ASP.NET 4.5

**Configuration IIS :**

- Fonctionnalités HTTP communes :
  - Document par défaut
- Développement d'applications :
  - ASP.NET 3.5 (et les options sélectionnées automatiquement)
  - Extensibilité .NET 3.5
  - ASP.NET 4.5 (et les options sélectionnées automatiquement)
  - .NET Extensibility 4.5
- Compatibilité avec la gestion IIS 6 :
  - Compatibilité avec la métabase de données IIS 6

**Mémoire de l'ordinateur :**

- L'ordinateur hébergeant ce rôle de système de site doit avoir au moins 5 % de mémoire disponible pour permettre au rôle de système de site de traiter les demandes.
- Quand ce rôle de système de site coexiste avec un autre rôle de système de site qui a cette même exigence, la quantité de mémoire disponible requise pour l'ordinateur n'augmente pas, mais elle reste à un minimum de 5 %.

**Point proxy d'inscription**

**Rôles et fonctionnalités Windows Server :**

- .NET Framework 3.5 (ou version ultérieure).
- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1

  Pendant l'installation de ce rôle de système de site, Configuration Manager installe automatiquement .NET Framework 4.5.2. Cette installation peut placer le serveur dans un état d'attente redémarrage. Si un redémarrage est en attente pour .NET Framework, il est possible que les applications .NET ne puissent pas s'exécuter tant que le serveur n'a pas redémarré et que l'installation n'est pas terminée.

**Configuration IIS :**

- Fonctionnalités HTTP communes :
  - Document par défaut
  - Contenu statique
- Développement d'applications :
  - ASP.NET 3.5 (et les options sélectionnées automatiquement)

- ASP.NET 4.5 (et les options sélectionnées automatiquement)
- Extensibilité .NET 3.5
- Extensibilité .NET 4.5

- Sécurité :
  - Authentification Windows
- Compatibilité avec la gestion IIS 6 :
  - Compatibilité avec la métabase de données IIS 6

**Mémoire de l'ordinateur :**

- L'ordinateur hébergeant ce rôle de système de site doit avoir au moins 5 % de mémoire disponible pour permettre au rôle de système de site de traiter les demandes.
- Quand ce rôle de système de site coexiste avec un autre rôle de système de site qui a cette même exigence, la quantité de mémoire disponible requise pour l'ordinateur n'augmente pas, mais elle reste à un minimum de 5 %.

**Point d'état de secours**

La configuration IIS par défaut est nécessaire, avec les ajouts suivants :

- Compatibilité avec la gestion IIS 6 :
  - Compatibilité avec la métabase de données IIS 6

**Point de gestion**

**Rôles et fonctionnalités Windows Server :**

- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1
- Extensions du serveur BITS (et options sélectionnées automatiquement) ou services BITS (et options sélectionnées automatiquement)

**Configuration IIS :**

- Développement d'applications :
  - Extensions ISAPI
- Sécurité :
  - Authentification Windows
- Compatibilité avec la gestion IIS 6 :
  - Compatibilité avec la métabase de données IIS 6
  - Compatibilité WMI d'IIS 6

**Point de Reporting Services**

**Rôles et fonctionnalités Windows Server :**

- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1

**SQL Server Reporting Services :**

- Avant d'installer le point de Reporting Services, installez et configurez au moins une instance de SQL Server pour prendre en charge SQL Server Reporting Services.
- L'instance que vous utilisez pour SQL Server Reporting Services peut être la même que celle utilisée pour

la base de données du site.

- En outre, l'instance que vous utilisez peut être partagée avec d'autres produits System Center, dès lors que ceux-ci n'ont pas de restrictions pour le partage de l'instance de SQL Server.

**Point de connexion de service**

**Rôles et fonctionnalités Windows Server :**

- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1

  Pendant l'installation de ce rôle de système de site, Configuration Manager installe automatiquement .NET Framework 4.5.2. Cette installation peut placer le serveur dans un état d'attente redémarrage. Si un redémarrage est en attente pour .NET Framework, il est possible que les applications .NET ne puissent pas s'exécuter tant que le serveur n'a pas redémarré et que l'installation n'est pas terminée.

**Redistribuable Visual C++ :**

- Configuration Manager installe Microsoft Visual C++ 2013 Redistributable Package sur chaque ordinateur hébergeant un point de distribution.
- Le rôle de système de site nécessite la version x64.

**Point de mise à jour logicielle**

**Rôles et fonctionnalités Windows Server :**

- .NET Framework 3.5 SP1 (ou version ultérieure)
- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1

La configuration IIS par défaut est nécessaire.

**Windows Server Update Services :**

- Vous devez installer le rôle Windows Server Update Services (WSUS) de Windows Server sur un ordinateur avant d'installer un point de mise à jour logicielle.
- Pour plus d'informations, consultez Planifier les mises à jour logicielles dans System Center Configuration Manager.

**Point de migration d'état**

La configuration IIS par défaut est nécessaire.

## Conditions préalables pour Windows Server 2008 R2 et Windows Server 2008

Windows Server 2008 et Windows Server 2008 R2 bénéficient désormais du support étendu au lieu du support standard, comme indiqué dans la Politique de support Microsoft. Pour plus d'informations sur la prise en charge à venir de ces systèmes d'exploitation utilisés comme serveurs de système de site avec Configuration Manager, consultez Systèmes d'exploitation serveur supprimés et dépréciés.

**Ce qui suit s'applique à toutes les conditions requises pour .NET Framework :**

- Installez la version complète de .NET Framework avant d'installer les rôles de système de site. Par exemple, consultez Microsoft .NET Framework 4 (programme d'installation autonome). Le profil client .NET Framework 4 ne correspond pas à la configuration requise.

**Ce qui suit s'applique à toutes les conditions requises pour l'activation de Windows Communication Foundation (WCF) :**

- Vous pouvez configurer l'activation de WCF comme faisant partie de la fonctionnalité Windows du .NET Framework sur le serveur de système de site. Par exemple, sur Windows Server 2008 R2, exécutez l'**Assistant Ajout de fonctionnalités** pour installer des fonctionnalités supplémentaires sur le serveur. Sur la page **Sélectionner des fonctionnalités**, développez **Fonctionnalités de .NET Framework 3.5.1** et développez **Activation WCF**. Cochez les cases **Activation HTTP** et **Activation non HTTP** pour activer ces options.

**Serveur de site : site d'administration centrale et site principal**

**.NET Framework :**

- .NET Framework 3.5 SP1 (ou version ultérieure)
- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1

**Fonctionnalité Windows :**

- Compression différentielle à distance

**Windows ADK :**

- Avant d'installer ou de mettre à niveau un site d'administration centrale ou un site principal, vous devez installer la version de Windows ADK nécessaire pour la version de Configuration Manager que vous installez ou vers laquelle vous effectuez une mise à niveau. Consultez Windows 10 ADK dans l'article Prise en charge pour Windows 10 comme client.
- Pour plus d'informations sur cette configuration requise, consultez Configuration requise de l'infrastructure pour le déploiement de système d'exploitation.

**Redistribuable Visual C++ :**

- Configuration Manager installe Microsoft Visual C++ 2013 Redistributable Package sur chaque ordinateur sur lequel est installé un serveur de site.
- Les sites d'administration centrale et les sites principaux requièrent à la fois les versions x86 et x64 du fichier redistribuable applicable.

**Serveur de site : site secondaire**

**.NET Framework :**

- .NET Framework 3.5 SP1 (ou version ultérieure)
- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1

**Redistribuable Visual C++ :**

- Configuration Manager installe Microsoft Visual C++ 2013 Redistributable Package sur chaque ordinateur sur lequel est installé un serveur de site.
- Les sites secondaires requièrent seulement la version x64.

**Rôles de système de site par défaut :**

- Par défaut, un site secondaire installe un **point de gestion** et un **point de distribution**.
- Assurez-vous que le serveur de site secondaire remplit les conditions préalables pour ces rôles de système de site.

**Serveur de base de données**

**Service d'accès à distance au Registre :**

- Durant l'installation du site Configuration Manager, vous devez activer le service d'accès à distance au Registre sur l'ordinateur qui hébergera la base de données du site.

**SQL Server :**

- Avant d'installer un site d'administration centrale ou un site principal, vous devez installer une version prise en charge de SQL Server pour héberger la base de données du site.
- Avant d'installer un site secondaire, vous pouvez installer une version prise en charge de SQL Server.
- Si vous souhaitez que Configuration Manager installe SQL Server Express en même temps que le site secondaire, vérifiez que l'ordinateur présente la configuration requise pour exécuter SQL Server Express.

**Serveur de fournisseur SMS**

**Windows ADK :**

- L'ordinateur sur lequel vous installez une instance du fournisseur SMS doit disposer de la version de Windows ADK nécessaire à la version de Configuration Manager que vous installez ou vers laquelle vous effectuez une mise à niveau. Consultez Windows 10 ADK dans l'article Prise en charge pour Windows 10 comme client.
- Pour plus d'informations sur cette configuration requise, consultez Configuration requise de l'infrastructure pour le déploiement de système d'exploitation.

**Point du site web du catalogue des applications**

**.NET Framework :**

- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1

**Configuration IIS :**

La configuration IIS par défaut est nécessaire, avec les ajouts suivants :

- Fonctionnalités HTTP communes :
  - Contenu statique
  - Document par défaut
- Développement d'applications :
  - ASP.NET (et options sélectionnées automatiquement)

    Dans certains scénarios, par exemple quand IIS est installé ou reconfiguré après l'installation de .NET Framework version 4.5.2, vous devez activer explicitement ASP.NET version 4.5. Par exemple, sur un ordinateur 64 bits exécutant .NET Framework version 4.0.30319, exécutez la commande suivante : **%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -i -enable**
- Sécurité :
  - Authentification Windows
- Compatibilité avec la gestion IIS 6 :
  - Compatibilité avec la métabase de données IIS 6

**Point de service web du catalogue des applications**

**.NET Framework :**

- .NET Framework 3.5 SP1 (ou version ultérieure)
- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1

**Activation de Windows Communication Foundation (WCF) :**

- Activation HTTP

- Activation non-HTTP

**Configuration IIS :**

La configuration IIS par défaut est nécessaire, avec les ajouts suivants :

- Développement d'applications :
  - ASP.NET (et options sélectionnées automatiquement)

    Dans certains scénarios, par exemple quand IIS est installé ou reconfiguré après l'installation de .NET Framework version 4.5.2, vous devez activer explicitement ASP.NET version 4.5. Par exemple, sur un ordinateur 64 bits exécutant .NET Framework version 4.0.30319, exécutez la commande suivante : **%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -i -enable**
- Compatibilité avec la gestion IIS 6 :
  - Compatibilité avec la métabase de données IIS 6

**Mémoire de l'ordinateur :**

- L'ordinateur hébergeant ce rôle de système de site doit avoir au moins 5 % de mémoire disponible pour permettre au rôle de système de site de traiter les demandes.
- Quand ce rôle de système de site coexiste avec un autre rôle de système de site qui a cette même exigence, la quantité de mémoire disponible requise pour l'ordinateur n'augmente pas, mais elle reste à un minimum de 5 %.

**Point de synchronisation Asset Intelligence**

**.NET Framework :**

- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1

**Point d'enregistrement de certificat**

**.NET Framework :**

- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1
- Activation HTTP

**Configuration IIS :**

La configuration IIS par défaut est nécessaire, avec les ajouts suivants :

- Compatibilité avec la gestion IIS 6 :
  - Compatibilité avec la métabase de données IIS 6
  - Compatibilité WMI d'IIS 6

**Point de distribution**

**Configuration IIS :**

Vous pouvez utiliser la configuration IIS par défaut ou une configuration personnalisée. Pour utiliser une configuration IIS personnalisée, vous devez activer les options suivantes pour IIS :

- Développement d'applications :
  - Extensions ISAPI
- Sécurité :

    - Authentification Windows
- Compatibilité avec la gestion IIS 6 :
    - Compatibilité avec la métabase de données IIS 6
    - Compatibilité WMI d'IIS 6

Quand vous utilisez une configuration IIS personnalisée, vous pouvez supprimer les options qui ne sont pas nécessaires, comme les éléments suivants :

- Fonctionnalités HTTP communes :
    - Redirection HTTP
- Scripts et outils de gestion IIS

**Fonctionnalité Windows :**

- Compression différentielle à distance

**Redistribuable Visual C++ :**

- Configuration Manager installe Microsoft Visual C++ 2013 Redistributable Package sur chaque ordinateur hébergeant un point de distribution.
- La version installée dépend de la plateforme de l'ordinateur (x86 ou x64).

**Microsoft Azure :**

- Pour héberger un point de distribution, vous pouvez utiliser un service cloud dans Azure.

**Pour prendre en charge PXE ou la multidiffusion :**

- Installez et configurez le rôle WDS (Windows Deployment Services) de Windows Server.

> **NOTE**
> WDS s'installe et se configure automatiquement quand vous configurez un point de distribution pour prendre en charge PXE ou la multidiffusion sur un serveur exécutant Windows Server 2012 ou une version ultérieure.

> **NOTE**
> Lorsque le point de distribution transfère du contenu, il le fait à l'aide du **Service de transfert intelligent en arrière-plan** (BITS) intégré au système d'exploitation Windows. Le rôle du point de distribution ne requiert pas que la fonctionnalité BITS IIS Server Extension facultative soit installée car le client n'y charge pas d'informations.

**Point Endpoint Protection**

**.NET Framework :**

- .NET Framework 3.5 SP1 (ou version ultérieure)

**Point d'inscription**

**.NET Framework :**

- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1

  Si, quand ce rôle de système de site est installé, aucune version prise en charge de .NET Framework n'est installée sur le serveur, Configuration Manager installe automatiquement .NET Framework 4.5.2. Cette installation peut placer le serveur dans un état d'attente redémarrage. Si un redémarrage est en attente

pour .NET Framework, il est possible que les applications .NET ne puissent pas s'exécuter tant que le serveur n'a pas redémarré et que l'installation n'est pas terminée.

**Activation de Windows Communication Foundation (WCF) :**

- Activation HTTP
- Activation non-HTTP

**Configuration IIS :**

La configuration IIS par défaut est nécessaire, avec les ajouts suivants :

- Développement d'applications :
  - ASP.NET (et options sélectionnées automatiquement)

    Dans certains scénarios, par exemple quand IIS est installé ou reconfiguré après l'installation de .NET Framework version 4.5.2, vous devez activer explicitement ASP.NET version 4.5. Par exemple, sur un ordinateur 64 bits exécutant .NET Framework version 4.0.30319, exécutez la commande suivante : **%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -i -enable**

**Mémoire de l'ordinateur :**

- L'ordinateur hébergeant ce rôle de système de site doit avoir au moins 5 % de mémoire disponible pour permettre au rôle de système de site de traiter les demandes.
- Quand ce rôle de système de site coexiste avec un autre rôle de système de site qui a cette même exigence, la quantité de mémoire disponible requise pour l'ordinateur n'augmente pas, mais elle reste à un minimum de 5 %.

**Point proxy d'inscription**

**.NET Framework :**

- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1

  Si, quand ce rôle de système de site est installé, aucune version prise en charge de .NET Framework n'est installée sur le serveur, Configuration Manager installe automatiquement .NET Framework 4.5.2. Cette installation peut placer le serveur dans un état d'attente redémarrage. Quand un redémarrage est en attente pour .NET Framework, il est possible que les applications .NET ne puissent pas s'exécuter tant que le serveur n'a pas redémarré et que l'installation n'est pas terminée.

**Activation de Windows Communication Foundation (WCF) :**

- Activation HTTP
- Activation non-HTTP

**Configuration IIS :**

La configuration IIS par défaut est nécessaire, avec les ajouts suivants :

- Développement d'applications :
  - ASP.NET (et options sélectionnées automatiquement)

    Dans certains scénarios, par exemple quand IIS est installé ou reconfiguré après l'installation de .NET Framework version 4.5.2, vous devez activer explicitement ASP.NET version 4.5. Par exemple, sur un ordinateur 64 bits exécutant .NET Framework version 4.0.30319, exécutez la commande suivante : **%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -i -enable**

**Mémoire de l'ordinateur :**

- L'ordinateur hébergeant ce rôle de système de site doit avoir au moins 5 % de mémoire disponible pour permettre au rôle de système de site de traiter les demandes.
- Quand ce rôle de système de site coexiste avec un autre rôle de système de site qui a cette même exigence, la quantité de mémoire disponible requise pour l'ordinateur n'augmente pas, mais elle reste à un minimum de 5 %.

**Point d'état de secours**

**Configuration IIS :**

La configuration IIS par défaut est nécessaire, avec les ajouts suivants :

- Compatibilité avec la gestion IIS 6 :
  - Compatibilité avec la métabase de données IIS 6

**Point de gestion**

**.NET Framework :**

- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1

**Configuration IIS :**

Vous pouvez utiliser la configuration IIS par défaut ou une configuration personnalisée. Chaque point de gestion que vous activez pour la prise en charge des appareils mobiles requiert une configuration d'IIS supplémentaire pour ASP.NET (et ses options sélectionnées automatiquement).

Dans certains scénarios, par exemple quand IIS est installé ou reconfiguré après l'installation de .NET Framework version 4.5.2, vous devez activer explicitement ASP.NET version 4.5. Par exemple, sur un ordinateur 64 bits exécutant .NET Framework version 4.0.30319, exécutez la commande suivante :
**%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -i -enable**

Pour utiliser une configuration IIS personnalisée, vous devez activer les options suivantes pour IIS :

- Développement d'applications :
  - Extensions ISAPI
- Sécurité :
  - Authentification Windows
- Compatibilité avec la gestion IIS 6 :
  - Compatibilité avec la métabase de données IIS 6
  - Compatibilité WMI d'IIS 6

Quand vous utilisez une configuration IIS personnalisée, vous pouvez supprimer les options qui ne sont pas nécessaires, comme les options suivantes :

- Fonctionnalités HTTP communes :
  - Redirection HTTP
- Scripts et outils de gestion IIS

**Fonctionnalité Windows :**

- Extensions du serveur BITS (et options sélectionnées automatiquement) ou service de transfert intelligent en arrière-plan (BITS) (et options sélectionnées automatiquement)

**Point de Reporting Services**

**.NET Framework :**

- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1

**SQL Server Reporting Services :**

- Avant d'installer le point de Reporting Services, installez et configurez au moins une instance de SQL Server pour prendre en charge SQL Server Reporting Services.
- L'instance que vous utilisez pour SQL Server Reporting Services peut être la même que celle utilisée pour la base de données du site.
- En outre, l'instance que vous utilisez peut être partagée avec d'autres produits System Center, dès lors que ceux-ci n'ont pas de restrictions pour le partage de l'instance de SQL Server.

**Point de connexion de service**

**.NET Framework :**

- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1

  Si, quand ce rôle de système de site est installé, aucune version prise en charge de .NET Framework n'est installée sur le serveur, Configuration Manager installe automatiquement .NET Framework 4.5.2. Cette installation peut placer le serveur dans un état d'attente redémarrage. Si un redémarrage est en attente pour .NET Framework, il est possible que les applications .NET ne puissent pas s'exécuter tant que le serveur n'a pas redémarré et que l'installation n'est pas terminée.

**Redistribuable Visual C++ :**

- Configuration Manager installe Microsoft Visual C++ 2013 Redistributable Package sur chaque ordinateur hébergeant un point de distribution.
- Le rôle de système de site nécessite la version x64.

**Point de mise à jour logicielle**

**.NET Framework :**

- .NET Framework 3.5 SP1 (ou version ultérieure)
- .NET Framework 4.5.2, 4.6.1, 4.6.2, 4.7 ou 4.7.1

**Configuration IIS :**

La configuration IIS par défaut est nécessaire.

**Windows Server Update Services :**

- Vous devez installer le rôle Windows Server Update Services (WSUS) de Windows Server sur un ordinateur avant d'installer un point de mise à jour logicielle.
- Pour plus d'informations, consultez Planifier les mises à jour logicielles dans System Center Configuration Manager.

**Point de migration d'état**

**Configuration IIS :**

La configuration IIS par défaut est nécessaire.

# Systèmes d'exploitation pris en charge pour les serveurs de système de site System Center Configuration Manager

26/06/2018 • 15 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cet article explique en détail les versions de Windows que vous pouvez utiliser pour héberger un site ou un rôle de système de site Configuration Manager.

Utilisez les informations de cet article ainsi que celles des articles suivants :

- Matériel recommandé pour Configuration Manager
- Prérequis des sites et systèmes de site pour Configuration Manager
- Taille et échelle de Configuration Manager en chiffres

## Windows Server 2016 : Standard et Datacenter

Avec le correctif cumulatif proposé dans l'article KB3186654, ce système d'exploitation est pris en charge pour les rôles suivants :

**Serveurs de site :**

- Site d'administration centrale
- Site principal
- Site secondaire

**Serveurs de système de site :**

- Point de service web du catalogue des applications
- Point du site web du catalogue des applications
- Point de synchronisation Asset Intelligence
- Point d'enregistrement de certificat
- Point de distribution

  Les points de distribution prennent en charge plusieurs configurations différentes ayant chacune des exigences différentes. Dans certains cas, ces configurations prennent en charge l'installation sur des serveurs, mais aussi sur des systèmes d'exploitation clients. Pour plus d'informations sur les options disponibles pour les points de distribution, consultez Gérer le contenu et l'infrastructure de contenu.
- Point Endpoint Protection
- Point d'inscription
- Point proxy d'inscription
- Point d'état de secours
- Point de gestion

- Point de Reporting Services
- point de connexion de service
- Serveur de bases de données du site

  Les serveurs de bases de données du site ne sont pas pris en charge sur un contrôleur de domaine en lecture seule (RODC). Pour plus d'informations, voir Vous pouvez rencontrer des problèmes lors de l'installation de SQL Server sur un contrôleur de domaine dans la Base de connaissances Microsoft. En outre, les serveurs de site secondaire ne sont pris en charge sur aucun contrôleur de domaine.
- SMS_Provider
- Point de mise à jour logicielle
- Point de migration d'état

## Windows Storage Server 2016

**Serveur de système de site :**

- Point de distribution

## Windows Server 2012 R2 (x64) : Standard et Datacenter

**Serveurs de site :**

- Site d'administration centrale
- Site principal
- Site secondaire

**Serveurs de système de site :**

- Point de service web du catalogue des applications
- Point du site web du catalogue des applications
- Point de synchronisation Asset Intelligence
- Point d'enregistrement de certificat
- Point de distribution

  Les points de distribution prennent en charge plusieurs configurations différentes ayant chacune des exigences différentes. Dans certains cas, ces configurations prennent en charge l'installation sur des serveurs, mais aussi sur des systèmes d'exploitation clients. Pour plus d'informations sur les options disponibles pour les points de distribution, consultez Gérer le contenu et l'infrastructure de contenu.
- Point Endpoint Protection
- Point d'inscription
- Point proxy d'inscription
- Point d'état de secours
- Point de gestion
- Point de Reporting Services
- point de connexion de service

- Serveur de bases de données du site

  Les serveurs de bases de données du site ne sont pas pris en charge sur un contrôleur de domaine en lecture seule (RODC). Pour plus d'informations, voir Vous pouvez rencontrer des problèmes lors de l'installation de SQL Server sur un contrôleur de domaine dans la Base de connaissances Microsoft. En outre, les serveurs de site secondaire ne sont pris en charge sur aucun contrôleur de domaine.

- SMS_Provider
- Point de mise à jour logicielle
- Point de migration d'état

## Windows Server 2012 R2 (x64) : Standard et Datacenter

**Serveurs de site :**

- Site d'administration centrale
- Site principal
- Site secondaire

**Serveurs de système de site :**

- Point de service web du catalogue des applications
- Point du site web du catalogue des applications
- Point de synchronisation Asset Intelligence
- Point d'enregistrement de certificat
- Point de distribution

  Les points de distribution prennent en charge plusieurs configurations différentes ayant chacune des exigences différentes. Dans certains cas, ces configurations prennent en charge l'installation sur des serveurs, mais aussi sur des systèmes d'exploitation clients. Pour plus d'informations sur les options disponibles pour les points de distribution, consultez Gérer le contenu et l'infrastructure de contenu.

- Point Endpoint Protection
- Point d'inscription
- Point proxy d'inscription
- Point d'état de secours
- Point de gestion
- Point de Reporting Services
- point de connexion de service
- Serveur de bases de données du site

  Les serveurs de bases de données du site ne sont pas pris en charge sur un contrôleur de domaine en lecture seule (RODC). Pour plus d'informations, voir Vous pouvez rencontrer des problèmes lors de l'installation de SQL Server sur un contrôleur de domaine dans la Base de connaissances Microsoft. En outre, les serveurs de site secondaire ne sont pris en charge sur aucun contrôleur de domaine.

- SMS_Provider

- Point de mise à jour logicielle
- Point de migration d'état

## Windows Server 2008 R2 avec SP1 (x64) : Standard, Enterprise et Datacenter

Windows Server 2008 R2 bénéficie désormais du support étendu au lieu du support standard, comme indiqué dans la Politique de support Microsoft. Pour plus d'informations sur la prise en charge à venir de ces systèmes d'exploitation utilisés comme serveurs de système de site avec Configuration Manager, consultez Systèmes d'exploitation serveur dépréciés.

Ce système d'exploitation n'est pas pris en charge pour les serveurs de site ou la plupart des rôles de système de site. Il est toujours pris en charge pour le rôle de système de site du point de distribution, dont les points de distribution d'extraction, et pour PXE et la multidiffusion.

**Serveurs de système de site :**

- Point de distribution
  - Les points de distribution sur ce système d'exploitation ne prennent pas en charge la multidiffusion.
  - Les points de distribution sur ce système d'exploitation sont pris en charge pour PXE.
  - Les points de distribution prennent en charge plusieurs configurations différentes ayant chacune des exigences différentes. Dans certains cas, ces configurations prennent en charge l'installation sur des serveurs, mais aussi sur des systèmes d'exploitation clients. Pour plus d'informations sur les options disponibles pour les points de distribution, consultez Gérer le contenu et l'infrastructure de contenu.

## Windows Server 2008 avec SP2 (x86, x64) : Standard, Enterprise et Datacenter

Windows Server 2008 bénéficie désormais du support étendu au lieu du support standard, comme indiqué dans la Politique de support Microsoft. Pour plus d'informations sur la prise en charge à venir de ces systèmes d'exploitation utilisés comme serveurs de système de site avec Configuration Manager, consultez Systèmes d'exploitation serveur dépréciés.

Ce système d'exploitation n'est pas pris en charge pour les serveurs de site ou les rôles de système de site, à l'exception du point de distribution et du point de distribution d'extraction. Vous pouvez continuer à utiliser ce système d'exploitation comme point de distribution jusqu'à l'annonce de la dépréciation de ce support ou jusqu'à l'expiration de la période du support étendu de ce système d'exploitation. Pour plus d'informations, consultez Échec de l'installation de System Center Configuration Manager CB et LTSB sur Windows Server 2008.

**Serveurs de système de site :**

- Point de distribution
  - Les points de distribution sur ce système d'exploitation ne prennent pas en charge la multidiffusion.
  - Les points de distribution sur ce système d'exploitation sont pris en charge pour PXE, mais ne prennent pas en charge le démarrage réseau des ordinateurs clients en mode EFI. Les ordinateurs clients avec un démarrage BIOS ou EFI en mode hérité sont pris en charge.
  - Les points de distribution prennent en charge plusieurs configurations différentes ayant chacune des exigences différentes. Dans certains cas, ces configurations prennent en charge l'installation sur des serveurs, mais aussi sur des systèmes d'exploitation clients. Pour plus d'informations sur les options disponibles pour les points de distribution, consultez Gérer le contenu et l'infrastructure de contenu.

## Windows 10 (x86, x64) : Professionnel et Entreprise

**Serveurs de système de site :**

- Point de distribution
  - Les points de distribution sur ce système d'exploitation ne sont pas pris en charge pour PXE.
  - Les points de distribution sur cette version du système d'exploitation ne prennent pas en charge la multidiffusion.
  - Les points de distribution prennent en charge plusieurs configurations différentes ayant chacune des exigences différentes. Dans certains cas, ces configurations prennent en charge l'installation sur des serveurs, mais aussi sur des systèmes d'exploitation clients. Pour plus d'informations sur les options disponibles pour les points de distribution, consultez Gérer le contenu et l'infrastructure de contenu.

## Windows 8.1 (x86, x64) : Professionnel et Entreprise

**Serveurs de système de site :**

- Point de distribution
  - Les points de distribution sur ce système d'exploitation ne sont pas pris en charge pour PXE.
  - Les points de distribution sur cette version du système d'exploitation ne prennent pas en charge la multidiffusion.
  - Les points de distribution prennent en charge plusieurs configurations différentes ayant chacune des exigences différentes. Dans certains cas, ces configurations prennent en charge l'installation sur des serveurs, mais aussi sur des systèmes d'exploitation clients. Pour plus d'informations sur les options disponibles pour les points de distribution, consultez Gérer le contenu et l'infrastructure de contenu.

## Windows 7 avec SP1 (x86, x64) : Professionnel, Entreprise et Édition Intégrale

**Serveurs de système de site :**

- Point de distribution
  - Les points de distribution sur ce système d'exploitation ne sont pas pris en charge pour PXE.
  - Les points de distribution sur cette version du système d'exploitation ne prennent pas en charge la multidiffusion.
  - Les points de distribution prennent en charge plusieurs configurations différentes ayant chacune des exigences différentes. Dans certains cas, ces configurations prennent en charge l'installation sur des serveurs, mais aussi sur des systèmes d'exploitation clients. Pour plus d'informations sur les options disponibles pour les points de distribution, consultez Gérer le contenu et l'infrastructure de contenu.

## Installation minimale de Windows Server, version 1803

À compter de Configuration Manager 1802, Windows Server, version 1803 est pris en charge pour une utilisation en tant que point de distribution avec les restrictions suivantes :

- Seule la version 64 bits est prise en charge.
- Les points de distribution sur ce système d'exploitation ne prennent pas en charge PXE ou la multidiffusion.

## Installation minimale de Windows Server, version 1709

À compter de Configuration Manager 1710, Windows Server, version 1709 est pris en charge pour une utilisation en tant que point de distribution avec les restrictions suivantes :

- Seule la version 64 bits est prise en charge.
- Les points de distribution sur ce système d'exploitation ne prennent pas en charge PXE ou la multidiffusion.

## Installation minimale de Windows Server 2016

Avec le correctif cumulatif proposé dans l'article KB3186654, ce système d'exploitation est pris en charge pour être utilisé comme point de distribution avec les limitations suivantes :

- Seule la version 64 bits est prise en charge.
- Les points de distribution sur ce système d'exploitation ne prennent pas en charge PXE ou la multidiffusion.

## Installation minimale de Windows Server 2012 R2

L'installation minimale de Windows Server 2012 R2 est prise en charge pour une utilisation comme point de distribution avec les limitations suivantes :

- Seule la version 64 bits est prise en charge.
- Les points de distribution sur ce système d'exploitation ne prennent pas en charge PXE ou la multidiffusion.

## Installation minimale de Windows Server 2012

L'installation minimale de Windows Server 2012 est prise en charge pour une utilisation comme point de distribution avec les limitations suivantes :

- Seule la version 64 bits est prise en charge.
- Les points de distribution sur ce système d'exploitation ne prennent pas en charge PXE ou la multidiffusion.

# Systèmes d'exploitation pris en charge pour les clients et les appareils pour System Center Configuration Manager

10/07/2018 • 17 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Configuration Manager prend en charge l'installation de logiciels clients sur différents ordinateurs Windows, Mac, Linux et UNIX.

**Conditions requises et limitations pour tous les clients :**

- La modification du type de démarrage ou des paramètres **Se connecter en tant que** pour un service Configuration Manager n'est pas prise en charge et peut empêcher les services clés de s'exécuter correctement.
- L'installation ou l'exécution du client Configuration Manager pour Linux ou UNIX, ou du client pour Mac sur des ordinateurs sous un autre compte que le compte racine n'est pas prise en charge. Cela peut empêcher l'exécution correcte de certains services clés.

## Ordinateurs Windows

Vous pouvez utiliser le client Configuration Manager inclus dans Configuration Manager pour gérer les systèmes d'exploitation Windows suivants. Pour plus d'informations, consultez Guide pratique pour déployer des clients sur des ordinateurs Windows dans System Center Configuration Manager.

**Systèmes d'exploitation pris en charge :**

- **Windows Server 2016** : Standard, Datacenter [1]
  - Ce système d'exploitation est pris en charge à compter de Configuration Manager version 1606, avec le correctif cumulatif KB3186654 (ou la version de base de référence 1606 publiée en octobre 2016).
- **Windows Storage Server 2016** : Workgroup, Standard
- **Windows Server 2012 R2** (x64) : Standard, Datacenter [1]
- **Windows Storage Server 2012 R2** (x64)
- **Windows Server 2012** (x64) : Standard, Datacenter [1]
- **Windows Storage Server 2012** (x64)
- **Windows Server 2008 R2 avec SP1** (x64) : Standard, Enterprise, Datacenter [1]
- **Windows Storage Server 2008 R2** (x86, x64) : Workgroup, Standard, Enterprise
- **Windows Server 2008 avec SP2** (x86, x64) : Standard, Enterprise, Datacenter [1]
- **Windows 10**Consultez Prise en charge des versions de Windows 10 pour plus d'informations sur les différentes versions commerciales de Windows 10 qui sont prises en charge par les différentes versions de Configuration Manager.
- **Windows 8.1** (x86, x64) : Professionnel, Entreprise

- **Windows 7 avec SP1** (x86, x64) : Professionnel, Entreprise et Édition Intégrale
- **Installation minimale de Windows Server, version 1709** (x64) [2]
  - Ce système d'exploitation est pris en charge depuis la version 1710.
- **Installation minimale de Windows Server 2016** (x64) [2]
  - Ce système d'exploitation est pris en charge à compter de la version 1606, avec le correctif cumulatif KB3186654 (ou la version de base de référence 1606 publiée en octobre 2016).
- **Installation minimale de Windows Server 2012 R2** (x64) [2]
- **Installation minimale de Windows Server 2012** (x64) [2]
- **Installation minimale de Windows Server 2008 R2 (sans Service Pack ou avec SP1)** (x64)
- **Installation minimale de Windows Server 2008 SP2** (x86, x64)

[1] Les versions Datacenter sont prises en charge, mais ne sont pas certifiées pour Configuration Manager. Les correctifs ne sont pas pris en charge pour résoudre les problèmes spécifiques de l'édition Windows Server Datacenter.

[2] Pour prendre en charge l'installation Push du client, l'ordinateur exécutant cette version du système d'exploitation doit exécuter le service de rôle Serveur de fichiers pour le rôle serveur Services de fichiers et de stockage. Pour plus d'informations sur l'installation des fonctionnalités Windows sur un ordinateur Server Core, consultez Installer des rôles et fonctionnalités de serveur sur un serveur en mode d'installation minimale dans la bibliothèque TechNet de Windows Server 2012.

## Ordinateurs Windows Embedded

Vous pouvez gérer les appareils Windows Embedded en installant le logiciel client Configuration Manager sur ceux-ci. Pour plus d'informations, consultez Planification du déploiement de clients sur des appareils Windows Embedded dans System Center Configuration Manager.

**Configuration requise et limitations :**

- Toutes les fonctionnalités du client sont prises en charges sur les systèmes Windows Embedded qui ne disposent pas de filtres d'écriture activés.
- Les clients qui utilisent l'un des éléments suivants sont pris en charge pour toutes les fonctionnalités, à l'exception de la gestion de l'alimentation :
  - Filtres d'écriture améliorés (EWF)
  - Filtres d'écriture basés sur des fichiers RAM (FBWF)
  - Filtres d'écriture unifiés (UWF)
- Le catalogue des applications n'est pris en charge pour aucun appareil Windows Embedded.
- Pour pouvoir surveiller les programmes malveillants détectés sur les appareils Windows Embedded basés sur Windows XP, vous devez installer le package de script Microsoft Windows WMI sur l'appareil. Utilisez Windows Embedded Target Designer pour installer ce package. Les fichiers **WBEMDISP.DLL** et **WBEMDISP.TLB** doivent exister et être inscrits dans le dossier **%windir%\System32\WBEM** sur l'appareil intégré pour garantir que les programmes malveillants sont signalés.

**Systèmes d'exploitation pris en charge :**

- **Windows 10 Entreprise** (x86, x64)

- **Windows 10 IoT Entreprise** (x86, x64)
- **Windows Embedded 8.1 Industry** (x86, x64)
- **Windows Embedded 8 Standard** (x86, x64)
- **Windows Thin PC** (x86, x64)
- **Windows Embedded POSReady 7** (x86, x64)
- **Windows Embedded Standard 7 avec SP1** (x86, x64)

Les systèmes d'exploitation suivants sont basés sur Windows XP Embedded et ne sont pris en charge qu'avec la version 1610 et les versions antérieures de Configuration Manager. À partir de la version 1702, ces systèmes d'exploitation embarqués ne sont plus pris en charge.

- **WEPOS 1.1 avec SP3** (x86)
- **Windows Embedded POSReady 2009** (x86, x64)
- **Windows Fundamentals for Legacy PCs (WinFLP)** (x86)
- **Windows XP Embedded SP3** (x86)
- **Windows Embedded Standard 2009** (x86)

## Ordinateurs Windows CE

Vous pouvez gérer les appareils Windows CE avec le client hérité d'appareil mobile Configuration Manager inclus dans Configuration Manager.

**Configuration requise et limitations**

- L'installation du client d'appareil mobile nécessite 0,78 Mo d'espace de stockage. La connexion peut nécessiter jusqu'à 256 Ko d'espace de stockage supplémentaire.
- Les fonctionnalités de ces appareils mobiles varient selon la plateforme et le type de client. Pour plus d'informations sur les fonctions de gestion prises en charge, consultez Choisir une solution de gestion d'appareils pour System Center Configuration Manager.

**Systèmes d'exploitation pris en charge :**

- Windows CE 7.0 (processeurs ARM et x86)

**Langues prises en charge :**

- Chinois (simplifié et traditionnel)
- Anglais (États-Unis)
- Français (France)
- Allemand
- Italien
- Japonais
- Coréen
- Portugais (Brésil)
- Russe

- Espagnol (Espagne)

## Ordinateurs Mac

Vous pouvez gérer les ordinateurs Mac OS X à l'aide du client Configuration Manager pour Mac.

Le package d'installation de client Mac n'est pas fourni avec le support d'installation de Configuration Manager. Téléchargez les **clients pour d'autres systèmes d'exploitation** à partir du Centre de téléchargement Microsoft.

Pour plus d'informations, consultez Guide pratique pour déployer des clients sur des ordinateurs Mac dans System Center Configuration Manager.

**Versions prises en charge :**

- **Mac OS X 10.6** (Snow Leopard)
- **Mac OS X 10.7** (Lion)
- **Mac OS X 10.8** (Mountain Lion)
- **Mac OS X 10.9** (Mavericks)
- **Mac OS X 10.10** (Yosemite)
- **Mac OS X 10.11** (El Capitan)
- **Mac OS X 10.12** (macOS Sierra)
- **Mac OS X 10.13** (macOS High Sierra)

## Serveurs Linux et UNIX

Vous pouvez gérer les serveurs Linux et UNIX avec le client Configuration Manager pour Linux et UNIX.

Les packages d'installation du client Linux et UNIX ne sont pas fournis avec le média Configuration Manager. Téléchargez les **clients pour d'autres systèmes d'exploitation** à partir du Centre de téléchargement Microsoft. En plus des packages d'installation de client, le téléchargement du client comprend le script qui gère l'installation du client sur chaque ordinateur.

**Configuration requise et limitations :**

- Pour vérifier les dépendances des fichiers du système d'exploitation pour le client pour Linux et UNIX, consultez Conditions préalables pour le déploiement du client pour les serveurs Linux et UNIX.
- Pour obtenir une vue d'ensemble des fonctionnalités de gestion prises en charge sur Linux ou UNIX, consultez Guide pratique pour déployer des clients sur des serveurs UNIX et Linux dans System Center Configuration Manager.
- Pour versions prises en charge de Linux et UNIX, la version répertoriée inclut toutes les versions mineures suivantes. Par exemple, CentOS version 6 inclut CentOS 6.3. De même, la prise en charge d'un système d'exploitation qui utilise des Service Packs (comme SUSE Linux Enterprise Server 11 SP1), inclut les Service Packs suivants pour cette version du système d'exploitation.
- Pour plus d'informations sur les packages d'installation client et l'agent universel, consultez Guide pratique pour déployer des clients sur des serveurs UNIX et Linux dans System Center Configuration Manager.

**Versions prises en charge** : les versions suivantes sont prises en charge en utilisant le fichier .tar indiqué.

**AIX**

| | |
|---|---|
| Version 6.1 (Power) | ccm-Aix61ppc.<version>.tar |
| Version 7.1 (Power) | ccm-Aix71ppc.<version>.tar |

**CentOS**

| | |
|---|---|
| Version 5 x86 | ccm-Universalx86.<version>.tar |
| Version 5 x64 | ccm-Universalx64.<version>.tar |
| Version 6 x86 | ccm-Universalx86.<version>.tar |
| Version 6 x64 | ccm-Universalx64.<version>.tar |
| Version 7 x64 | ccm-Universalx64.<version>.tar |

**Debian**

| | |
|---|---|
| Version 5 x86 | ccm-Universalx86.<version>.tar |
| Version 5 x64 | ccm-Universalx64.<version>.tar |
| Version 6 x86 | ccm-Universalx86.<version>.tar |
| Version 6 x64 | ccm-Universalx64.<version>.tar |
| Version 7 x86 | ccm-Universalx86.<version>.tar |
| Version 7 x64 | ccm-Universalx64.<version>.tar |
| Version 8 x86 | ccm-Universalx86.<version>.tar |
| Version 8 x64 | ccm-Universalx64.<version>.tar |

**HP-UX**

| | |
|---|---|
| Version 11iv3 IA64 | ccm-HpuxB.11.31i64.<version>.tar |

**Oracle Linux**

| | |
|---|---|
| Version 5 x86 | ccm-Universalx86.<version>.tar |
| Version 5 x64 | ccm-Universalx64.<version>.tar |
| Version 6 x86 | ccm-Universalx86.<version>.tar |

| | |
|---|---|
| Version 6 x64 | ccm-Universalx64.<version>.tar |
| Version 7 x64 | ccm-Universalx64.<version>.tar |

**Red Hat Enterprise Linux (RHEL)**

| | |
|---|---|
| Version 5 x86 | ccm-Universalx86.<version>.tar |
| Version 5 x64 | ccm-Universalx64.<version>.tar |
| Version 6 x86 | ccm-Universalx86.<version>.tar |
| Version 6 x64 | ccm-Universalx64.<version>.tar |
| Version 7 x64 | ccm-Universalx64.<version>.tar |

**Solaris**

| | |
|---|---|
| Version 10 x86 | ccm-Sol10x86.<version>.tar |
| SPARC version 10 | ccm-Sol10sparc.<version>.tar |
| Version 11 x86 | ccm-Sol11x86.<version>.tar |
| SPARC version 11 | ccm-Sol11sparc.<version>.tar |

**SUSE Linux Enterprise Server (SLES)**

| | |
|---|---|
| Version 10 SP1 x86 | ccm-Universalx86.<version>.tar |
| Version 10 SP1 x64 | ccm-Universalx64.<version>.tar |
| Version 11 SP1 x86 | ccm-Universalx86.<version>.tar |
| Version 11 SP1 x64 | ccm-Universalx64.<version>.tar |
| Version 12 x64 | ccm-Universalx64.<version>.tar |

**Ubuntu**

| | |
|---|---|
| Version 10.04 LTS x86 | ccm-Universalx86.<version>.tar |
| Version 10.04 LTS x64 | ccm-Universalx64.<version>.tar |
| Version 12.04 LTS x86 | ccm-Universalx86.<version>.tar |

| | |
|---|---|
| Version 12.04 LTS x64 | ccm-Universalx64.<version>.tar |
| Version 14.04 LTS x86 | ccm-Universalx86.<version>.tar |
| Version 14.04 LTS x64 | ccm-Universalx64.<version>.tar |
| Version 16.04 LTS x86 | ccm-Universalx86.<version>.tar |
| Version 16.04 LTS x64 | ccm-Universalx64.<version>.tar |

## Appareils mobiles inscrits par Microsoft Intune

Pour plus d'informations sur les ordinateurs et les appareils que vous pouvez gérer quand vous intégrez Microsoft Intune à Configuration Manager, consultez les deux rubriques suivantes dans la bibliothèque de la documentation Microsoft Intune :

- Fonctionnalités de gestion des appareils mobiles dans Microsoft Intune
- Fonctionnalités de gestion des PC Windows dans Microsoft Intune

## Gestion des appareils mobiles locale

Configuration Manager offre des fonctionnalités intégrées permettant de gérer des appareils locaux sans devoir installer de logiciel client. Pour plus d'informations, consultez Gérer des appareils mobiles avec une infrastructure locale dans System Center Configuration Manager.

**Configuration requise et limitations :**

- Vous devez configurer le **point de connexion de service** sur le site de plus haut niveau de votre hiérarchie.

**Systèmes d'exploitation pris en charge :**

- **Windows 10 Professionnel** (x86, x64)
- **Windows 10 Entreprise** (x86, x64)
- **Windows 10 IoT Entreprise** (x86, x64)
- **Windows 10 Mobile**
- **Windows 10 Mobile Entreprise**
- **Windows 10 IoT Mobile Entreprise**
- **Windows 10 Collaboration pour Surface Hub**

## Connecteur Exchange Server

Configuration Manager prend en charge une gestion limitée des appareils qui se connectent à Exchange Server, sans installation du client Configuration Manager. Pour plus d'informations, consultez Gérer les appareils mobiles avec System Center Configuration Manager et Exchange.

**Configuration requise et limitations :**

- Configuration Manager assure une gestion limitée des appareils mobiles quand vous utilisez des appareils avec le connecteur Exchange Server pour Exchange Active Sync qui se connectent à un serveur exécutant Exchange Server ou Exchange Online.

- Pour plus d'informations sur les fonctions de gestion prises en charge par Configuration Manager pour les appareils mobiles gérés par le connecteur Exchange Server, consultez Déterminer comment gérer des appareils mobiles dans Configuration Manager.

**Versions d'Exchange Server prises en charge** :

- **Exchange Server 2010 SP1**
- **Exchange Server 2010 SP2**
- **Exchange Server 2013**
- **Exchange Online (Office 365)** : Inclut Business Productivity Online Standard Suite

# Prise en charge de Windows 10 dans System Center Configuration Manager

10/07/2018 • 5 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Découvrez les versions de Windows 10 prises en charge par Configuration Manager, notamment :

- Windows 10 comme client Configuration Manager
- Kit de déploiement et d'évaluation Windows (ADK) pour Windows 10

## Windows 10 comme client

Configuration Manager tente d'assurer une prise en charge comme client pour chaque nouvelle version de Windows 10 dès que possible après sa publication. Étant donné que les produits ont des calendriers de développement et de publication distincts, la prise en charge assurée par Configuration Manager dépend du moment de leur mise en circulation respective.

Par exemple, une version de Configuration Manager est supprimée de la matrice quand la prise en charge de cette version se termine. De même, la prise en charge de versions de Windows 10 comme Enterprise 2015 LTSB or 1511 est supprimée de la matrice quand elles seront retirées de la prise en charge. Pour plus d'informations, consultez Systèmes d'exploitation dépréciés.

- Ces informations viennent s'ajouter à Systèmes d'exploitation pris en charge pour les clients et appareils.
- Si vous utilisez LTSB (Long Term Servicing Branch) de Configuration Manager, consultez Configurations prises en charge pour Long Term Servicing Branch.

Le tableau suivant liste les versions de Windows 10 que vous pouvez utiliser comme client avec différentes versions de Configuration Manager.

| VERSION DE WINDOWS 10 | CONFIGURATION MANAGER 1706 | CONFIGURATION MANAGER 1710 | CONFIGURATION MANAGER 1802 |
|---|---|---|---|
| Enterprise 2015 LTSB | ✓ | ✓ | ✓ |
| Entreprise 2016 LTSB | ✓ | ✓ | ✓ |
| 1607 (*voir éditions*) | ✓ 1 | ✓ 1 | ✓ 1 |
| 1703 (*voir éditions*) | ✓ | ✓ | ✓ |
| 1709 (*voir éditions*) | BC | ✓ | ✓ |
| 1803 (*voir éditions*) | ✗ | ✗ | ✓ |

**Éditions :** Entreprise, Professionnel, Éducation, Professionnel Éducation

[1] Pour plus d'informations, consultez Infos-clés sur le cycle de vie Windows et la section « Extension de maintenance pour les éditions Entreprise et Éducation ».

| CLÉ |
| --- |
| ✅ = **Prise en charge** |
| 🅱️ = **Rétrocompatible**<br>Les fonctionnalités de gestion du client existantes devraient fonctionner avec cette nouvelle version Windows 10. Par exemple, l'inventaire matériel, l'inventaire logiciel et les mises à jour logicielles. Nous documentons tous problèmes connus ou mises en garde.<br><br>Cette approche vous offre la possibilité de déployer et de gérer de nouvelles versions de Windows immédiatement avec prise en charge de la compatibilité des applications et sans nécessiter de nouvelle version de mise à jour de Configuration Manager. |
| ❌ = **Non pris en charge** |

> **NOTE**
> À compter de la version 1802, Configuration Manager prend en charge le client sur les appareils Windows 10 ARM64. Les fonctionnalités de gestion du client existantes devraient fonctionner avec ces nouveaux appareils, par exemple, l'inventaire matériel et logiciel, les mises à jour logicielles et la gestion des applications. Le déploiement de système d'exploitation n'est pas pris en charge pour le moment.

## Windows 10 ADK

Quand vous déployez des systèmes d'exploitation avec Configuration Manager, le Windows ADK est une dépendance externe obligatoire.

Le tableau suivant répertorie les versions du Windows 10 ADK que vous pouvez utiliser avec différentes versions de Configuration Manager.

| VERSION DE WINDOWS 10 ADK | CONFIGURATION MANAGER 1706 | CONFIGURATION MANAGER 1710 | CONFIGURATION MANAGER 1802 |
| --- | --- | --- | --- |
| 1703 | ✅ | 🅱️ | 🅱️ |
| 1709 | ✅ | ✅ | ✅ |
| 1803 | ❌ | ❌ | ✅ |

| CLÉ |
| --- |
| ✅ = **Prise en charge**<br>Microsoft recommande d'utiliser le Windows ADK qui correspond à la version de Windows que vous déployez. Par exemple, utilisez le Windows ADK pour Windows 10 version 1703 quand vous déployez Windows 10 version 1703. Pour plus d'informations sur la prise en charge du composant Windows ADK, consultez Plateformes prises en charge par DISM et Exigences de l'outil USMT. |
| 🅱️ = **Rétrocompatible**<br>Cette combinaison n'est pas testée mais devrait fonctionner. Nous documentons tous problèmes connus ou mises en garde. |

| CLÉ |
| --- |
| ❌ = **Non pris en charge** |

> **NOTE**
> Configuration Manager prend uniquement en charge les composants x86 et amd64 de Windows 10 ADK. Il ne prend pas en charge les composants ARM ou ARM64 pour l'instant.

# Systèmes d'exploitation pris en charge pour les consoles System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Pour prendre en charge la console System Center Configuration Manager, les systèmes d'exploitation suivants nécessitent au minimum .NET Framework 4.5.2. L'exception est Windows 10 qui requiert au minimum .NET Framework 4.6.

- **Windows Server 2016** : Standard, Datacenter
  - Windows Server 2016 est pris en charge à compter de Configuration Manager version 1606, avec le correctif cumulatif KB3186654 (ou la version de référence 1606 publiée en octobre 2016).
- **Windows Server 2012 R2** (x64) : Standard, Datacenter
- **Windows Server 2012** (x64) : Standard, Datacenter
- **Windows Server 2008 R2 avec SP1** (x64) : Standard, Entreprise, Datacenter
- **Windows 10** (x86, x64) : Professionnel, Entreprise
- **Windows 8.1** (x86, x64) : Professionnel, Entreprise
- **Windows 7 avec SP1** (x86, x64) : Professionnel, Entreprise, Édition Intégrale

# Matériel recommandé pour System Center Configuration Manager

29/06/2018 • 15 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les recommandations suivantes sont des indications destinées à vous aider à adapter votre environnement System Center Configuration Manager pour qu'il prenne en charge un déploiement plus complexe de sites, de systèmes de site et de clients. Elles ne sont pas prévues pour couvrir toutes les configurations possibles de site et de hiérarchie.

Aidez-vous des informations des sections suivantes pour prévoir le matériel capable de répondre aux charges de traitement des clients et des sites qui utilisent les fonctionnalités de Configuration Manager disponibles avec les configurations par défaut.

## Systèmes de site

Cette section présente les configurations matérielles recommandées pour les systèmes de site Configuration Manager pour les déploiements prenant en charge le nombre maximal de clients et utilisant la plupart ou l'ensemble des fonctionnalités de Configuration Manager. Les déploiements qui ne prennent pas en charge le nombre maximal de clients et qui n'utilisent pas toutes les fonctionnalités disponibles nécessitent généralement moins de ressources informatiques. En règle générale, les facteurs clés qui limitent les performances de l'ensemble du système sont les suivants, par ordre d'importance :

1. Performances d'E/S du disque
2. Mémoire disponible
3. Processeur

Pour des performances optimales, utilisez des configurations RAID 10 pour tous les lecteurs de données et une connectivité réseau Ethernet 1 Gbit/s.

**Serveurs de site**

| CONFIGURATION DE SITE | CŒURS DE PROCESSEUR | MÉMOIRE (GO) | % D'ALLOCATION DE MÉMOIRE POUR SQL SERVER |
|---|---|---|---|
| Serveur de site principal autonome avec un rôle site de base de données sur le même serveur[1] | 16 | 96 | 80 |
| Serveur de site principal autonome avec une base de données de site distante | 8 | 16 | - |
| Serveur de bases de données distant pour un site principal autonome | 16 | 72 | 90 |

| CONFIGURATION DE SITE | CŒURS DE PROCESSEUR | MÉMOIRE (GO) | % D'ALLOCATION DE MÉMOIRE POUR SQL SERVER |
|---|---|---|---|
| Serveur de site d'administration centrale avec un rôle site de base de données sur le même serveur[1] | 20 | 128 | 80 |
| Serveur de site d'administration centrale avec une base de données de site distante | 8 | 16 | - |
| Serveur de bases de données distant pour un site d'administration centrale | 16 | 96 | 90 |
| Site principal enfant avec un rôle site de base de données sur le même serveur | 16 | 96 | 80 |
| Serveur de site principal enfant avec une base de données de site distante | 8 | 16 | - |
| Serveur de bases de données distant pour un site principal enfant | 16 | 72 | 90 |
| Serveur de site secondaire | 8 | 16 | - |

[1] Quand le serveur de site et SQL Server sont installés sur le même ordinateur, le déploiement prend en charge les tailles et échelles maximales pour les sites et les clients. Toutefois, cette configuration peut limiter les options de haute disponibilité pour System Center Configuration Manager, comme l'utilisation d'un cluster SQL Server. De plus, en raison d'un plus grand nombre d'E/S nécessaire pour prendre en charge l'exécution de SQL Server et du serveur de site Configuration Manager sur le même ordinateur, nous vous conseillons d'utiliser une configuration avec une machine SQL Server distante dans les déploiements de plus grande taille.

**Serveurs de système de site distants**

Les indications ci-dessous concernent les ordinateurs qui ont un seul rôle de système de site. Ajustez les valeurs indiquées si vous installez plusieurs rôles de système de site sur le même ordinateur.

| RÔLE DE SYSTÈME DE SITE | CŒURS DE PROCESSEUR | MÉMOIRE (GO) | ESPACE DISQUE (GO) |
|---|---|---|---|
| Point de gestion | 4 | 8 | 50 |
| Point de distribution | 2 | 8 | Espace disque exigé par le système d'exploitation et pour stocker le contenu que vous déployez |
| Catalogue d'applications, avec le service Web et le site Web sur l'ordinateur du système de site | 4 | 16 | 50 |

| RÔLE DE SYSTÈME DE SITE | CŒURS DE PROCESSEUR | MÉMOIRE (GO) | ESPACE DISQUE (GO) |
|---|---|---|---|
| Point de mise à jour logicielle[1] | 8 | 16 | Espace disque exigé par le système d'exploitation et pour stocker les mises à jour que vous déployez |
| Tous les autres rôles de système de site | 4 | 8 | 50 |

[1] L'ordinateur qui héberge un point de mise à jour logicielle nécessite les configurations suivantes pour les pools d'applications IIS :

- Augmenter la **longueur de file d'attente WsusPool** à **2000**.
- Multiplier par quatre la **limite de mémoire privée WsusPool**, ou lui affecter la valeur **0** (illimitée).

**Espace disque pour les systèmes de site**

L'allocation et la configuration de disque contribuent aux performances de Configuration Manager. Comme chaque environnement Configuration Manager est différent, ajustez les valeurs indiquées ci-dessous en fonction de vos besoins.

Pour des performances optimales, placez chaque objet sur un volume RAID séparé et dédié. Pour tous les volumes de données (Configuration Manager et ses fichiers de base de données), utilisez RAID 10 pour des performances optimales.

| UTILISATION DES DONNÉES | ESPACE DISQUE MINIMUM | 25 000 CLIENTS | 50 000 CLIENTS | 100 000 CLIENTS | 150 000 CLIENTS | 700 000 CLIENTS (SITE D'ADMINISTRATION CENTRALE) |
|---|---|---|---|---|---|---|
| Système d'exploitation | Consultez les conseils pour le système d'exploitation. | Consultez les conseils pour le système d'exploitation. | Consultez les conseils pour le système d'exploitation. | Consultez les conseils pour le système d'exploitation. | Consultez les conseils pour le système d'exploitation. | Consultez les conseils pour le système d'exploitation. |
| Fichiers journaux et d'application de Configuration Manager | 25 Go | 50 Go | 100 Go | 200 Go | 300 Go | 200 Go |
| Fichier .mdf de base de données du site | 75 Go par tranche de 25 000 clients | 75 Go | 150 Go | 300 Go | 500 Go | 2 To |
| Fichier .ldf de base de données du site | 25 Go par tranche de 25 000 clients | 25 Go | 50 Go | 100 Go | 150 Go | 100 Go |
| Fichiers de base de données temporaires (.mdf et .ldf) | En fonction des besoins | En fonction des besoins | En fonction des besoins | En fonction des besoins | En fonction des besoins | En fonction des besoins |

| UTILISATION DES DONNÉES | ESPACE DISQUE MINIMUM | 25 000 CLIENTS | 50 000 CLIENTS | 100 000 CLIENTS | 150 000 CLIENTS | 700 000 CLIENTS (SITE D'ADMINISTRATION CENTRALE) |
|---|---|---|---|---|---|---|
| Contenu (partages de point de distribution) | En fonction des besoins[1] | En fonction des besoins[1] | En fonction des besoins[1] | En fonction des besoins[1] | En fonction des besoins[1] | En fonction des besoins[1] |

[1] Les instructions relatives à l'espace disque n'incluent pas l'espace requis pour le contenu situé dans la bibliothèque de contenu sur le serveur de site ou les points de distribution. Pour plus d'informations sur la planification de la bibliothèque de contenu, consultez Bibliothèque de contenu.

En plus des indications précédentes, prenez en compte les recommandations suivantes pour prévoir l'espace disque nécessaire :

- Chaque client nécessite environ 5 Mo d'espace.
- Quand vous planifiez la taille de la base de données temporaire pour un site principal, prévoyez une taille combinée de 25 à 30 % du fichier .mdf de la base de données du site. La taille réelle peut être beaucoup plus petite ou plus grande en fonction des performances du serveur de site et du volume de données entrantes sur de courtes et longues périodes.

  > **NOTE**
  > Quand vous avez 50 000 clients ou plus sur un site, prévoyez d'utiliser au moins quatre fichiers .mdf de base de données temporaire.

- La taille de la base de données temporaire pour un site d'administration centrale est généralement beaucoup plus petite que celle d'un site principal.
- La base de données d'un site secondaire a les limitations de taille suivantes :
  - SQL Server 2012 Express : 10 Go
  - SQL Server 2014 Express : 10 Go

# Clients

Cette section présente les configurations matérielles recommandées pour les ordinateurs que vous gérez à l'aide du logiciel client Configuration Manager.

**Client pour les ordinateurs Windows**

Le tableau suivant indique la configuration minimale requise pour les ordinateurs Windows gérés à l'aide de Configuration Manager, y compris les systèmes d'exploitation embarqués :

- **Processeur et mémoire :** reportez-vous à la configuration de processeur et mémoire RAM requise pour le système d'exploitation de l'ordinateur.
- **Espace disque :** 500 Mo d'espace disque disponible, avec 5 Go recommandés pour le cache du client Configuration Manager. L'espace disque requis est moindre si vous utilisez des paramètres personnalisés pour installer le client Configuration Manager :
  - Utilisez la propriété /skipprereq de la ligne de commande de CCMSetup pour éviter d'installer des fichiers dont le client n'a pas besoin. Par exemple, exécutez `CCMSetup.exe /skipprereq:silverlight.exe` si le client n'utilise pas le catalogue d'applications. À

compter de Configuration Manager 1802, Silverlight n'est plus installé automatiquement.

- Utilisez la propriété SMSCACHESIZE de Client.msi pour définir un fichier de cache d'une taille inférieure à la taille par défaut de 5 120 Mo. La taille minimale est de 1 Mo. Par exemple, `CCMSetup.exe SMSCachesize=2` crée un cache d'une taille de 2 Mo.

Pour plus d'informations sur ces paramètres d'installation du client, consultez À propos des propriétés d'installation du client.

> **TIP**
> L'installation du client avec un minimum d'espace disque est utile pour les appareils Windows Embedded qui ont généralement des tailles de disque plus petites que les ordinateurs Windows standard.

Voici des configurations matérielles minimales supplémentaires pour les fonctionnalités facultatives dans Configuration Manager.

- **Déploiement du système d'exploitation :** 384 Mo de RAM
- **Centre logiciel :** processeur 500 MHz
- **Contrôle à distance :** Pentium 4 Hyper-Threaded 3 GHz (simple cœur) ou processeur comparable, avec au moins 1 Go de RAM pour une expérience optimale

**Client pour Linux et UNIX**

Le tableau suivant indique la configuration minimale requise pour les ordinateurs Linux et UNIX que vous gérez avec Configuration Manager.

| EXIGENCE | DÉTAILS |
|---|---|
| Processeur et mémoire | Reportez-vous à la configuration de processeur et mémoire RAM requise pour le système d'exploitation de l'ordinateur. |
| Espace disque | 500 Mo d'espace disque disponible, avec 5 Go recommandés pour le cache du client Configuration Manager. |
| Connectivité réseau | Les ordinateurs clients Configuration Manager doivent disposer d'une connexion réseau aux systèmes de site Configuration Manager pour en permettre la gestion. |

## Console Configuration Manager

La configuration requise indiquée dans le tableau ci-dessous s'applique à chaque ordinateur qui exécute la console Configuration Manager.

**Configuration matérielle minimale :**

- Intel i3 ou processeur comparable
- 2 Go de RAM
- 2 Go d'espace disque

| PARAMÈTRE PPP | RÉSOLUTION MINIMALE |
|---|---|
| 96 / 100 % | 1024 x 768 |

| PARAMÈTRE PPP | RÉSOLUTION MINIMALE |
|---|---|
| 120 /125 % | 1280 x 960 |
| 144 / 150 % | 1600 x 1200 |
| 196 / 200 % | 2500 x 1600 |

**Prise en charge de PowerShell :**

Quand vous installez la prise en charge de PowerShell sur un ordinateur qui exécute la console Configuration Manager, vous pouvez exécuter des applets de commande PowerShell sur cet ordinateur pour gérer Configuration Manager.

- PowerShell 3.0 ou ultérieur est pris en charge

En plus de PowerShell, WMF (Windows Management Framework) version 3.0 ou ultérieure est pris en charge.

## Déploiements de laboratoire

Utilisez les recommandations de configuration matérielle suivantes pour les déploiements de laboratoire et de test de Configuration Manager. Ces recommandations s'appliquent à tous les types de sites, avec un maximum de 100 clients :

| RÔLE | CŒURS DE PROCESSEUR | MÉMOIRE (GO) | ESPACE DISQUE (GO) |
|---|---|---|---|
| Serveur de site et de bases de données | 2 - 4 | 8 - 12 | 100 |
| Serveur de système de site | 1 - 4 | 2 - 4 | 50 |
| Client | 1 - 2 | 1 - 3 | 30 |

# Versions SQL Server prises en charge pour System Center Configuration Manager

26/06/2018 • 23 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Chaque site System Center Configuration Manager a besoin d'une version et d'une configuration de SQL Server prises en charge pour héberger la base de données du site.

## Emplacements et instances SQL Server

**Site d'administration centrale et sites principaux**

La base de données du site doit utiliser une installation complète de SQL Server.

SQL Server peut être à l'un de ces emplacements :

- L'ordinateur de serveur de site.
- Un ordinateur distant du serveur de site.

Les instances suivantes sont prises en charge :

- L'instance par défaut ou nommée de SQL Server.
- Des configurations d'instances multiples.
- Un cluster SQL Server. Consultez Utiliser un cluster SQL Server pour héberger la base de données de site.
- Un groupe de disponibilité SQL Server AlwaysOn. Cette option nécessite Configuration Manager version 1602 ou ultérieure. Pour plus d'informations, consultez SQL Server AlwaysOn pour une base de données de site à haut niveau de disponibilité pour System Center Configuration Manager.

**Sites secondaires**

La base de données du site peut utiliser l'instance par défaut d'une installation complète de SQL Server ou de SQL Server Express.

SQL Server doit se trouver sur l'ordinateur du serveur de site.

**Limitations de la prise en charge**

Les configurations suivantes ne sont pas prises en charge :

- Un cluster SQL Server dans une configuration de cluster d'équilibrage de la charge réseau (NLB)
- Un cluster SQL Server sur un volume partagé de cluster (CSV)
- La technologie de mise en miroir de base de données SQL Server et la réplication d'égal à égal

La réplication transactionnelle de SQL Server est prise en charge uniquement pour répliquer des objets sur des points de gestion configurés pour utiliser des réplicas de base de données.

## Versions SQL Server prises en charge

Dans une hiérarchie comprenant plusieurs sites, chaque site peut utiliser différentes versions de SQL Server pour héberger la base de données du site. Dès lors que les conditions suivantes sont réunies :

- Configuration Manager prend en charge les versions de SQL Server que vous utilisez.
- Les versions SQL Server que vous utilisez restent prises en charge par Microsoft.

- SQL Server prend en charge la réplication entre les deux versions de SQL Server. Par exemple, SQL Server ne prend pas en charge la réplication entre SQL Server 2008 R2 et SQL Server 2016.

Sauf indication contraire, les versions suivantes de SQL Server sont prises en charge avec toutes les versions System Center Configuration Manager actives. Si vous ajoutez la prise en charge d'une nouvelle version de SQL Server ou un Service Pack, la version de Configuration Manager qui ajoute cette prise en charge est indiquée. De même, si la prise en charge est dépréciée, recherchez plus d'informations sur les versions de Configuration Manager concernées.

La prise en charge d'un Service Pack de SQL Server spécifique inclut les mises à jour cumulatives, sauf si elles rompent la compatibilité descendante avec la version de base du Service Pack. Si aucune version du Service Pack n'est indiquée, la prise en charge s'applique à la version de SQL Server sans Service Pack. À l'avenir, si un Service Pack est fourni pour une version de SQL Server, une instruction de prise en charge distincte est déclarée avant que la nouvelle version du Service Pack ne soit prise en charge.

> **IMPORTANT**
> Si vous utilisez SQL Server Standard pour la base de données du site d'administration centrale, vous limitez le nombre total de clients qu'une hiérarchie peut prendre en charge. Consultez Taille et échelle en chiffres.

**SQL Server 2017 : Standard, Enterprise**

Vous pouvez utiliser cette version de SQL Server, avec au minimum la version de mise à jour cumulative 2, en commençant par Configuration Manager version 1710 pour les sites suivants :

- Un site d'administration centrale
- Un serveur de site principal
- Un site secondaire

**SQL Server 2016 SP2 : Standard, Enterprise**

Vous pouvez utiliser cette version de SQL Server sans version de mise à jour cumulative minimale pour les sites suivants :

- Un site d'administration centrale
- Un serveur de site principal
- Un site secondaire

**SQL Server 2016 SP1 : Standard, Enterprise**

Vous pouvez utiliser cette version de SQL Server sans version de mise à jour cumulative minimale pour les sites suivants :

- Un site d'administration centrale
- Un serveur de site principal
- Un site secondaire

**SQL Server 2016 : Standard, Enterprise**

Vous pouvez utiliser cette version de SQL Server sans version de mise à jour cumulative minimale pour les sites suivants :

- Un site d'administration centrale
- Un serveur de site principal
- Un site secondaire

**SQL Server 2014 SP2 : Standard, Enterprise**

Vous pouvez utiliser cette version de SQL Server sans version de mise à jour cumulative minimale pour les sites

suivants :

- Un site d'administration centrale
- Un serveur de site principal
- Un site secondaire

**SQL Server 2014 SP1 : Standard, Enterprise**

Vous pouvez utiliser cette version de SQL Server sans version de mise à jour cumulative minimale pour les sites suivants :

- Un site d'administration centrale
- Un serveur de site principal
- Un site secondaire

**SQL Server 2012 SP4 : Standard, Enterprise**

Vous pouvez utiliser cette version de SQL Server sans version de mise à jour cumulative minimale pour les sites suivants :

- Un site d'administration centrale
- Un serveur de site principal
- Un site secondaire

**SQL Server 2012 SP3 : Standard, Enterprise**

Vous pouvez utiliser cette version de SQL Server sans version de mise à jour cumulative minimale pour les sites suivants :

- Un site d'administration centrale
- Un serveur de site principal
- Un site secondaire

**SQL Server 2008 R2 SP3 : Standard, Enterprise, Datacenter**

Cette version de SQL Server n'est pas prise en charge depuis la version 1702.
Cette version de SQL Server reste prise en charge si vous utilisez une version de Configuration Manager antérieure à la version 1702.

Si elle est prise en charge par la version de Configuration Manager, vous pouvez utiliser cette version de SQL Server sans version de mise à jour cumulative minimale pour les sites suivants :

- Un site d'administration centrale
- Un serveur de site principal
- Un site secondaire

**SQL Server 2017 Express**

Vous pouvez utiliser cette version de SQL Server, avec au minimum la version de mise à jour cumulative 2, en commençant par Configuration Manager version 1710 pour les sites suivants :

- Un site secondaire

**SQL Server 2016 Express SP2**

Vous pouvez utiliser cette version de SQL Server sans version de mise à jour cumulative minimale pour les sites suivants :

- Un site secondaire

**SQL Server 2016 Express SP1**

Vous pouvez utiliser cette version de SQL Server sans version de mise à jour cumulative minimale pour les sites

suivants :

- Un site secondaire

**SQL Server 2016 Express**

Vous pouvez utiliser cette version de SQL Server sans version de mise à jour cumulative minimale pour les sites suivants :

- Un site secondaire

**SQL Server 2014 Express SP2**

Vous pouvez utiliser cette version de SQL Server sans version de mise à jour cumulative minimale pour les sites suivants :

- Un site secondaire

**SQL Server 2014 Express SP1**

Vous pouvez utiliser cette version de SQL Server sans version de mise à jour cumulative minimale pour les sites suivants :

- Un site secondaire

**SQL Server 2012 Express SP3**

Vous pouvez utiliser cette version de SQL Server sans version de mise à jour cumulative minimale pour les sites suivants :

- Un site secondaire

## Configurations requises pour SQL Server

Les éléments suivants sont nécessaires pour toutes les installations de SQL Server que vous utilisez pour une base de données de site (y compris SQL Server Express). Quand Configuration Manager installe SQL Server Express dans le cadre d'une installation de site secondaire, ces configurations sont créées automatiquement.

**Version d'architecture de SQL Server**

Configuration Manager requiert une version 64 bits de SQL Server pour héberger la base de données de site.

**Classement de base de données**

Sur chaque site, à la fois l'instance de SQL Server qui est utilisée pour le site et la base de données de site doivent utiliser le classement suivant : **SQL_Latin1_General_CP1_CI_AS**.

Configuration Manager prend en charge deux exceptions à ce classement pour satisfaire aux normes définies dans GB18030 pour une utilisation en Chine. Pour plus d'informations, consultez Prise en charge internationale dans System Center Configuration Manager.

**Niveau de compatibilité de la base de données**

Configuration Manager exige que le niveau de compatibilité de la base de données du site ne soit pas inférieur à la version de SQL Server la plus basse pris en charge pour votre version de Configuration Manager. Par exemple, depuis la version 1702, vous devez avoir un niveau de compatibilité de base de données supérieur ou égal à 110.

**Fonctionnalités SQL Server**

Seule la fonctionnalité **Services Moteur de base de données** est requise pour chaque serveur de site.

La réplication de la base de données Configuration Manager ne nécessite pas la fonctionnalité **Réplication SQL Server**. Toutefois, cette configuration de SQL Server est requise lorsque vous utilisez des réplicas de base de données pour les points de gestion de System Center Configuration Manager.

#### Authentification Windows

Configuration Manager nécessite l'**authentification Windows** pour valider les connexions à la base de données.

#### Instance SQL Server

Vous devez utiliser une instance dédiée de SQL Server pour chaque site. Il peut s'agir d'une **instance nommée** ou de **l'instance par défaut**.

#### Mémoire de SQL Server

Réservez de la mémoire pour SQL Server en utilisant SQL Server Management Studio et en définissant le paramètre **Mémoire minimale du serveur** sous **Options mémoire du serveur**. Pour plus d'informations sur la configuration de ce paramètre, consultez Procédure : définir une quantité fixe de mémoire (SQL Server Management Studio).

- **Pour un serveur de base de données installé sur le même ordinateur que le serveur du site :** limitez la mémoire pour SQL Server à 50-80 % de la mémoire système adressable disponible.
- **Pour un serveur de base de données dédié (distant du serveur de site) :** limitez la mémoire pour SQL Server à 80-90 % de la mémoire système adressable disponible.
- **Pour une réserve de mémoire pour le pool de mémoires tampons de chaque instance SQL Server en cours d'utilisation** :
  - Pour un site d'administration centrale, définissez un minimum de 8 gigaoctets (Go).
  - Pour un site principal, définissez un minimum de 8 gigaoctets (Go).
  - Pour un site secondaire, définissez un minimum de 4 gigaoctets (Go).

#### Déclencheurs imbriqués SQL

Lesdéclencheurs imbriqués SQL doivent être activés.

#### Intégration du CLR SQL Server

La base de données du site nécessite que le CLR (Common Language Runtime) SQL Server soit activé. Cette option est activée automatiquement lors de l'installation de Configuration Manager. Pour plus d'informations sur le CLR, consultez Présentation de l'intégration de CLR dans SQL Server.

## Configurations facultatives pour SQL Server

Les configurations suivantes sont facultatives pour chaque base de données utilisant une installation complète de SQL Server.

#### Service SQL Server

Vous pouvez configurer le service SQL Server pour s'exécuter avec les ressources suivantes :

- Un compte *d'utilisateur de domaine doté de droits restreints* :
  - Il s'agit d'une bonne pratique qui peut exiger que vous enregistriez manuellement le nom de principal du service (SPN) pour le compte.
- Le compte **système local** de l'ordinateur exécutant SQL Server :
  - Utilisez le compte système local pour simplifier le processus de configuration.
  - Quand vous utilisez le compte système local, Configuration Manager inscrit automatiquement le SPN pour le service SQL Server.
  - L'utilisation du compte système local pour le service SQL Server n'est pas une meilleure pratique SQL Server.

Si l'ordinateur qui exécute SQL Server n'utilise pas son compte système local pour exécuter le service SQL

Server, vous devez configurer le SPN du compte qui exécute le service SQL Server dans Active Directory Domain Services. (Quand le compte système est utilisé, le SPN est inscrit automatiquement.)

Pour plus d'informations sur les SPN pour la base de données du site, consultez Gérer le SPN pour le serveur de base de données du site dans l'article Modifier votre infrastructure System Center Configuration Manager.

Pour plus d'informations sur la façon de modifier le compte utilisé par le service SQL Server, consultez Modifier le compte de démarrage du service pour SQL Server (Gestionnaire de configuration SQL Server).

**SQL Server Reporting Services**

SQL Server Reporting Services est nécessaire pour installer un point de Reporting Services permettant de générer des rapports.

> **IMPORTANT**
> Une fois SQL Server mis à niveau à partir d'une version précédente, l'erreur suivante peut s'afficher : *Le Générateur de rapports n'existe pas*.
> Pour corriger cette erreur, vous devez réinstaller le rôle de système de site du point de Reporting Services.

**Ports SQL Server**

Pour la communication vers le moteur de base de données SQL Server et pour la réplication intersites, vous pouvez utiliser les configurations de port SQL Server par défaut ou spécifier des ports personnalisés :

- Les **communications intersites** font appel à SQL Server Service Broker, qui utilise le port TCP 4022 par défaut.
- Les **communications intrasite** entre le moteur de base de données SQL Server et les divers rôles de système de site Configuration Manager utilisent le port TCP 1433 par défaut. Les rôles de système de site suivants communiquent directement avec la base de données SQL Server :
  - Point de gestion
  - Ordinateur du fournisseur SMS
  - Point de Reporting Services
  - Serveur de site

Quand un ordinateur exécutant SQL Server héberge une base de données de plusieurs sites, chaque base de données doit utiliser une instance distincte de SQL Server. De plus, chaque instance doit être configurée pour utiliser un ensemble de ports unique.

> **WARNING**
> Configuration Manager ne prend pas en charge les ports dynamiques. Étant donné que les instances nommées de SQL Server utilisent par défaut des ports dynamiques pour les connexions au moteur de base de données, lorsque vous utilisez une instance nommée, vous devez configurer manuellement le port statique que vous souhaitez utiliser pour la communication intrasite.

Si un pare-feu est activé sur l'ordinateur exécutant SQL Server, assurez-vous qu'il est configuré pour autoriser les ports utilisés par votre déploiement et, à tous les emplacements du réseau, entre les ordinateurs qui communiquent avec SQL Server.

Pour obtenir un exemple montrant comment configurer SQL Server pour utiliser un port spécifique, consultez Configurer un serveur pour écouter un port TCP spécifique (Gestionnaire de configuration SQL Server) dans la bibliothèque TechNet relative à SQL Server.

## Options de mise à niveau pour SQL Server

Si vous devez mettre à niveau votre version de SQL Server, nous vous recommandons les méthodes suivantes, de la plus simple à la plus complexe.

1. Mise à niveau de SQL Server sur place (recommandé).
2. Installez une nouvelle version de SQL Server sur un nouvel ordinateur, puis utilisez l'option de déplacement de la base de données du programme d'installation de Configuration Manager pour pointer votre serveur de site vers la nouvelle version de SQL Server.
3. Utilisez la sauvegarde et la récupération. L'utilisation de la sauvegarde et la récupération pour un scénario de mise à niveau SQL est prise en charge. Vous pouvez ignorer l'exigence de contrôle de version SQL lorsque vous parcourez les Considérations à prendre en compte avant la récupération d'un site.

# Domaines Active Directory pris en charge pour System Center Configuration Manager

22/06/2018 • 7 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Tous les systèmes de site System Center Configuration Manager doivent être membres d'un domaine Windows Server Active Directory pris en charge. Les ordinateurs clients Configuration Manager peuvent être membres du domaine ou membres d'un groupe de travail.

**Configuration requise et limitations :**

- L'appartenance à un domaine s'applique à des systèmes de site prenant en charge la gestion du client basée sur Internet dans un réseau de périmètre (également appelé DMZ, zone démilitarisée et sous-réseau filtré).
- Cela ne permet pas de modifier les paramètres suivants pour un ordinateur qui héberge un rôle de système de site :
  - Appartenance au domaine *(y compris suppression d'un système de site du domaine et rattachement au même domaine)*
  - Nom du domaine
  - Nom de l'ordinateur

Vous devez désinstaller le rôle de système de site (y compris le site s'il s'agit d'un serveur de site) avant d'apporter ces modifications.

**Les domaines avec les niveaux fonctionnels de domaine suivants sont pris en charge :**

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008

## Espace de noms disjoint

Configuration Manager prend en charge l'installation de systèmes de site et de clients dans un domaine qui a un espace de noms disjoint.

Dans un scénario d'espace de noms disjoint, le suffixe du DNS principal d'un ordinateur ne correspond pas au nom de domaine DNS Active Directory où se trouve cet ordinateur. L'ordinateur qui utilise le suffixe DNS principal qui ne correspond pas est dit « disjoint ». Un autre scénario d'espace de noms disjoint se produit si le nom de domaine NetBIOS d'un contrôleur de domaine ne correspond pas au nom de domaine DNS Active Directory.

Le tableau suivant identifie les scénarios pris en charge pour un espace de noms disjoint.

| SCÉNARIO | PLUS D'INFORMATIONS |
| --- | --- |
| **Scénario 1 :**<br><br>Le suffixe DNS principal du contrôleur de domaine diffère du nom de domaine DNS d'Active Directory. Les ordinateurs qui sont membres du domaine peuvent être disjoints ou non disjoints. | Dans ce scénario, le suffixe DNS principal du contrôleur de domaine diffère du nom de domaine DNS d'Active Directory. Le contrôleur de domaine est disjoint dans ce scénario. Les ordinateurs qui sont membres du domaine, comme les serveurs et les ordinateurs de site, peuvent avoir un suffixe DNS principal qui correspond soit au suffixe DNS principal du contrôleur de domaine ou au nom de domaine DNS d'Active Directory. |
| **Scénario 2 :**<br><br>Un ordinateur membre d'un domaine Active Directory est disjoint, même si le contrôleur de domaine n'est pas disjoint. | Dans ce scénario, le suffixe DNS principal d'un ordinateur membre sur lequel un système de site est installé diffère du nom de domaine DNS d'Active Directory, même si le suffixe DNS principal du contrôleur de domaine est le même que le nom de domaine DNS d'Active Directory. Dans ce scénario, un contrôleur de domaine n'est pas disjoint et un ordinateur membre est disjoint. Les ordinateurs membres qui exécutent le client Configuration Manager peuvent posséder un suffixe DNS principal qui correspond soit au suffixe DNS principal du serveur du système de site disjoint, soit au nom de domaine DNS d'Active Directory. |

Pour permettre à un ordinateur d'accéder à des contrôleurs de domaine disjoints, vous devez changer l'attribut d'Active Directory **msDS-AllowedDNSSuffixes** sur le conteneur d'objets du domaine. Vous devez ajouter les deux suffixes DNS à l'attribut.

De plus, pour vérifier que la liste de recherche des suffixes DNS contient tous les espaces de noms DNS déployés au sein de l'organisation, vous devez configurer la liste de recherche pour chaque ordinateur du domaine disjoint. Vérifiez que vous incluez ce qui suit dans la liste d'espaces de noms : le suffixe DNS principal du contrôleur de domaine, le nom de domaine DNS et tous les espaces de noms supplémentaires d'autres serveurs avec lesquels Configuration Manager peut interagir. Vous pouvez utiliser la console de Gestion de stratégie de groupe pour configurer la liste de **Recherche de suffixe de nom de domaine (DNS)** .

> **IMPORTANT**
> Lorsque vous référencez un ordinateur dans Configuration Manager, entrez-le à l'aide de son suffixe DNS principal. Ce suffixe doit correspondre au nom de domaine complet inscrit comme attribut **dnsHostName** dans le domaine Active Directory et au nom de principal du service associé au système.

## Noms de domaine en une seule partie

Configuration Manager prend en charge les systèmes de site et les clients dans un nom domaine en une seule partie quand les critères suivants sont remplis :

- Le nom de domaine en une seule partie dans les services de domaine Active Directory doit être configuré avec un espace de noms DNS disjoint associé à un domaine de niveau supérieur valide.

  **Exemple** : le nom de domaine en une seule partie Contoso est configuré pour avoir un espace de noms disjoint contoso.com dans DNS. Ainsi, quand vous spécifiez le suffixe DNS dans Configuration Manager pour un ordinateur du domaine Contoso, vous spécifiez « Contoso.com » et non pas « Contoso ».

- Les connexions DCOM (Distributed Component Object Model) entre serveurs de site dans le contexte système doivent être établies avec l'authentification Kerberos.

# Prise en charge des fonctionnalités de Windows et des réseaux dans System Center Configuration Manager

22/06/2018 • 12 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cet article identifie la prise en charge par Configuration Manager des fonctionnalités courantes de Windows et des réseaux.

## BranchCache

Vous pouvez utiliser Windows BranchCache avec Configuration Manager quand vous l'activez sur des points de distribution, puis configurer les clients pour qu'ils l'utilisent en mode de cache distribué.

Vous pouvez configurer les paramètres de BranchCache sur un type de déploiement d'applications, sur le déploiement d'un package et pour des séquences de tâches.

Quand les conditions requises de BranchCache sont remplies, cette fonctionnalité permet aux clients situés à des emplacements distants d'obtenir le contenu des clients locaux qui ont un cache actif du contenu.

Par exemple, quand le premier client BranchCache demande du contenu à partir d'un point de distribution configuré comme serveur BranchCache, le client télécharge et met en cache ce contenu. Ce contenu est ensuite rendu disponible pour les clients sur le même sous-réseau qui celui qui a demandé ce contenu.

Ces clients mettent également en cache le contenu. Les autres clients du même sous-réseau n'ont pas à télécharger le contenu à partir du point de distribution. Le contenu est distribué sur plusieurs clients, en vue de transferts futurs.

**Exigences pour prendre en charge BranchCache avec Configuration Manager**

- **Configurer des points de distribution** : ajoutez la fonctionnalité **Windows BranchCache** au serveur de système de site qui est configuré comme point de distribution.
  - Les points de distribution sur les serveurs configurés pour prendre en charge BranchCache ne nécessitent aucune configuration supplémentaire.
  - Vous ne pouvez pas ajouter Windows BranchCache à un point de distribution cloud. Les points de distribution cloud prennent en charge le téléchargement de contenu par les clients configurés pour Windows BranchCache.
- **Configurer des clients** :
  - Les clients pouvant prendre en charge BranchCache doivent être configurés pour le mode de cache distribué de BranchCache.
  - Le paramètre de système d'exploitation pour les paramètres du client BITS doit être activé pour prendre en charge BranchCache.

  Pour plus d'informations, consultez Configurer les clients pour BranchCache dans la documentation Windows.

**Versions de système d'exploitation prises en charge par Configuration Manager avec Windows BranchCache**

| SYSTÈME D'EXPLOITATION | DÉTAILS DE LA PRISE EN CHARGE |
|---|---|
| Windows 7 avec SP1 | Pris en charge par défaut |
| Windows 8 | Pris en charge par défaut |
| Windows 8.1 | Pris en charge par défaut |
| Windows 10 | Pris en charge par défaut |
| Windows Server 2008 avec SP2 | **Nécessite BITS 4.0** : vous pouvez installer BITS 4.0 sur des clients Configuration Manager à l'aide de mises à jour logicielles ou d'une distribution de logiciels. Pour plus d'informations, consultez Windows Management Framework.<br><br>Sur ce système d'exploitation, la fonctionnalité de client BranchCache n'est pas prise en charge pour la distribution de logiciels exécutée à partir du réseau ou pour les transferts de fichiers SMB. De plus, ce système d'exploitation ne peut pas utiliser la fonctionnalité BranchCache avec des points de distribution cloud. |
| Windows Server 2008 R2 | Pris en charge par défaut |
| Windows Server 2012 | Pris en charge par défaut |
| Windows Server 2012 R2 | Pris en charge par défaut |
| Windows Server 2016 | Pris en charge par défaut |

Pour plus d'informations, consultez BranchCache pour Windows dans la documentation de Windows Server.

## Ordinateurs dans des groupes de travail

Configuration Manager prend en charge les clients dans des groupes de travail.

- Configuration Manager prend en charge le déplacement d'un client depuis un groupe de travail vers un domaine, et inversement. Pour plus d'informations, consultez Guide pratique pour installer des clients Configuration Manager sur des ordinateurs de groupe de travail dans la rubrique Guide pratique pour déployer des clients sur des ordinateurs Windows.

> **NOTE**
> Les clients des groupes de travail sont pris en charge, mais tous les systèmes de site doivent être membres d'un domaine Active Directory pris en charge.

## Déduplication des données

Configuration Manager prend en charge l'utilisation de la déduplication des données avec des points de distribution sur les systèmes d'exploitation suivants :

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012

> **IMPORTANT**
> Le volume qui héberge les fichiers sources de package ne peut pas être marqué pour la déduplication des données. Cette limitation est due au fait que la déduplication des données utilise des points d'analyse. Configuration Manager ne prend pas en charge l'utilisation d'un emplacement source de contenu avec des fichiers stockés sur des points d'analyse.

Pour plus d'informations, consultez Points de distribution Configuration Manager et déduplication des données de Windows Server 2012 sur le blog de l'équipe Configuration Manager et Vue d'ensemble de la déduplication des données dans la documentation de Windows Server.

## DirectAccess

Configuration Manager prend en charge la fonctionnalité DirectAccess pour la communication entre les clients et les systèmes de serveur de site.

- Quand toutes les exigences pour DirectAccess sont satisfaites, ce dernier permet aux clients Configuration Manager sur Internet de communiquer avec le site qui leur est affecté comme s'ils étaient sur l'intranet.
- Pour les actions lancées par le serveur, comme le contrôle à distance et l'installation Push du client, l'ordinateur qui initialise l'action doit exécuter IPv6. Ce protocole doit être pris en charge sur tous les périphériques réseau qui interviennent.

Configuration Manager ne prend pas en charge les fonctionnalités suivantes sur DirectAccess :

- Le déploiement de systèmes d'exploitation
- Communication entre les sites Configuration Manager
- Communication entre les serveurs de système de site Configuration Manager au sein d'un site

## Ordinateurs à double démarrage

Configuration Manager ne peut pas gérer plusieurs systèmes d'exploitation sur un seul ordinateur. Si plusieurs systèmes d'exploitation sont présents sur un ordinateur à gérer, ajustez les méthodes de détection et d'installation du client du site afin de garantir que le client Configuration Manager est installé uniquement sur le système d'exploitation qui doit être géré.

## Protocole Internet version 6

En plus du protocole Internet version 4 (IPv4), Configuration Manager prend en charge le protocole Internet version 6 (IPv6) avec les exceptions suivantes :

| FONCTION | EXCEPTION À LA PRISE EN CHARGE IPV6 |
|---|---|
| Points de distribution cloud | IPv4 est requis pour prendre en charge Microsoft Azure et les points de distribution cloud. |
| Passerelle de gestion cloud | IPv4 est exigé pour prendre en charge Microsoft Azure et la passerelle de gestion cloud. |
| Appareils mobiles inscrits par Microsoft Intune et le connecteur de service Microsoft | IPv4 est requis pour prendre en charge les appareils mobiles inscrits par Microsoft Intune et le connecteur de service Microsoft. |

| FONCTION | EXCEPTION À LA PRISE EN CHARGE IPV6 |
| --- | --- |
| Découverte du réseau | IPv4 est requis lorsque vous configurez un serveur DHCP pour effectuer une recherche dans la découverte du réseau. |
| Déploiement de système d'exploitation | IPv4 est exigé pour prendre en charge le déploiement de système d'exploitation. |
| Communication avec le proxy de mise en éveil à distance | IPv4 est requis pour prendre en charge les paquets de proxy de mise en éveil du client. |
| Windows CE | IPv4 est requis pour prendre en charge le client Configuration Manager sur les appareils Windows CE. |

## Traduction d'adresses réseau

La traduction d'adresses réseau (NAT) n'est pas prise en charge dans Configuration Manager, sauf si le site prend en charge les clients qui se trouvent sur Internet et que le client détecte qu'ils sont connectés à Internet. Pour plus d'informations sur la gestion du client basée sur Internet, consultez Planifier la gestion des clients Internet.

## Technologie de stockage spécialisée

Configuration Manager est conçu pour fonctionner avec tout matériel approuvé dans la liste de conformité matérielle de Windows pour la version du système d'exploitation sur laquelle le composant Configuration Manager est installé.

Les rôles de serveur de site exigent NTFS afin que Configuration Manager puisse définir des autorisations sur les répertoires et les fichiers. Configuration Manager suppose qu'il a la propriété complète d'un lecteur logique. Les systèmes de site qui s'exécutent sur des ordinateurs distincts ne peuvent pas partager une partition logique sur une technologie de stockage, quelle qu'elle soit. Cependant, chaque ordinateur peut utiliser une partition logique distincte sur la même partition physique d'un dispositif de stockage partagé.

**Considérations relatives à la prise en charge**

- **Réseau de zone de stockage**: l'utilisation d'un réseau de zone de stockage (SAN) est prise en charge quand un serveur Windows pris en charge est directement associé au volume hébergé par le SAN.
- **Stockage d'instance simple (SIS)** : Configuration Manager ne prend pas en charge la configuration de dossiers de packages de points de distribution et de signatures sur un volume SIS.

  En outre, le cache d'un client Configuration Manager n'est pas pris en charge sur un volume SIS.
- **Lecteur de disque amovible** : Configuration Manager ne prend pas en charge l'installation d'un système de site ou de clients Configuration Manager sur un lecteur de disque amovible.

# Prise en charge des environnements de virtualisation pour System Center Configuration Manager

22/06/2018 • 5 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Configuration Manager prend en charge l'installation de rôles de système de site et de client sur les systèmes d'exploitation pris en charge qui s'exécutent comme machines virtuelles dans les environnements de virtualisation décrits dans cet article. Cette prise en charge se fait même quand l'hôte de la machine virtuelle (environnement de virtualisation) n'est pas pris en charge comme client ou comme serveur de site.

Par exemple, si vous utilisez Microsoft Hyper-V Server 2012 pour héberger une machine virtuelle qui exécute Windows Server 2012, vous pouvez installer les rôles de système de site ou de client sur la machine virtuelle (Windows Server 2012), mais pas sur l'hôte (Microsoft Hyper-V Server 2012).

| ENVIRONNEMENT DE VIRTUALISATION |
| --- |
| Windows Server 2008 R2 |
| Microsoft Hyper-V Server 2008 R2 |
| Windows Server 2012 |
| Microsoft Hyper-V Server 2012 |
| Windows Server 2012 R2 |
| Windows Server 2016 (voir la *remarque 1*) |
| Microsoft Hyper-V Server 2016 (voir la *remarque 1*) |

- *Remarque 1* : Configuration Manager ne prend pas en charge la virtualisation imbriquée, qui est une nouvelle fonctionnalité de Windows Server 2016.

Chaque machine virtuelle que vous utilisez doit respecter ou dépasser les mêmes configurations matérielle et logicielle requises que celles que vous utiliseriez pour un ordinateur Configuration Manager physique.

Vous pouvez vérifier que votre environnement de virtualisation est bien pris en charge pour Configuration Manager à l'aide du programme SVVP (Server Virtualization Validation Program) et de son Assistant Stratégie de prise en charge du programme de virtualisation en ligne. Pour plus d'informations sur le programme SVVP (Server Virtualization Validation Program), consultez Programme SVVP (Server Virtualization Validation Program) de Windows Server.

> **NOTE**
> Configuration Manager ne prend pas en charge les systèmes d'exploitation invités Virtual PC ou Virtual Server qui sont exécutés sur des ordinateurs Mac.

Configuration Manager ne peut pas gérer les machines virtuelles, sauf si elles sont en ligne. Il n'est pas possible de mettre à jour une image de machine virtuelle déconnectée, ni de collecter un inventaire via le client Configuration

Manager sur l'ordinateur hôte.

Aucune attention particulière n'est accordée aux machines virtuelles. Par exemple, si la mise à jour d'une image de machine virtuelle a été arrêtée puis redémarrée sans que l'état de la machine virtuelle à laquelle la mise à jour a été appliquée n'ait été enregistré, il est possible que Configuration Manager ne détermine pas s'il est nécessaire de réappliquer cette mise à jour.

## Machines virtuelles Microsoft Azure

Configuration Manager peut s'exécuter sur des machines virtuelles Azure de la même manière qu'il s'exécute localement dans votre réseau physique d'entreprise. Vous pouvez utiliser Configuration Manager sur des machines virtuelles Azure dans les scénarios suivants :

- **Scénario 1 :** vous pouvez exécuter Configuration Manager sur une machine virtuelle Azure et l'utiliser pour gérer des clients qui sont installés sur d'autres machines virtuelles Azure.
- **Scénario 2** : vous pouvez exécuter Configuration Manager sur une machine virtuelle Azure et l'utiliser pour gérer des clients qui ne s'exécutent pas sur Azure.
- **Scénario 3** : vous pouvez exécuter différents rôles de système de site Configuration Manager sur des machines virtuelles Azure tout en exécutant d'autres rôles dans votre réseau physique d'entreprise (avec une connectivité réseau appropriée pour les communications).

La même configuration requise de System Center Configuration Manager en matière de réseaux, de configurations prises en charge et de matériel, applicable à l'installation locale de Configuration Manager sur votre réseau d'entreprise physique, s'applique également aux installations effectuées sur des machines virtuelles Azure.

Pour plus d'informations, consultez Configuration Manager sur Azure : Forum Aux Questions.

> **IMPORTANT**
> Les sites et les clients Configuration Manager qui s'exécutent sur des machines virtuelles Azure sont soumis aux mêmes exigences de licence que les installations locales.

# Choisir une solution de gestion d'appareils pour System Center Configuration Manager

22/06/2018 • 7 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

System Center Configuration Manager (également appelé ConfgMgr or SCCM) offre différentes solutions pour la gestion des PC, des serveurs et des appareils. Choisissez la solution qui vous convient, en fonction des plateformes d'appareils que vous devez gérer et des fonctionnalités de gestion dont vous avez besoin.

## Vue d'ensemble des solutions de gestion d'appareils

Cet article aborde quatre solutions de gestion des appareils : l'application cliente Configuration Manager, l'infrastructure Configuration Manager locale, Microsoft Intune et Exchange. Il est suivi de deux tableaux qui permettent de comparer les solutions de gestion : un tableau basé sur les plateformes d'appareils prises en charge et un tableau basé sur les fonctionnalités de gestion.

**Gérer les appareils avec le client Configuration Manager**

Cette option, qui nécessite l'installation de l'application cliente Configuration Manager sur les appareils, offre la gamme de fonctionnalités la plus étendue pour gérer les PC, les serveurs et les autres appareils de votre environnement. Pour plus d'informations, consultez Méthodes d'installation du client dans System Center Configuration Manager.

**Gérer les appareils mobiles avec une infrastructure Configuration Manager locale**

Cette option utilise les fonctionnalités de gestion des appareils intégrées aux systèmes d'exploitation de certaines plateformes d'appareils. Bien qu'elle ne soit pas aussi complète que la gestion basée sur le client, la gestion locale des appareils mobiles fournit une approche de gestion plus légère en faisant appel aux ressources Configuration Manager locales pour atteindre et gérer les appareils. Notez que cette option n'est pour l'instant prise en charge que sur les PC Windows 10 et sur les appareils Windows 10 Mobile.

Pour plus d'informations, consultez Gérer des appareils mobiles avec une infrastructure locale dans System Center Configuration Manager.

**Gérer les appareils avec Microsoft Intune (hybride)**

Cette option utilise Microsoft Intune pour inscrire et gérer les appareils au lieu d'utiliser les ressources locales Configuration Manager. Même si Intune gère les appareils, vous accédez à vos tâches de gestion dans la console Configuration Manager. Cette option prend en charge tous les principaux systèmes d'exploitation pour appareils mobiles, notamment Windows 10 Mobile, Windows Phone, iOS et Android. Elle permet également de gérer les ordinateurs Windows 8.1 et Windows 10 de votre organisation.

Pour plus d'informations, consultez Gestion des appareils mobiles (MDM) hybride avec System Center Configuration Manager et Microsoft Intune.

**Gérer les appareils avec Microsoft Exchange**

Cette option utilise le connecteur du serveur Exchange Server pour connecter plusieurs serveurs Exchange à Configuration Manager. Cela centralise la gestion des appareils en mesure de se connecter à Exchange ActiveSync. Vous pouvez configurer les fonctionnalités de gestion des appareils mobiles d'Exchange, telles que la réinitialisation à distance et le contrôle des paramètres de plusieurs serveurs Exchange, dans la console Configuration Manager.

Pour plus d'informations, consultez Gérer les appareils mobiles avec System Center Configuration Manager et Exchange.

Vous pouvez utiliser ces solutions de gestion des appareils par elles-mêmes ou les combiner entre elles. Par exemple, vous pouvez utiliser l'approche de la gestion basée sur le client pour gérer les ordinateurs et les serveurs de votre organisation, et utiliser aussi Intune pour gérer les appareils mobiles. En combinant les méthodes de cette façon, vous pouvez couvrir tous vos besoins en matière de gestion d'appareils à partir de la console Configuration Manager.

## Comparer les solutions de gestion des appareils en fonction des plateformes d'appareils mobiles prises en charge

| PLATE-FORME | AVEC LE CLIENT CONFIGURATION MANAGER | CONFIGURATION MANAGER AVEC MICROSOFT INTUNE (HYBRIDE) | GESTION LOCALE DES APPAREILS MOBILES | CONFIGURATION MANAGER AVEC EXCHANGE |
|---|---|---|---|---|
| Android | | Oui | | Oui |
| iOS | | Oui | | Oui |
| Mac OS X | Oui | | | Oui |
| UNIX/Linux | Oui | | | Oui |
| Windows 10 | Oui | Oui | Oui | Oui |
| Windows 10 Mobile | | Oui | Oui | Oui |
| Windows (versions précédentes) | Oui | Oui | | Oui |
| Windows CE | Oui (avec le client hérité de l'appareil mobile) | | | Oui |
| Windows Embedded | Oui | | | |
| Windows Phone | | Oui | | Oui |
| Windows Server | Oui | | | Oui |

Pour obtenir la liste complète des plateformes prises en charge, consultez Systèmes d'exploitation pris en charge pour les clients et les appareils pour System Center Configuration Manager.

## Comparer les solutions de gestion des appareils mobiles en fonction des fonctionnalités de gestion

| FONCTIONNALITÉ DE GESTION | AVEC LE CLIENT CONFIGURATION MANAGER | CONFIGURATION MANAGER AVEC MICROSOFT INTUNE (HYBRIDE) | GESTION LOCALE DES APPAREILS MOBILES | CONFIGURATION MANAGER AVEC EXCHANGE |
|---|---|---|---|---|
| Sécurité de l'infrastructure à clé publique (PKI) entre l'appareil mobile et Configuration Manager (utilise l'authentification mutuelle et SSL pour le chiffrement des transferts de données) | Oui | Oui | Oui | |
| Installation du client | Oui | | | |
| Prise en charge via Internet | Oui | | | |
| découverte, | Oui | | | Oui |
| Inventaire matériel | Oui | Oui | Oui | Oui |
| Inventaire logiciel | Oui | | | Oui |
| Paramètres | Oui | Oui | Oui | Oui |
| Déploiement logiciel | Oui | Oui | Oui | |
| Surveillance avec point d'état de secours | Oui | | | |
| Connexions aux points de gestion | Oui | | Oui | |
| Connexions aux points de distribution | Oui | | Oui | |
| Blocage à partir de Configuration Manager | Oui | Oui | Oui | |
| Mise en quarantaine et blocage à partir d'Exchange Server (et Configuration Manager) | | | | Oui |
| Réinitialisation à distance | | Oui | Oui | Oui |

# Concevoir une hiérarchie de sites pour System Center Configuration Manager

22/06/2018 • 23 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Avant d'installer le premier site d'une nouvelle hiérarchie System Center Configuration Manager, il est judicieux de comprendre les topologies disponibles pour Configuration Manager, les types de sites disponibles et leurs relations mutuelles, ainsi que l'étendue de gestion fournie par chaque type de site. Après avoir étudié les options de gestion de contenu qui peuvent réduire le nombre de sites à installer, vous pouvez planifier une topologie qui répond efficacement aux besoins de votre entreprise et peut être étendue par la suite pour gérer la croissance à venir.

Lors de la planification, gardez à l'esprit les restrictions qui s'appliquent à l'ajout de sites supplémentaires à une hiérarchie ou à un site autonome :

- Vous pouvez installer un nouveau site principal sous un site d'administration centrale, jusqu'au nombre de sites principaux pris en charge pour la hiérarchie.
- Vous pouvez développer un site principal autonome pour installer un nouveau site d'administration centrale, ce qui vous permet d'installer des sites principaux supplémentaires.
- Vous pouvez installer de nouveaux sites secondaires sous un site principal, jusqu'aux limites prises en charge pour le site principal et la hiérarchie globale.
- Vous ne pouvez pas ajouter un site précédemment installé dans une hiérarchie existante en vue de fusionner deux sites autonomes. Seule l'installation de nouveaux sites dans une hiérarchie existante de sites est prise en charge.

> **NOTE**
> Quand vous planifiez une nouvelle installation de Configuration Manager, tenez compte des notes de publication qui décrivent en détail les problèmes dans les versions actives. Les notes de publication s'appliquent à toutes les branches de Configuration Manager. Toutefois, quand vous utilisez l'édition Technical Preview, vous rencontrez des problèmes spécifiques uniquement à cette édition dans la documentation pour chaque version de Technical Preview.

## Topologie de la hiérarchie

Les topologies de hiérarchie peuvent aller d'un site principal autonome unique à un groupe de sites principaux et secondaires connectés avec un site d'administration centrale dans le site de niveau supérieur de la hiérarchie. Le principal facteur qui détermine le type et le nombre de sites que vous utilisez dans une hiérarchie est généralement le nombre et le type d'appareils que vous devez prendre en charge, comme illustré ci-dessous :

**Site principal autonome :** utilisez un site principal autonome quand un seul site principal peut prendre en charge la gestion de tous vos appareils et utilisateurs (consultez Le dimensionnement et la mise à l'échelle en nombres). Cette topologie convient également quand les différents emplacements géographiques de votre société peuvent être correctement servis par un seul site principal. Pour mieux gérer le trafic réseau, vous pouvez utiliser des points de gestion préférés et une infrastructure de contenu soigneusement planifiée (consultez Concepts fondamentaux de la gestion de contenu dans System Center Configuration Manager).

Les avantages de cette topologie sont notamment les suivants :

- Surcharge administrative simplifiée.

- Attribution des sites clients simplifiée et découverte des services et des ressources disponibles.
- Élimination du retard possible engendré par la réplication de base de données entre sites.
- Possibilité de développer une hiérarchie principale autonome en une hiérarchie plus grande avec un site d'administration centrale. Cela vous permet d'installer ensuite de nouveaux sites principaux pour étendre l'échelle de votre déploiement.

**Site d'administration centrale avec un ou plusieurs sites principaux enfants :** Utilisez cette topologie quand vous avez besoin de plusieurs sites principaux pour prendre en charge la gestion de tous les appareils et utilisateurs. Elle est nécessaire quand vous avez besoin d'utiliser plusieurs sites principaux. Les avantages de cette topologie sont notamment les suivants :

- Elle prend en charge jusqu'à 25 sites principaux, ce qui vous permet d'étendre l'échelle de votre hiérarchie.
- Vous utiliserez toujours le site d'administration centrale, sauf si vous réinstallez vos sites. Ce choix est définitif. Vous ne pouvez pas détacher un site principal enfant pour en faire un site principal autonome.

  Les sections suivantes peuvent vous aider à déterminer quand utiliser un site ou une option de gestion de contenu spécifique plutôt qu'un site supplémentaire.

## Déterminer quand utiliser un site d'administration centrale

Utilisez un site d'administration centrale pour configurer des paramètres à l'échelle de la hiérarchie et surveiller tous les sites et objets dans la hiérarchie. Ce type de site ne gère pas directement les clients, mais il coordonne la réplication de données inter-site, y compris la configuration de sites et de clients dans toute la hiérarchie.

**Les informations suivantes peuvent vous aider à déterminer quand installer un site d'administration centrale :**

- Le site d'administration centrale est le site de niveau supérieur dans une hiérarchie.
- Lorsque vous configurez une hiérarchie comprenant plusieurs sites principaux, vous devez installer un site d'administration centrale. Si vous avez immédiatement besoin de deux ou plusieurs sites principaux, installez tout d'abord le site d'administration centrale. Si vous disposez déjà d'un site principal et que vous souhaitez installer un site d'administration centrale, vous devez développer le site principal autonome pour installer le site administration centrale.
- Le site d'administration centrale prend en charge uniquement des sites principaux en tant que sites enfants.
- Vous ne pouvez pas attribuer de clients au site d'administration centrale.
- Le site d'administration centrale ne prend pas en charge les rôles de système de site qui prennent directement en charge les clients, comme les points de gestion et les points de distribution.
- Vous pouvez gérer tous les clients dans la hiérarchie et exécuter des tâches de gestion de site pour tout site enfant quand vous utilisez une console Configuration Manager connectée au site d'administration centrale. Cela peut comprendre l'installation de points de gestion ou d'autres rôles de système de site sur des sites principaux ou secondaires enfants.
- Quand vous utilisez un site d'administration centrale, il s'agit du seul emplacement où vous pouvez consulter les données de tous les sites de votre hiérarchie. Ces données incluent des informations telles que des données d'inventaire et des messages d'état.
- Vous pouvez configurer des opérations de découverte dans toute la hiérarchie à partir du site d'administration centrale en attribuant l'exécution de méthodes de découverte sur des sites individuels.
- Vous pouvez gérer la sécurité dans toute la hiérarchie en attribuant différents rôles de sécurité, étendues de sécurité et regroupements à différents utilisateurs administratifs. Ces configurations s'appliquent à chaque

site dans la hiérarchie.

- Vous pouvez configurer la réplication de fichiers et la réplication de base de données pour contrôler la communication entre les sites de la hiérarchie. Cela consiste notamment à planifier la réplication de base de données pour les données de site et à gérer la bande passante pour le transfert de données basées sur des fichiers entre les sites.

## Déterminer quand utiliser un site principal

Utilisez les sites principaux pour gérer les clients. Vous pouvez installer un site principal en tant que site principal enfant sous un site d'administration centrale, ou en tant que premier site d'une nouvelle hiérarchie. Un site principal installé en tant que premier site d'une hiérarchie crée un site principal autonome. Les sites principaux enfants et les sites principaux autonomes prennent en charge les sites secondaires en tant que sites enfants du site principal.

Utilisez un site principal pour l'une des raisons suivantes :

- Pour gérer des appareils et des utilisateurs.
- Pour augmenter le nombre d'appareils que vous pouvez gérer avec une hiérarchie unique.
- Pour fournir un point de connectivité supplémentaire pour l'administration de votre déploiement.
- Pour répondre aux exigences de gestion organisationnelles. Par exemple, vous pouvez installer un site principal à un emplacement distant pour gérer le transfert de contenu de déploiement dans un réseau à faible bande passante. Cependant, avec System Center Configuration Manager, vous pouvez utiliser des options pour limiter l'utilisation de la bande passante réseau lors du transfert de données vers un point de distribution. Cette fonctionnalité de gestion du contenu peut remplacer le besoin d'installer des sites supplémentaires.

**Les informations suivantes peuvent vous aider à déterminer quand installer un site principal :**

- Un site principal peut être un site principal autonome ou un site principal enfant dans une hiérarchie plus grande. Lorsqu'un site principal est membre d'une hiérarchie avec un site d'administration centrale, les sites utilisent la réplication de base de données pour répliquer des données entre les sites. Sauf si vous avez besoin de prendre en charge un nombre de clients et de périphériques supérieur à la capacité d'un seul site principal, envisagez l'installation d'un site principal autonome. Après l'installation d'un site principal autonome, vous pouvez l'étendre pour qu'il rende compte à un nouveau site d'administration centrale, pour faire monter votre déploiement en puissance.
- Un site principal prend en charge uniquement un site d'administration centrale en tant que site parent.
- Un site principal prend en charge uniquement des sites secondaires en tant que sites enfants, et peut aussi prendre en charge plusieurs sites enfants secondaires.
- Les sites principaux sont chargés de traiter toutes les données du client à partir de leurs clients attribués.
- Les sites principaux utilisent la réplication de base de données pour communiquer directement avec leur site d'administration centrale (qui est configuré automatiquement lors de l'installation d'un nouveau site).

## Déterminer quand utiliser un site secondaire

Utilisez des sites secondaires pour gérer le transfert de contenu de déploiement et de données client dans les réseaux à faible bande passante.

Vous gérez un site secondaire à partir d'un site d'administration centrale ou du site principal parent direct du site secondaire. Vous devez associer les sites secondaires à un site principal, et vous ne pouvez pas les déplacer vers un autre site parent sans les avoir préalablement désinstallés puis réinstallés en tant que site enfant sous le

nouveau site principal.

Toutefois, vous pouvez acheminer du contenu entre deux sites secondaires homologues pour aider à gérer la réplication basée sur les fichiers du contenu de déploiement. Pour transférer des données du client vers un site principal, le site secondaire utilise la réplication basée sur les fichiers. Un site secondaire utilise également la réplication de base de données pour communiquer avec son site principal parent.

Envisagez d'installer un site secondaire si l'une des conditions suivantes est remplie :

- Vous n'avez pas besoin de point de connectivité local pour un utilisateur administratif.
- Vous devez gérer le transfert de contenu de déploiement vers des sites qui se trouvent à un niveau inférieur dans la hiérarchie.
- Vous devez gérer des informations clientes qui sont envoyées à des sites à un niveau supérieur dans la hiérarchie.

  Si vous ne souhaitez pas installer de site secondaire et que vous avez des clients à des emplacements distants, utilisez Windows BranchCache ou installez des points de distribution qui sont activés pour la planification et le contrôle de la bande passante. Vous pouvez utiliser ces options de gestion de contenu avec ou sans sites secondaires et elles peuvent vous aider à réduire le nombre de sites et de serveurs que vous devez installer. Pour plus d'informations sur les options de gestion de contenu dans Configuration Manager, consultez Déterminer quand utiliser les options de gestion de contenu.

**Les informations suivantes peuvent vous aider à déterminer quand installer un site secondaire :**

- Les sites secondaires installent automatiquement SQL Server Express lors de l'installation de site si une instance locale de SQL Server n'est pas disponible.
- Une installation de site secondaire est lancée à partir de la console Configuration Manager plutôt qu'en exécutant le programme d'installation directement sur un ordinateur.
- Les sites secondaires utilisent un sous-ensemble des informations contenues dans la base de données de site, ce qui réduit la quantité de données répliquées par la réplication de base de données entre le site principal et le site secondaire.
- Les sites secondaires prennent en charge l'acheminement de contenu basé sur des fichiers vers d'autres sites secondaires qui possèdent un site principal parent commun.
- Les installations de site secondaire déploient automatiquement un point de gestion et un point de distribution situés sur le serveur de site secondaire.

## Déterminer quand utiliser les options de gestion de contenu

Si vous possédez des clients dans des emplacements réseau distants, envisagez d'utiliser une ou plusieurs options de gestion de contenu plutôt qu'un site principal ou secondaire. Souvent, vous n'avez pas besoin d'installer un site quand vous utilisez Windows BranchCache, quand vous configurez des points de distribution pour le contrôle de la bande passante, ou quand vous copiez manuellement du contenu vers des points de distribution (préparation du contenu).

**Envisagez de déployer un point de distribution plutôt que d'installer un autre site si l'une des conditions suivantes s'applique :**

- Votre bande passante réseau est suffisante pour que les ordinateurs clients situés à l'emplacement distant communiquent avec un point de gestion afin de télécharger une stratégie client et envoient un inventaire, un état du rapport et des informations de découverte.
- Le service de transfert intelligent en arrière-plan (BITS) ne fournit pas de contrôle de bande passante suffisant pour les besoins de votre réseau.

Pour plus d'informations sur les options de gestion de contenu dans Configuration Manager, consultez Concepts fondamentaux de la gestion de contenu dans System Center Configuration Manager.

## Au-delà de la topologie de la hiérarchie

En plus de la topologie de la hiérarchie initiale, réfléchissez aux services ou aux fonctionnalités qui seront disponibles à partir de différents sites dans la hiérarchie (rôles de système de site), et à la façon dont les fonctionnalités et configurations à l'échelle de la hiérarchie seront gérées dans votre infrastructure. Les considérations courantes suivantes sont traitées dans des rubriques distinctes. Ces éléments sont importants, car ils peuvent influencer la conception de votre hiérarchie ou être influencés par celle-ci :

- Quand vous vous préparez à gérer des ordinateurs et des appareils avec System Center Configuration Manager, déterminez si les appareils que vous gérez sont locaux, situés dans le cloud ou comptent des appareils appartenant à l'utilisateur (BYOD). Étudiez également la façon dont vous allez gérer les appareils qui sont pris en charge par plusieurs options de gestion, tels que des ordinateurs Windows 10 pouvant être gérés directement par Configuration Manager ou via l'intégration à Microsoft Intune.
- Découvrez comment votre infrastructure réseau disponible peut affecter le flux de données entre des sites distants (consultez Préparer votre environnement réseau pour System Center Configuration Manager). Tenez aussi compte de l'emplacement géographique des utilisateurs et appareils que vous gérez, et déterminez s'ils accèdent à votre infrastructure par l'intermédiaire de votre domaine d'entreprise ou d'Internet.
- Planifiez une infrastructure de contenu pour distribuer efficacement les informations que vous déployez (fichiers et applications) sur les appareils que vous gérez (consultez Gérer le contenu et l'infrastructure de contenu pour System Center Configuration Manager).
- Identifiez les fonctions et fonctionnalités de System Center Configuration Manager que vous envisagez d'utiliser, les rôles de système de site ou l'infrastructure Windows nécessaires ainsi que les sites au niveau desquels vous pouvez les déployer dans une hiérarchie comportant plusieurs sites pour une utilisation optimale du réseau et des ressources serveur.
- Prenez en compte la sécurité des données et des appareils, notamment l'utilisation d'une infrastructure à clé publique. Consultez Configuration requise des certificats PKI pour System Center Configuration Manager.

**Passez en revue les ressources suivantes pour les configurations spécifiques aux sites :**

- Planifier le fournisseur SMS pour System Center Configuration Manager
- Planifier la base de données du site pour System Center Configuration Manager
- Planifier des serveurs de système de site et des rôles système de site pour System Center Configuration Manager
- Planifier la sécurité dans System Center Configuration Manager
- Managing network bandwidth lors du déploiement de contenu dans un site

**Tenez compte des configurations qui couvrent plusieurs sites et hiérarchies :**

- Options de haute disponibilité pour System Center Configuration Manager pour les sites et hiérarchies
- Étendre le schéma Active Directory pour System Center Configuration Manager et configurer des sites pour la publication de données de site pour System Center Configuration Manager
- Transfert de données entre sites dans System Center Configuration Manager
- Principes de base de l'administration basée sur des rôles pour System Center Configuration Manager

# Planifier le fournisseur SMS pour System Center Configuration Manager

22/06/2018 • 21 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Pour gérer System Center Configuration Manager, vous devez utiliser une console Configuration Manager qui se connecte à une instance du **fournisseur SMS**. Par défaut, un fournisseur SMS est installé sur le serveur de site durant l'installation d'un site d'administration centrale ou d'un site principal.

## À propos du fournisseur SMS

Le fournisseur SMS est un fournisseur WMI (Windows Management Instrumentation) qui affecte un accès en **lecture** et en **écriture** à la base de données Configuration Manager d'un site :

- Chaque site d'administration centrale et site principal doit posséder au moins un fournisseur SMS. Vous pouvez installer d'autres fournisseurs en fonction des besoins.
- Le groupe de sécurité **Administrateurs SMS** fournit l'accès au fournisseur SMS. Configuration Manager crée automatiquement ce groupe sur le serveur de site et sur chaque ordinateur sur lequel vous installez une instance du fournisseur SMS.
- Les sites secondaires ne prennent pas en charge le fournisseur SMS.

Les utilisateurs administratifs de Configuration Manager utilisent un fournisseur SMS pour accéder aux informations stockées dans la base de données. Pour ce faire, les administrateurs peuvent utiliser la console Configuration Manager, l'Explorateur de ressources, des outils et des scripts personnalisés. Le fournisseur SMS n'interagit pas avec les clients Configuration Manager. Quand une console Configuration Manager se connecte à un site, la console Configuration Manager interroge le service WMI sur le serveur de site pour localiser une instance du fournisseur SMS à utiliser.

Le fournisseur SMS contribue à l'application de la sécurité de Configuration Manager. Il retourne uniquement les informations que l'utilisateur administratif qui exécute la console Configuration Manager est autorisé à afficher.

> **IMPORTANT**
> Quand chaque ordinateur qui héberge un fournisseur SMS pour un site est hors connexion, les consoles Configuration Manager ne peuvent pas se connecter à la base de données de ce site.

Pour plus d'informations sur la façon de gérer le fournisseur SMS, consultez Gérer le fournisseur SMS dans Modifier votre infrastructure System Center Configuration Manager.

## Prérequis à l'installation du fournisseur SMS

Pour prendre en charge le fournisseur SMS :

- L'ordinateur doit être dans un domaine qui entretient une relation d'approbation bidirectionnelle avec le serveur de site et les systèmes de site de base de données du site.
- L'ordinateur ne peut pas disposer d'un rôle de système de site à partir d'un autre site.
- L'ordinateur ne peut pas disposer d'un fournisseur SMS à partir de n'importe quel site.

- L'ordinateur doit exécuter un système d'exploitation pris en charge pour un serveur de site.
- L'ordinateur doit disposer d'au moins 650 Mo d'espace disque libre pour prendre en charge les composants du kit de déploiement automatisé Windows (Windows ADK) qui sont installés avec le fournisseur SMS. Pour plus d'informations sur le kit Windows ADK et sur le fournisseur SMS, consultez Configuration de déploiement de système d'exploitation requise pour le fournisseur SMS dans cette rubrique.

## Emplacements des fournisseurs SMS

Quand vous installez un site, le premier fournisseur SMS du site est installé automatiquement. Vous pouvez spécifier l'un des emplacements suivants pris en charge pour le fournisseur SMS :

- L'ordinateur de serveur de site
- L'ordinateur de base de données du site
- Un ordinateur de classe serveur qui ne possède pas de fournisseur SMS, ou un rôle de système de site à partir d'un autre site

Pour afficher les emplacements de chaque fournisseur SMS installé sur un site, sélectionnez l'onglet **Général** de la boîte de dialogue **Propriétés** du site.

Chaque fournisseur SMS prend en charge des connexions simultanées à partir de plusieurs demandes. Les seules limites sur ces connexions sont le nombre de connexions au serveur qui sont disponibles sur l'ordinateur du fournisseur SMS et les ressources disponibles sur l'ordinateur du fournisseur SMS pour répondre aux demandes de connexion.

Après avoir installé un site, vous pouvez procéder à nouveau à l'installation sur le serveur de site pour modifier l'emplacement d'un fournisseur SMS existant ou pour installer d'autres fournisseurs SMS sur ce site. Vous pouvez installer un seul fournisseur SMS sur un ordinateur et un ordinateur ne peut pas installer un fournisseur SMS à partir de plusieurs sites.

Utilisez la section suivante pour identifier les avantages et inconvénients liés à l'installation d'un fournisseur SMS sur chaque emplacement pris en charge :

**Serveur de site Configuration Manager**

- **Avantages :**
  - Le fournisseur SMS n'utilise pas les ressources système de l'ordinateur de base de données du site.
  - Cet emplacement peut fournir de meilleures performances qu'un fournisseur SMS situé sur un ordinateur autre que le serveur de site ou l'ordinateur de base de données du site.
- **Inconvénients :**
  - Le fournisseur SMS utilise des ressources réseau et système qui pourraient être dédiées aux opérations du serveur de site.

**SQL Server qui héberge la base de données du site**

- **Avantages :**
  - Le fournisseur SMS n'utilise pas les ressources du système de site sur le serveur de site.
  - Parmi les trois emplacements, cet emplacement peut fournir les meilleures performances, si des ressources serveur suffisantes sont disponibles.
- **Inconvénients :**

- Le fournisseur SMS utilise des ressources réseau et système qui pourraient être dédiées aux opérations de la base de données de site.
- Quand la base de données du site est hébergée sur une instance en cluster de SQL Server, vous ne pouvez pas utiliser cet emplacement.

**Ordinateur autre que le serveur de site ou l'ordinateur de base de données du site**

- **Avantages :**
  - Le fournisseur SMS n'utilise pas le serveur de site ou les ressources informatiques de base de données du site.
  - Ce type d'emplacement vous permet de déployer d'autres fournisseurs SMS afin de fournir une haute disponibilité pour les connexions.
- **Inconvénients :**
  - Les performances du fournisseur SMS peuvent être réduites en raison de l'augmentation de l'activité réseau nécessaire à sa coordination avec le serveur de site et l'ordinateur de base de données du site.
  - L'ordinateur de la base de données du site et tous les ordinateurs sur lesquels la console Configuration Manager est installée doivent toujours pouvoir accéder à ce serveur.
  - Cet emplacement peut utiliser les ressources système qui, dans le cas contraire, seraient dédiées à d'autres services.

# À propos des langues du fournisseur SMS

Le fournisseur SMS fonctionne indépendamment de la langue d'affichage de l'ordinateur sur lequel il est installé.

Quand un utilisateur administratif ou un processus Configuration Manager sollicite des données à l'aide du fournisseur SMS, ce dernier tente de retourner les données dans un format correspondant à la langue du système d'exploitation de l'ordinateur émetteur de la requête.

La méthode utilisée pour tenter de déterminer la langue est indirecte. Le fournisseur SMS ne traduit pas les informations d'une langue à l'autre. À la place, quand les données sont retournées pour être affichées dans la console Configuration Manager, leur langue d'affichage varie en fonction de la source de l'objet et du type de stockage.

Lorsque les données d'un objet sont stockées dans la base de données, les langues qui seront disponibles dépendent des éléments suivants :

- Les objets créés par Configuration Manager sont stockés dans la base de données via la prise en charge de plusieurs langues. L'objet est stocké à l'aide des langues qui sont configurées sur le site sur lequel l'objet est créé lorsque vous procédez à l'installation. Ces objets sont affichés dans la console Configuration Manager dans la langue d'affichage de l'ordinateur qui émet la requête, quand cette langue est disponible pour l'objet. Si l'objet ne peut pas être affiché dans la langue d'affichage de l'ordinateur qui émet la demande, il est affiché dans la langue par défaut, à savoir l'anglais.
- Les objets créés par un utilisateur administratif sont stockés dans la base de données à l'aide de la langue utilisée pour créer l'objet. Ces objets s'affichent dans la console Configuration Manager dans la même langue. Ils ne peuvent pas être traduits par le fournisseur SMS et ne possèdent pas plusieurs options de langue.

# Utiliser plusieurs fournisseurs SMS

Après l'installation d'un site, vous pouvez installer des fournisseurs SMS supplémentaires pour ce site. Pour installer des fournisseurs SMS supplémentaires, exécutez le programme d'installation de Configuration Manager sur le serveur de site. Envisagez l'installation de fournisseurs SMS supplémentaires lorsque l'une des affirmations suivantes est vraie :

- Un grand nombre d'utilisateurs administratifs exécutent une console Configuration Manager et se connectent à un site en même temps.
- Vous comptez utiliser le SDK Configuration Manager, ou d'autres produits, qui peuvent générer des appels fréquents au fournisseur SMS.
- Vous voulez garantir une haute disponibilité pour le fournisseur SMS.

Quand plusieurs fournisseurs SMS sont installés sur un site et qu'une demande de connexion est effectuée, le site attribue de façon aléatoire à chaque nouvelle demande de connexion l'utilisation d'un fournisseur SMS installé. Vous ne pouvez pas spécifier l'emplacement du fournisseur SMS à utiliser avec une session de connexion spécifique.

> **NOTE**
> Tenez compte des avantages et des inconvénients de chaque emplacement du fournisseur SMS. Trouvez un équilibre entre ces considérations et le fait que vous ne pouvez pas contrôler le fournisseur SMS qui est utilisé pour chaque nouvelle connexion.

Par exemple, quand vous connectez une console Configuration Manager à un site pour la première fois, la connexion interroge le service WMI sur le serveur de site pour identifier l'instance du fournisseur SMS à utiliser. Cette instance spécifique du fournisseur SMS reste utilisée par la console Configuration Manager jusqu'à la fin de sa session. Si la session prend fin car l'ordinateur du fournisseur SMS n'est plus disponible sur le réseau, quand vous reconnectez la console Configuration Manager, le site répète simplement la tâche d'identification d'une instance du fournisseur SMS à laquelle se connecter. Il est possible que le même ordinateur du fournisseur SMS non disponible soit attribué. Si cela se produit, vous pouvez tenter de reconnecter la console Configuration Manager jusqu'à ce qu'un ordinateur du fournisseur SMS disponible soit affecté.

## À propos du groupe Administrateurs SMS

Le groupe Administrateurs SMS permet de fournir aux utilisateurs administratifs l'accès au fournisseur SMS. Le groupe est créé automatiquement sur le serveur de site au moment de l'installation du site, et sur chaque ordinateur qui installe un fournisseur SMS. Informations supplémentaires concernant le groupe Administrateurs SMS :

- Lorsque l'ordinateur est un serveur membre, le groupe Administrateurs SMS est créé en tant que groupe local.
- Lorsque l'ordinateur est un contrôleur de domaine, le groupe Administrateurs SMS est créé en tant que groupe de domaine local.
- Lorsque le fournisseur SMS est désinstallé d'un ordinateur, le groupe Administrateurs SMS n'est pas supprimé de l'ordinateur.

Avant qu'un utilisateur puisse établir une connexion correcte à un fournisseur SMS, son compte d'utilisateur doit être un membre du groupe Administrateurs SMS. Chaque utilisateur administratif que vous configurez dans la console Configuration Manager est automatiquement ajouté au groupe Administrateurs SMS sur chaque serveur de site et chaque ordinateur du fournisseur SMS de la hiérarchie. Quand vous supprimez un utilisateur administratif de la console Configuration Manager, cet utilisateur est supprimé du groupe Administrateurs SMS sur chaque serveur de site et chaque ordinateur du fournisseur SMS de la hiérarchie.

Une fois la connexion au fournisseur SMS réussie, l'administration basée sur des rôles permet de déterminer les ressources Configuration Manager auxquelles cet utilisateur peut accéder ou qu'il peut gérer.

Vous pouvez afficher et configurer les autorisations et les droits du groupe Administrateurs SMS à l'aide du composant logiciel enfichable MMC Contrôle WMI. Par défaut, **Tout le monde** dispose des autorisations **Méthodes d'exécution**, **Écriture fournisseur**et **Activer le compte** . Une fois connecté au fournisseur SMS, l'utilisateur se voit accorder l'accès aux données dans la base de données du site en fonction des droits de sécurité d'administration basée sur des rôles définis dans la console Configuration Manager. Les autorisations **Activer le compte** et **Appel à distance autorisé** sont accordées explicitement au groupe Administrateurs SMS dans l'espace de noms **Root\SMS**.

> **NOTE**
> Chaque utilisateur administratif qui utilise une console Configuration Manager distante doit avoir des autorisations DCOM d'activation à distance à la fois sur le serveur de site et sur l'ordinateur du fournisseur SMS. Même si ces droits peuvent être accordés à des utilisateurs ou des groupes, il est conseillé de les accorder au groupe Administrateurs SMS pour simplifier l'administration. Pour plus d'informations, consultez la section Configurer les autorisations DCOM pour les consoles Configuration Manager distantes dans la rubrique Modifier votre infrastructure System Center Configuration Manager.

## À propos de l'espace de noms du fournisseur SMS

La structure du fournisseur SMS est définie par le schéma WMI. Les espaces de noms du schéma décrivent l'emplacement des données Configuration Manager dans le schéma du fournisseur SMS. Le tableau ci-dessous contient certains des espaces de noms communs utilisés par le fournisseur SMS.

| ESPACE DE NOMS | DESCRIPTION |
|---|---|
| Root\SMS\site_<*code de site*> | Fournisseur SMS, qui est utilisé de façon intensive par la console Configuration Manager, l'Explorateur de ressources, les outils Configuration Manager et les scripts. |
| Root\SMS\SMS_ProviderLocation | Emplacement des ordinateurs du fournisseur SMS pour un site. |
| Root\CIMv2 | Emplacement inventorié pour des informations d'espaces de noms WMI au cours de l'inventaire matériel et logiciel. |
| Root\CCM | Stratégies de configuration et données du client Configuration Manager. |
| root\CIMv2\SMS | Emplacement des classes de rapports d'inventaire collectées par l'Agent du client d'inventaire. Ces paramètres compilés par des clients au cours de l'évaluation des stratégies de l'ordinateur sont basés sur la configuration des paramètres du client de l'ordinateur. |

## Exigences liées au déploiement de système d'exploitation pour le fournisseur SMS

L'ordinateur sur lequel vous installez une instance du fournisseur SMS doit disposer de la version du Windows ADK exigée par la version de Configuration Manager que vous utilisez.

- Par exemple, la version 1511 de Configuration Manager exige la version Windows 10 RTM (10.0.10240) du Windows ADK.

- Pour plus d'informations sur cette configuration requise, consultez Configuration requise de l'infrastructure pour le déploiement de système d'exploitation.

Quand vous gérez des déploiements de système d'exploitation, le Windows ADK permet au fournisseur SMS d'effectuer diverses tâches, notamment :

- Afficher les informations du fichier WIM.
- Ajouter des fichiers de pilote aux images de démarrage existantes.
- Créer des fichiers .ISO de démarrage.

L'installation du kit Windows ADK peut nécessiter jusqu'à 650 Mo d'espace disque libre sur chaque ordinateur où le fournisseur SMS est installé. Cet espace disque élevé est nécessaire pour permettre à Configuration Manager d'installer les images de démarrage Windows PE.

# Planifier la base de données du site pour System Center Configuration Manager

22/06/2018 • 5 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Le serveur de base de données de site est un ordinateur qui exécute une version prise en charge de Microsoft SQL Server. SQL Server est utilisé pour stocker des informations pour les sites Configuration Manager. Chaque site d'une hiérarchie Configuration Manager contient une base de données du site et un serveur qui est attribué au rôle serveur de la base de données du site.

- Pour les sites d'administration centrale et les sites principaux, vous pouvez installer SQL Server sur le serveur de site, ou vous pouvez installer SQL Server sur un ordinateur autre que le serveur de site.
- Pour les sites secondaires, vous pouvez utiliser SQL Server Express au lieu d'une installation complète de SQL Server. Le serveur de base de données doit cependant être exécuté sur le serveur de site secondaire.
- Pour l'utilisation du groupe de disponibilité SQL, le modèle de récupération de la base de données doit être défini sur FULL
- Pour l'utilisation du groupe de disponibilité non SQL, le modèle de récupération de la base de données doit être défini sur SIMPLE

Vous trouverez plus d'informations sur les modes de récupération SQL dans Modèles de récupération (SQL Server).

Les configurations SQL Server suivantes peuvent servir à héberger la base de données du site :

- Instance par défaut de SQL Server
- Une instance nommée sur un seul ordinateur exécutant SQL Server
- Une instance nommée sur une instance en cluster de SQL Server
- Un groupe de disponibilité AlwaysOn SQL Server (à compter de la version 1602 de System Center Configuration Manager)

Pour héberger la base de données du site, SQL Server doit remplir les conditions requises décrites dans Prise en charge des versions de SQL Server pour System Center Configuration Manager.

## Considérations relatives à l'emplacement du serveur de base de données distant

Si vous utilisez un ordinateur serveur de base de données distant, vérifiez que la connexion réseau est à large bande passante et haute disponibilité. Le serveur de site et certains rôles de système de site doivent communiquer en permanence avec le serveur distant qui héberge la base de données de site.

- La quantité de bande passante requise pour les communications avec le serveur de base de données dépend de l'association de nombreuses configurations de site et de client. Par conséquent, la bande passante réelle requise ne peut pas être déterminée correctement.
- Chaque ordinateur qui exécute le fournisseur SMS et qui se connecte à la base de données du site augmente les besoins en bande passante réseau.

- L’ordinateur qui exécute SQL Server doit se trouver dans un domaine qui entretient une relation d’approbation bidirectionnelle avec le serveur de site et tous les ordinateurs exécutant le fournisseur SMS.
- Vous ne pouvez pas utiliser un SQL Server en cluster pour le serveur de base de données de site lorsque la base de données de site se trouve au même emplacement que le serveur de site.

En règle générale, un serveur de système de site prend en charge les rôles de système de site d’un seul site Configuration Manager. Vous pouvez toutefois utiliser différentes instances de SQL Server, sur des serveurs cluster ou non cluster exécutant SQL Server, pour héberger une base de données de différents sites Configuration Manager. Pour prendre en charge des bases de données à partir de différents sites, vous devez configurer chaque instance de SQL Server afin qu'elle utilise des ports uniques pour la communication.

# Planifier des serveurs de système de site et des rôles système de site pour System Center Configuration Manager

22/06/2018 • 29 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Chaque site System Center Configuration Manager que vous installez comprend un serveur de site qui est un **serveur de système de site**. Le site peut également inclure des serveurs de système de site supplémentaires sur des ordinateurs distants par rapport au serveur de site. Les serveurs de système de site (serveur de site ou serveur de système de site distant) prennent en charge les **rôles de système de site**.

## Serveurs de système de site

Lorsque vous installez un rôle de système de site sur un ordinateur, celui-ci devient un serveur de système de site. Sur chaque site, vous pouvez installer un ou plusieurs serveurs de système de site supplémentaires. Vous pouvez également décider de ne pas installer de serveurs de système de site supplémentaires et exécuter tous les rôles de système de site directement sur l'ordinateur serveur de site. Chaque serveur de système de site prend en charge un ou plusieurs rôles de système de site. Les serveurs supplémentaires permettent d'augmenter les fonctionnalités et capacités d'un site en partageant la charge de traitement du processeur que les rôles de système de site font peser sur un serveur.

Lorsque vous envisagez l'ajout d'un serveur de système de site, assurez-vous que le serveur répond aux conditions requises pour l'utilisation prévue. Il est également judicieux de l'ajouter à un emplacement réseau bénéficiant d'une bande passante suffisante pour communiquer avec les points de terminaison attendus, y compris le serveur de site, les ressources de domaine, un emplacement cloud, les serveurs de système de site et les clients).

Si vous configurez le serveur de système de site avec un proxy pour une utilisation par des rôles de système de site, consultez Rôles système de site pouvant utiliser un serveur proxy.

## Rôles système de site

Des rôles système de site sont installés sur un ordinateur pour fournir au site des fonctionnalités supplémentaires. En voici quelques exemples :

- Points de gestion supplémentaires permettant au site de prendre en charge davantage d'appareils, jusqu'à sa capacité maximale.
- Points de distribution supplémentaires pour développer votre infrastructure de contenu, ce qui améliore les performances des distributions de contenu aux appareils et utilisateurs.
- Un ou plusieurs rôles de système de site propres aux fonctions. Par exemple, un point de mise à jour logicielle vous permet de gérer les mises à jour logicielles des appareils pris en charge. Un point de Reporting Services vous permet de générer des rapports pour analyser et comprendre votre déploiement, ou partager des informations sur ce dernier.

Différents sites Configuration Manager peuvent prendre en charge différents ensembles de rôles de système de site. L'ensemble pris en charge de rôles de système de site dépend du type de site (site d'administration centrale, site principal ou site secondaire). La topologie de votre hiérarchie peut limiter le placement de certains rôles sur

certains types de sites. Par exemple, le point de connexion de service est pris en charge uniquement sur le site de niveau supérieur de la hiérarchie, qui peut être un site d'administration centrale ou un site principal autonome. Ce rôle n'est pas pris en charge sur un site principal enfant ou sur des sites secondaires.

Après l'installation d'un site, vous pouvez déplacer certains rôles de système de site depuis leur emplacement par défaut sur le serveur de site vers un autre serveur. Cela vaut notamment pour le point de gestion ou le point de distribution, qui sont installés par défaut sur un serveur de site principal ou secondaire. Vous pouvez également installer des instances supplémentaires de certains rôles de système de site pour étendre les capacités de votre site (fournir davantage de services aux clients) et répondre aux besoins de votre entreprise. Certains rôles sont obligatoires, tandis que d'autres sont facultatifs.

- **Serveur de site Configuration Manager**. Ce rôle identifie le serveur sur lequel le programme d'installation de Configuration Manager est exécuté pour installer un site, ou le serveur sur lequel vous installez un site secondaire. Ce rôle ne peut pas être déplacé ni désinstallé tant que le site n'a pas été désinstallé.

- **Système de site Configuration Manager**. Ce rôle est attribué à tout ordinateur sur lequel vous installez un site ou un rôle de système de site. Ce rôle ne peut pas être déplacé ni désinstallé tant que le dernier rôle de système de site n'a pas été supprimé de l'ordinateur.

- **Rôle de système de site de composant Configuration Manager**. Ce rôle identifie un système de site exécutant une instance du service SMS Executive. Il est obligatoire pour prendre en charge d'autres rôles, comme des points de gestion. Ce rôle ne peut pas être déplacé ni désinstallé tant que le dernier rôle de système de site applicable n'a pas été supprimé de l'ordinateur.

- **Serveur de base de données de site Configuration Manager**. Ce rôle est attribué aux serveurs de système de site qui contiennent une instance de la base de données d'un site. Il ne peut être déplacé vers un nouveau serveur qu'en modifiant le site pour qu'il héberge la base de données du site sur un autre serveur SQL Server.

- **Fournisseur SMS**. Ce rôle est attribué à chaque ordinateur qui héberge une instance du fournisseur SMS (l'interface entre une console Configuration Manager et la base de données du site). Par défaut, ce rôle est installé automatiquement sur le serveur d'un site d'administration centrale et les sites principaux. Vous pouvez installer des instances supplémentaires sur chaque site pour fournir un accès à d'autres utilisateurs administratifs.

  Pour installer des fournisseurs SMS supplémentaires, exécutez le programme d'installation de Configuration Manager afin de gérer le fournisseur SMS. Ensuite, installez d'autres fournisseurs sur d'autres ordinateurs. Vous ne pouvez installer qu'une seule instance du fournisseur SMS sur un ordinateur, et celui-ci doit être dans le même domaine que le serveur de site.

- **Point de service web du catalogue des applications**. Un rôle de système de site qui fournit des informations logicielles au site Web du catalogue d'applications à partir de la bibliothèque de logiciels. Bien que ce rôle soit pris en charge uniquement sur des sites principaux, vous pouvez en installer plusieurs instances sur un site ou sur plusieurs sites dans la même hiérarchie.

- **Point du site web du catalogue des applications**. Un rôle de système de site qui fournit aux utilisateurs une liste des logiciels disponibles à partir du catalogue d'applications. Bien que ce rôle soit pris en charge uniquement sur des sites principaux, vous pouvez en installer plusieurs instances sur un site ou sur plusieurs sites dans la même hiérarchie.

  Si le catalogue d'applications prend en charge des ordinateurs clients sur Internet, il est plus sûr d'installer le point de site Web du catalogue des applications dans un réseau de périmètre et le point de service web du catalogue des applications sur l'intranet.

- **Point de synchronisation Asset Intelligence**. Ce rôle de système de site se connecte à Microsoft afin de télécharger des informations pour le catalogue Asset Intelligence. Il charge également les titres sans

catégorie, en vue de leur éventuelle future intégration dans le catalogue. Une hiérarchie ne prend en charge qu'une seule instance de ce rôle, qui doit se trouver sur le site de niveau supérieur de votre hiérarchie (site d'administration centrale ou site principal autonome). Si vous étendez un site principal autonome à une hiérarchie plus importante, vous devez désinstaller ce rôle du site principal, puis l'installer sur le site d'administration centrale. Pour plus d'informations, consultez Asset Intelligence dans System Center Configuration Manager.

- **Point d'enregistrement de certificat**. Ce rôle de système de site communique avec un serveur qui exécute le Service d'inscription de périphériques réseau. Il gère les demandes de certificat de périphérique qui utilisent le protocole SCEP (Simple Certificate Enrollment Protocol). Ce rôle est pris en charge uniquement sur des sites principaux et le site d'administration centrale.

  Bien qu'un point d'enregistrement de certificat puisse fournir une fonctionnalité à une hiérarchie entière, vous pouvez installer plusieurs instances de ce rôle sur un site et sur plusieurs sites dans la même hiérarchie. Cela facilite l'équilibrage de charge. Quand plusieurs instances existent dans une hiérarchie, des clients sont affectés de façon aléatoire à l'un des points d'enregistrement de certificat.

  Chaque point d'enregistrement de certificat requiert l'accès à une instance distincte d'un service d'inscription d'appareils réseau. Vous ne pouvez pas configurer plusieurs points d'enregistrement de certificat pour utiliser le même service d'inscription d'appareils réseau. En outre, le point d'enregistrement de certificat ne doit pas être installé sur le serveur exécutant le service d'inscription de périphérique réseau.

- **Point de connecteur de passerelle de gestion cloud**. Ce rôle de système de site communique avec la passerelle de gestion cloud.

- **Point de distribution**. Un rôle de système de site qui contient des fichiers sources que les clients peuvent télécharger, notamment le contenu de l'application, les packages logiciels, les mises à jour logicielles, les images du système d'exploitation et les images de démarrage. Par défaut, ce rôle est installé sur l'ordinateur du serveur de site de nouveaux sites principaux et secondaires lors de l'installation du site. Ce rôle n'est pas pris en charge sur un site d'administration centrale. Vous pouvez installer plusieurs instances de ce rôle sur un site pris en charge et sur plusieurs sites dans la même hiérarchie. Pour plus d'informations, consultez Concepts fondamentaux de la gestion de contenu dans System Center Configuration Manager et Gérer le contenu et l'infrastructure de contenu pour System Center Configuration Manager.

- **Point d'état de secours**. Ce rôle de système de site vous aide à surveiller l'installation des clients et à identifier ceux qui ne sont pas pris en charge, car ils ne peuvent pas communiquer avec leur point de gestion. Bien que ce rôle soit pris en charge uniquement sur des sites principaux, vous pouvez en installer plusieurs instances sur un site et sur plusieurs sites dans la même hiérarchie.

- **Point Endpoint Protection.** Configuration Manager utilise ce rôle de système de site pour accepter le contrat de licence Endpoint Protection et configurer l'appartenance par défaut à Microsoft Active Protection Service. Une hiérarchie ne prend en charge qu'une seule instance de ce rôle, qui doit se trouver sur le site de niveau supérieur de votre hiérarchie (site d'administration centrale ou site principal autonome). Si vous étendez un site principal autonome à une hiérarchie plus importante, vous devez désinstaller ce rôle du site principal, puis l'installer sur le site d'administration centrale. Pour plus d'informations, consultez Endpoint Protection.

- **Point d'inscription.** Ce rôle de système de site utilise des certificats PKI pour permettre à Configuration Manager d'inscrire des appareils mobiles et des ordinateurs Mac. Bien que ce rôle soit pris en charge uniquement sur des sites principaux, vous pouvez en installer plusieurs instances sur un site ou sur plusieurs sites dans la même hiérarchie.

  Si un utilisateur inscrit des appareils mobiles à l'aide de Configuration Manager et que son compte Active Directory se trouve dans une forêt non approuvée par la forêt du serveur de site, vous devez installer un point d'inscription dans la forêt de l'utilisateur. L'utilisateur peut alors être authentifié.

- **Point proxy d'inscription**. Rôle de système de site qui gère les demandes d'inscription Configuration Manager issues des appareils mobiles et des ordinateurs Mac. Bien que ce rôle soit pris en charge uniquement sur des sites principaux, vous pouvez en installer plusieurs instances sur un site ou sur plusieurs sites dans la même hiérarchie.

  Lors de la prise en charge d'appareils mobiles sur Internet, installez le point proxy d'inscription dans un réseau de périmètre et le point d'inscription sur l'intranet.

- **Connecteur Exchange Server**. Pour plus d'informations sur ce rôle, consultez Gérer des appareils mobiles à l'aide de System Center Configuration Manager et d'Exchange.

- **Point de gestion**. Ce rôle de système de site fournit aux clients des informations sur l'emplacement du service et de la stratégie, et reçoit les données de configuration de la part des clients.

  Par défaut, ce rôle est installé sur l'ordinateur du serveur de site de nouveaux sites principaux et secondaires lors de l'installation du site. Les sites principaux prennent en charge plusieurs instances de ce rôle. Les sites secondaires prennent en charge un seul point de gestion comme point de contact local permettant aux clients d'obtenir des stratégies d'ordinateur et d'utilisateur. (Sur un site secondaire, un point de gestion est appelé point de gestion proxy.)

  Vous pouvez configurer des points de gestion pour prendre en charge le protocole HTTP ou HTTPS, ainsi que les appareils mobiles que vous gérez via la fonctionnalité de gestion des appareils mobiles locale de System Center Configuration Manager. Vous pouvez utiliser des réplicas de base de données pour les points de gestion de System Center Configuration Manager pour réduire la charge processeur placée sur le serveur de base de données du site par les points de gestion à mesure qu'ils traitent les demandes des clients.

- **Point de Reporting Services**. Rôle de système de site qui est intégré à SQL Server Reporting Services pour créer et gérer des rapports pour Configuration Manager. Ce rôle est pris en charge sur les sites principaux et le site d'administration centrale, et vous pouvez en installer plusieurs instances sur un site pris en charge. Pour plus d'informations, consultez Planification de la création de rapports dans System Center Configuration Manager.

- **Point de connexion de service**. Ce rôle de système de site permet de gérer les appareils mobiles avec Microsoft Intune et d'assurer la gestion MDM locale. Il charge aussi les données d'utilisation à partir de votre site et est nécessaire pour mettre les mises à jour de Configuration Manager disponibles dans la console Configuration Manager. Une hiérarchie ne prend en charge qu'une seule instance de ce rôle, qui doit se trouver sur le site de niveau supérieur de votre hiérarchie (site d'administration centrale ou site principal autonome). Si vous étendez un site principal autonome à une hiérarchie plus importante, vous devez désinstaller ce rôle du site principal, puis l'installer sur le site d'administration centrale. Pour plus d'informations, voir À propos du point de connexion de service dans System Center Configuration Manager.

- **Point de mise à jour logicielle**. Un rôle de système de site qui est intégré à Windows Server Update Services (WSUS) pour fournir des mises à jour logicielles aux clients Configuration Manager. Ce rôle est pris en charge sur tous les sites :

  - Installez ce système de site sur le site d'administration centrale pour une synchronisation avec WSUS.
  - Configurez chaque instance de ce rôle sur les sites principaux enfants à synchroniser avec le site d'administration centrale.
  - Envisagez d'installer un point de mise à jour logicielle sur des sites secondaires quand le transfert de données sur le réseau est lent.

  Pour plus d'informations, consultez Planifier les mises à jour logicielles dans System Center Configuration

Manager.

- **Point de migration d'état**. Un rôle de système de site qui stocke les données d'état utilisateur lorsqu'un ordinateur est migré vers un nouveau système d'exploitation. Ce rôle est pris en charge sur les sites principaux et les sites secondaires. Vous pouvez installer plusieurs instances de ce rôle sur un site et sur plusieurs sites dans la même hiérarchie. Pour plus d'informations sur le stockage de l'état utilisateur quand vous déployez un système d'exploitation, consultez Gérer l'état utilisateur dans System Center Configuration Manager.

- **Point du programme de validation d'intégrité système**. Ce rôle de système de site est toujours visible dans la console Configuration Manager, mais il n'est plus utilisé.

**Rôles système de site pouvant utiliser un serveur proxy**

Certains rôles de système de site Configuration Manager requièrent des connexions à Internet et utilisent un serveur proxy quand le serveur de système de site hébergeant le rôle est configuré pour cela. En règle générale, cette connexion est établie dans le **système** de l'ordinateur sur lequel le rôle de système de site est installé. La connexion ne peut pas utiliser une configuration proxy pour les comptes d'utilisateurs standard. Quand un serveur proxy est requis pour établir une connexion à Internet, vous devez configurer l'ordinateur pour qu'il utilise un serveur proxy :

- Vous pouvez configurer un serveur proxy lors de l'installation d'un rôle de système de site.

- Vous pouvez ajouter ou modifier une configuration de serveur proxy quand vous utilisez la console Configuration Manager.

- Tous les rôles de système de site sur un serveur de système de site qui peuvent utiliser une configuration de serveur proxy adoptent la même configuration. S'il est nécessaire que différents rôles de système de site utilisent différents serveurs proxy, vous devez installer les rôles de système de site sur différents ordinateurs de serveur de système de site.

- Si vous modifiez la configuration du serveur proxy, ou installez un nouveau rôle système de site sur un ordinateur ayant déjà une configuration du serveur proxy, la configuration d'origine est remplacée par la nouvelle.

Pour connaître les procédures de configuration du serveur proxy pour des rôles de système de site, consultez la rubrique Ajouter des rôles de système de site pour System Center Configuration Manager.

Les rôles système de site pouvant utiliser un serveur proxy sont les suivants :

- **Point de synchronisation Asset Intelligence**. Ce rôle de système de site se connecte à Microsoft et utilise une configuration de serveur proxy sur l'ordinateur hébergeant le point de synchronisation Asset Intelligence.

- **Point de distribution cloud**. Lorsque vous utilisez un point de distribution cloud, le site principal qui gère ce point doit pouvoir se connecter à Microsoft Azure pour configurer, surveiller et distribuer un contenu au point de distribution. Si un serveur proxy est requis pour cette connexion, vous devez configurer le serveur proxy sur le serveur de site principal. Vous ne pouvez pas configurer un serveur proxy sur le point de distribution cloud dans Azure. Pour plus d'informations, consultez la section Configurer les paramètres de proxy pour des sites principaux gérant des services cloud dans la rubrique Installer des points de distribution cloud dans Microsoft Azure pour System Center Configuration Manager.

- **Connecteur Exchange Server**. Ce rôle de système de site se connecte à un serveur Exchange Server et utilise une configuration de serveur proxy sur l'ordinateur qui héberge le connecteur Exchange Server.

- **Point de mise à jour logicielle**. Ce rôle de système de site peut nécessiter des connexions à Microsoft Update pour télécharger des correctifs et synchroniser les informations sur les mises à jour. En règle générale, lorsque vous configurez le serveur proxy, chaque rôle de système de site sur l'ordinateur qui

prend en charge l'utilisation du serveur proxy utilise le serveur proxy. Aucune configuration manuelle n'est requise. Le point de mise à jour logicielle est une exception à cette règle. Par défaut, un point de mise à jour logicielle n'utilise pas de serveur proxy disponible, sauf si vous activez également les options suivantes lors de la configuration du point de mise à jour logicielle :

- **Utiliser un serveur proxy lors de la synchronisation des mises à jour logicielles**
- **Utiliser un serveur proxy lors du téléchargement du contenu avec des règles de déploiement automatiques**

> **TIP**
> Pour pouvoir sélectionner l'une ou l'autre option, vous devez configurer un serveur proxy sur le serveur de système de site qui héberge le point de mise à jour logicielle. Le serveur proxy est utilisé uniquement pour les options spécifiques que vous sélectionnez.

Pour plus d'informations sur les serveurs proxy associés aux points de mise à jour logicielle, consultez la section Paramètres du serveur proxy dans la rubrique Installer et configurer un point de mise à jour logicielle.

- **Point de connexion de service**. Lorsque ce rôle de système de site est configuré pour être en ligne (et non hors connexion), il se connecte à Microsoft Intune et au service cloud Microsoft.

# Principes de base de la gestion de contenu dans Configuration Manager

10/07/2018 • 26 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Configuration Manager fournit un puissant système d'outils et d'options pour vous aider à gérer le contenu que vous déployez (applications, packages, mises à jour logicielles et déploiements de système d'exploitation). Configuration Manager stocke le contenu à la fois sur les serveurs de site et sur les points de distribution. Le transfert de ce contenu d'un emplacement à un autre nécessite une large bande passante réseau. Pour planifier et utiliser efficacement l'infrastructure de gestion de contenu, de vous familiariser avec les options et configurations disponibles. Déterminez ensuite comment les utiliser au mieux en fonction de votre environnement réseau et de vos besoins en matière de déploiement de contenu.

> **TIP**
> Pour obtenir plus d'informations sur le processus de distribution de contenu, ainsi que trouver de l'aide sur le diagnostic et la résolution des problèmes généraux relatifs à la distribution de contenu, consultez Compréhension et résolution des problèmes de distribution de contenu dans Microsoft Configuration Manager.

Les rubriques suivantes exposent des concepts clés de la gestion de contenu. Si un concept doit être complété par des informations supplémentaires ou complexes, les liens d'accès à ces informations sont indiqués.

## Comptes utilisés pour la gestion de contenu

Les comptes suivants peuvent être utilisés pour la gestion de contenu :

- **Compte d'accès réseau**: compte utilisé par les clients pour se connecter à un point de distribution et accéder au contenu. Par défaut, le compte d'ordinateur est utilisé en premier.

  Ce compte est également utilisé par les points de distribution d'extraction pour télécharger du contenu à partir d'un point de distribution source dans une forêt distante.

- **Compte d'accès au package** : par défaut, Configuration Manager permet aux utilisateurs et aux administrateurs des comptes d'accès génériques d'accéder au contenu sur un point de distribution. Toutefois, vous pouvez configurer des autorisations supplémentaires pour limiter l'accès.

- **Compte de connexion multidiffusion** : utilisé pour les déploiements de système d'exploitation.

Pour plus d'informations sur ces comptes, consultez Gérer les comptes pour accéder au contenu.

## Limitation et planification de la bande passante

La limitation et la planification sont des options qui vous aident à contrôler la distribution du contenu d'un serveur de site vers des points de distribution. Ces fonctionnalités sont similaires aux contrôles de bande passante pour la réplication de site à site basée sur des fichiers, sans leur être directement liés.

Pour plus d'informations, consultez Gérer la bande passante réseau.

## Réplication différentielle binaire

La réplication différentielle binaire est un prérequis pour les points de distribution. Elle est parfois simplement appelée « réplication différentielle ». Lors de la distribution de mises à jour à un contenu que vous avez précédemment déployé sur d'autres sites ou sur des points de distribution distants, la réplication différentielle binaire est automatiquement utilisée pour réduire la bande passante utilisée.

Cette fonctionnalité réduit la bande passante réseau utilisée lors de l'envoi des mises à jour du contenu distribué. Elle renvoie uniquement le contenu nouveau ou modifié au lieu d'envoyer l'ensemble complet des fichiers sources de contenu chaque fois qu'un changement est apporté à ces fichiers.

Quand vous utilisez la réplication différentielle binaire, Configuration Manager identifie les changements apportés aux fichiers sources pour chaque jeu de contenus que vous avez précédemment distribué.

- Quand des fichiers du contenu source changent, le site crée une nouvelle version incrémentielle du jeu de contenus. Il ne réplique ensuite que les fichiers modifiés sur les sites de destination et les points de destination. Un fichier est considéré comme modifié si vous l'avez renommé ou déplacé, ou si vous avez modifié son contenu. Par exemple, si vous remplacez un seul fichier de pilote pour un package de pilotes que vous avez précédemment distribué vers plusieurs sites, seul le fichier du pilote modifié est répliqué.
- Configuration Manager prend en charge jusqu'à cinq versions incrémentielles d'un jeu de contenus avant de renvoyer le jeu de contenus entier. Après la cinquième mise à jour, la modification suivante du jeu de contenus entraîne la création, par le site, d'une nouvelle version du jeu de contenus. Configuration Manager distribue ensuite la nouvelle version du jeu de contenus pour remplacer le jeu précédent et toutes ses versions incrémentielles. Après la distribution du nouveau jeu de contenus, les modifications incrémentielles ultérieures apportées aux fichiers sources sont de nouveau répliquées en utilisant la réplication différentielle binaire.

La réplication différentielle binaire est prise en charge entre chaque site parent et enfant dans une hiérarchie. Elle est prise en charge dans un site entre le serveur de site et ses points de distribution normaux. Toutefois, les points de distribution d'extraction et les points de distribution cloud ne prennent pas en charge la réplication différentielle binaire pour le transfert de contenu. Les points de distribution d'extraction prennent en charge les deltas de niveau fichier et le transfert de nouveaux fichiers, mais pas les blocs au sein d'un fichier.

Les applications utilisent toujours la réplication différentielle binaire. La réplication différentielle binaire est facultative pour les packages et n'est pas activée par défaut. Pour utiliser la réplication différentielle binaire pour les packages, activez cette fonctionnalité pour chaque package. Sélectionnez l'option **Activer la réplication différentielle binaire** quand vous créez ou modifiez un package.

## BranchCache

BranchCache est une technologie Windows. Les clients prenant en charge BranchCache et ayant téléchargé un déploiement que vous configurez pour BranchCache font alors office de source de contenu pour d'autres clients BranchCache.

Par exemple, vous disposez d'un point de distribution qui exécute Windows Server 2012 ou une version ultérieure et qui est configuré comme serveur BranchCache. Quand le premier client prenant en charge BranchCache demande du contenu à partir de ce serveur, le client télécharge ce contenu et le met en cache.

- Ce client met ensuite le contenu à la disposition d'autres clients BranchCache du même sous-réseau qui mettent également en cache le contenu.
- Les autres clients du même sous-réseau n'ont pas à télécharger le contenu à partir du point de distribution.
- Le contenu est distribué sur plusieurs clients, en vue de transferts futurs.

Pour plus d'informations, consultez Prise en charge de Windows BranchCache.

## Optimisation de la distribution

Les groupes de limites Configuration Manager permettent de définir et de réguler la distribution de contenu sur le réseau de l'entreprise et dans les agences. L'Optimisation de la distribution de Windows est une technologie cloud pair à pair de partage de contenu entre appareils Windows 10. À compter de la version 1802, configurez-la de façon à ce qu'elle utilise vos groupes de limites pour partager du contenu entre homologues. Les paramètres client appliquent l'identificateur de groupe de limites comme identificateur du groupe Optimisation de la distribution sur le client. Lorsque le client communique avec le service de cloud d'Optimisation de la distribution, il utilise cet identificateur pour localiser les pairs possédant le contenu souhaité. Pour plus d'informations, consultez les paramètres client de l'optimisation de la distribution.

L'optimisation de la distribution est la technologie recommandée pour optimiser la distribution de la mise à jour Windows 10 des fichiers d'installation rapide pour les mises à jour de qualité de Windows 10.

## Cache d'homologue

Le cache d'homologue client vous permet de gérer le déploiement de contenu sur les clients distants. Le cache d'homologue est une solution Configuration Manager intégrée qui permet aux clients de partager du contenu avec d'autres clients directement à partir de leur cache local.

Une fois que vous avez déployé des paramètres client qui activent le cache d'homologue sur un regroupement, les membres de ce regroupement peuvent agir comme source de contenu homologue pour d'autres clients du même groupe de limites.

Pour plus d'informations, consultez Cache d'homologue pour les clients Configuration Manager.

## Mise en cache d'homologue Windows PE

Quand vous déployez un nouveau système d'exploitation avec Configuration Manager, les ordinateurs qui exécutent la séquence de tâches peuvent utiliser la mise en cache d'homologue Windows PE. Ils téléchargent le contenu à partir d'une source de mise en cache d'homologue au lieu de le télécharger à partir d'un point de distribution. Ce comportement permet de réduire le trafic WAN dans les scénarios de filiale où il n'existe aucun point de distribution local.

Pour plus d'informations, consultez Mise en cache d'homologue Windows PE.

## Emplacements des clients

Les clients accèdent au contenu à partir des emplacements suivants :

- **Intranet** (local) :
  - Les points de distribution peuvent utiliser HTTP ou HTTPS.
  - Utilisez uniquement un point de distribution cloud de secours quand les points de distribution locaux ne sont pas disponibles.
- **Internet** :
  - Exige des points de distribution qu'ils acceptent le protocole HTTPS.
  - Vous pouvez utiliser un point de distribution cloud de secours.
- **Groupe de travail**:
  - Exige des points de distribution qu'ils acceptent le protocole HTTPS.
  - Vous pouvez utiliser un point de distribution cloud de secours.

## Bibliothèque de contenu

La bibliothèque de contenu est un stockage SIS (Single-Instance-Store) de contenu dans Configuration Manager. Cette bibliothèque permet de réduire la taille globale du contenu que vous distribuez.

- En savoir plus sur la bibliothèque de contenu.
- Utilisez l'outil de nettoyage de la bibliothèque de contenu pour supprimer le contenu qui n'est plus associé à une application.

## Points de distribution

Configuration Manager utilise des points de distribution pour stocker les fichiers nécessaires à l'exécution de logiciels sur les ordinateurs clients. Les clients doivent avoir accès à au moins un point de distribution à partir duquel ils peuvent télécharger les fichiers du contenu que vous déployez.

Le point de distribution (non spécifique) de base est communément appelé point de distribution standard. Il existe deux variantes du point de distribution standard qui reçoivent une attention particulière :

- **Point de distribution d'extraction** : variation d'un point de distribution où le point de distribution obtient le contenu à partir d'un autre point de distribution (point de distribution source). Ce processus est similaire à la façon dont les clients téléchargent le contenu à partir de points de distribution. Les points de distribution d'extraction peuvent vous permettre d'éviter les goulots d'étranglement de bande passante réseau qui surviennent quand le serveur de site doit distribuer directement le contenu à chaque point de distribution. Utilisez un point de distribution d'extraction.
- **Point de distribution cloud** : variante d'un point de distribution, installée dans Microsoft Azure. Découvrez comment utiliser un point de distribution cloud.

Les points de distribution standard prennent en charge diverses configurations et fonctionnalités :

- Utilisez des contrôles tels que des **planifications** ou une **limitation de bande passante** pour contrôler ce transfert.
- Utilisez d'autres options, dont le **contenu préparé** et les **points de distribution d'extraction** pour réduire et contrôler la consommation réseau.
- **BranchCache**, le **cache d'homologue** et l'**optimisation de la distribution** sont des technologies pair à pair permettant de réduire la bande passante réseau utilisée quand vous déployez du contenu.
- Il existe différentes configurations pour les déploiements de système d'exploitation, comme **PXE** et la **multidiffusion**.
- Options pour les **appareils mobiles**

Les points de distribution d'extraction et cloud prennent en charge un grand nombre de ces configurations, mais présentent des limitations spécifiques à chaque variante de point de distribution.

## Groupes de points de distribution

Les groupes de points de distribution sont des regroupements logiques de points de distribution qui peuvent simplifier la distribution de contenu.

Pour plus d'informations, voir Gérer les groupes de points de distribution.

## Priorité des points de distribution

La valeur de priorité d'un point de distribution est basée sur le temps nécessaire au transfert des déploiements précédents vers ce point de distribution.

- Cette valeur s'ajuste automatiquement. Elle est définie sur chaque point de distribution pour aider Configuration Manager à transférer plus rapidement du contenu vers un plus grand nombre de points de distribution.

- Quand vous distribuez du contenu simultanément à plusieurs points de distribution, ou à un groupe de points de distribution, le site envoie d'abord le contenu au serveur avec la priorité la plus haute. Il envoie ensuite ce même contenu à un point de distribution avec une priorité plus faible.
- La priorité d'un point de distribution ne remplace pas la priorité de distribution pour les packages. La priorité des packages reste le facteur décisif du moment où le site envoie un contenu différent.

Par exemple, vous disposez d'un package ayant une priorité de package élevée. Vous le distribuez à un serveur ayant une priorité de point de distribution faible. Ce package à priorité élevée est toujours transféré avant un package ayant une priorité plus faible. La priorité des packages s'applique même si le site distribue des packages de priorité plus faible sur des serveurs ayant des priorités de point de distribution plus élevées.

La priorité élevée du package permet à Configuration Manager de distribuer ce contenu à des points de distribution avant d'envoyer les packages ayant une priorité inférieure.

> **NOTE**
> Les points de distribution d'extraction utilisent également un concept de priorité pour ordonner la séquence de leur points de distribution source.
>
> - La priorité des points de distribution pour les transferts de contenu vers le serveur est différente de la priorité qu'utilisent les points de distribution d'extraction. Les points de distribution d'extraction utilisent leur priorité quand ils recherchent du contenu à partir d'un point de distribution source.
> - Pour plus d'informations, consultez Utiliser un point de distribution d'extraction.

## Secours

Plusieurs choses ont changé avec Current Branch de Configuration Manager dans la manière dont les clients recherchent un point de distribution qui a du contenu, notamment les scénarios de secours.

Les clients qui ne trouvent pas de contenu à partir d'un point de distribution associé à leur groupe de limites actuel utilisent des emplacements sources de contenu associés à des groupes de limites voisins. Pour faire office de groupe de secours, un groupe de limites voisin doit avoir une relation définie avec le groupe de limites actuel du client. Cette relation inclut une durée configurée qui doit s'écouler avant qu'un client qui ne trouve pas de contenu localement inclut dans sa recherche des sources de contenu issues du groupe de limites voisin.

Les concepts de points de distribution préférés ne sont plus utilisés, et les paramètres d'**autorisation des emplacements sources de secours pour le contenu** ne sont plus disponibles ou appliqués.

Pour plus d'informations, consultez Groupes de limites.

## Bande passante du réseau

Pour mieux gérer la largeur de la bande passante réseau utilisée quand vous distribuez du contenu, vous pouvez utiliser les options suivantes :

- **Contenu préparé** : transfert de contenu vers un point de distribution sans distribuer le contenu sur le réseau.
- **Planification et limitation** : configurations qui vous aident à contrôler quand et comment le contenu est distribué aux points de distribution.

Pour plus d'informations, consultez Gérer la bande passante réseau.

## Vitesse de la connexion réseau vers la source de contenu

Plusieurs choses ont changé avec Current Branch de Configuration Manager dans la manière dont les clients

recherchent un point de distribution qui a du contenu. Ces changements incluent la vitesse du réseau pour accéder à une source de contenu.

Les vitesses de connexion réseau qui définissent un point de distribution comme **Rapide** ou **Lent** ne sont plus utilisées. Au lieu de cela, chaque système de site associé à un groupe de limites est traité de la même façon.

Pour plus d'informations, consultez Groupes de limites.

## Distribution de contenu à la demande

La distribution de contenu à la demande est une option pour les déploiements d'applications et de packages individuels. Cette option permet la distribution de contenu à la demande vers des serveurs préférés.

- Pour activer ce paramètre pour un déploiement, activez **Distribuer le contenu pour ce package vers les points de distribution préférés**.
- Quand cette option est activée pour un déploiement, si un client tente de demander du contenu qui n'est disponible sur aucun de ses points de distribution préférés, Configuration Manager distribue automatiquement ce contenu aux points de distribution préférés du client.
- Même si cette option force Configuration Manager à distribuer automatiquement le contenu aux points de distribution préférés de ce client, le client peut obtenir ce contenu auprès d'autres points de distribution avant que ses points de distribution préférés reçoivent le déploiement. Quand ce comportement se produit, le contenu est alors disponible sur ce point de distribution pour le prochain client qui cherche ce déploiement.

Pour plus d'informations, consultez Groupes de limites.

## Package Transfer Manager

Package Transfer Manager est le composant de serveur de site qui transfère du contenu vers des points de distribution situés sur d'autres ordinateurs.

Pour plus d'informations, reportez-vous à Package Transfer Manager.

## Contenu préparé

La préparation du contenu est un processus de transfert de contenu vers un point de distribution sans distribuer le contenu sur le réseau.

Pour plus d'informations, consultez Gérer la bande passante réseau.

# Utiliser un point de distribution cloud avec System Center Configuration Manager

22/06/2018 • 26 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Un point de distribution cloud est un point de distribution System Center Configuration Manager qui est hébergé dans Microsoft Azure. Les informations suivantes visent à vous faire découvrir les différentes configurations et limitations liées à l'utilisation d'un point de distribution cloud.

Quand vous avez installé un site principal et que vous êtes prêt à installer un point de distribution cloud, consultez Installer des points de distribution cloud dans Microsoft Azure.

## Planifier l'utilisation d'un point de distribution cloud

Lorsque vous utilisez une distribution cloud, vous devez :

- **Configurer les paramètres clients** pour permettre aux utilisateurs et aux appareils d'accéder au contenu.
- **Spécifier un site principal pour gérer le transfert de contenu** vers le point de distribution.
- **Définir des seuils** pour la quantité de contenu que vous voulez stocker sur le point de distribution et celle pouvant être transférée par les clients à partir du point de distribution.

Selon les seuils configurés, Configuration Manager peut déclencher des alertes pour vous avertir quand le volume total de contenu que vous avez stocké sur le point de distribution approche de la quantité de stockage spécifiée, ou quand les transferts de données par les clients avoisinent les seuils définis.

Les points de distribution cloud prennent en charge plusieurs fonctionnalités également proposées par les points de distribution locaux :

- Vous gérez les points de distribution cloud individuellement ou en tant que membres de groupes de points de distribution.
- Vous pouvez utiliser un point de distribution cloud comme emplacement de contenu de secours.
- Prise en charge des clients basés sur intranet et Internet.

Les points de distribution cloud offrent les autres avantages suivants :

- Configuration Manager chiffre le contenu envoyé à un point de distribution cloud, avant de l'envoyer à Azure.
- Dans Azure, vous pouvez adapter manuellement le service cloud en fonction des demandes de contenu émanant des clients, sans avoir à installer et préparer des points de distribution supplémentaires.
- Le point de distribution cloud prend en charge le téléchargement de contenu par les clients configurés pour Windows BranchCache.

Un point de distribution cloud présente les limitations suivantes :

- Avant d'utiliser la version 1610 avec le correctif KB4010155, vous ne pouvez pas utiliser un point de distribution cloud pour héberger des packages de mises à jour logicielles. Ce problème est résolu dans la version 1702 et les versions ultérieures.

- Vous ne pouvez pas utiliser un point de distribution cloud pour PXE ou les déploiements en multidiffusion.
- Aucun point de distribution cloud n'est proposé aux clients en guise d'emplacement de contenu pour une séquence de tâches déployée à l'aide de l'option **Télécharger le contenu localement si nécessaire, en exécutant la séquence de tâches**. Toutefois, les séquences de tâches qui sont déployées à l'aide de l'option de déploiement **Télécharger tout le contenu localement avant de démarrer la séquence de tâches** peuvent utiliser un point de distribution cloud en guise d'emplacement de contenu valide.
- Un point de distribution cloud ne prend pas en charge les packages exécutés à partir du point de distribution. Tout le contenu doit être téléchargé par le client et exécuté localement.
- Un point de distribution cloud ne prend pas en charge la diffusion en continu d'applications à l'aide d'Application Virtualization ou de programmes similaires.
- Un point de distribution cloud ne gère pas le contenu préparé. Le Gestionnaire de distribution du site principal qui gère le point de distribution transfère l'ensemble du contenu vers le point de distribution.
- Un point de distribution cloud ne peut pas être configuré en tant que point de distribution d'extraction.

## Conditions préalables pour les points de distribution cloud

Un point de distribution cloud requiert les conditions préalables suivantes pour son utilisation :

- Un abonnement à Azure (consultez À propos des abonnements et des certificats dans cette rubrique.).
- Un certificat de gestion auto-signé ou PKI pour la communication entre un serveur de site principal Configuration Manager et le service cloud dans Azure (consultez À propos des abonnements et des certificats dans cette rubrique).
- Certificat de service (PKI) que les clients Configuration Manager utilisent pour se connecter aux points de distribution cloud et y télécharger du contenu via HTTPS.
- Un appareil ou un utilisateur doit avoir le paramètre client **Autoriser l'accès au point de distribution cloud** réglé sur **Oui** dans **Services cloud** pour pouvoir accéder au contenu d'un point de distribution cloud. Par défaut, cette valeur est définie sur **Non**.
- Un client doit être en mesure de résoudre le nom du service cloud, ce qui nécessite la présence d'un alias DNS (Domain Name System) et d'un enregistrement CNAME dans votre espace de noms DNS.
- Un client doit pouvoir accéder à Internet pour utiliser le point de distribution cloud.

## Coût d'utilisation d'une distribution cloud

Lorsque vous utilisez un point de distribution cloud, planifiez le coût du stockage de données et des téléchargements que les clients Configuration Manager effectuent.

Configuration Manager inclut des options facilitant le contrôle des coûts et de l'accès aux données :

- Vous pouvez contrôler et surveiller la quantité de contenu que vous stockez dans un service cloud.
- Vous pouvez configurer Configuration Manager pour être averti lorsque les **seuils** mensuels des téléchargements du client sont atteints ou dépassés.
- De plus, vous pouvez utiliser la mise en cache d'homologue (Windows BranchCache) pour réduire le nombre de transferts de données que les clients effectuent à partir des points de distribution cloud. Les clients Configuration Manager configurés pour Windows BranchCache peuvent transférer du contenu à l'aide des points de distribution cloud.

**Options :**

- **Paramètres client pour cloud**: vous pouvez contrôler l'accès à tous les points de distribution cloud d'une hiérarchie à l'aide des **Paramètres client**.

  Dans **Paramètres client**, la catégorie des **paramètres cloud** prend en charge le paramètre **Autoriser l'accès au point de distribution cloud**. Par défaut, ce paramètre est défini sur **Non**. Vous pouvez l'activer pour les utilisateurs et les appareils.

- **Seuils pour les transferts de données**: vous pouvez configurer des seuils pour la quantité de données que vous voulez stocker sur le point de distribution et pour la quantité de données que les clients peuvent télécharger à partir du point de distribution.

  Les seuils des points de distribution cloud sont les suivants :

  - **Seuil d'alerte de stockage**: un seuil d'alerte de stockage définit la limite supérieure de la quantité de données ou de contenu que vous souhaitez stocker sur le point de distribution cloud. Configuration Manager peut générer une alerte d'avertissement lorsque l'espace disponible atteint le niveau défini.

  - **Seuil d'alerte de transfert**: un seuil d'alerte de transfert permet de surveiller la quantité de contenu transféré à partir du point de distribution vers les clients pendant une période de 30 jours. Le seuil d'alerte de transfert surveille le transfert de données pendant les 30 derniers jours et peut émettre une alerte d'avertissement et une alerte critique lorsque les transferts atteignent la valeur définie.

    > **IMPORTANT**
    > Configuration Manager surveille le transfert de données, mais n'interrompt pas ce transfert au-delà du seuil d'alerte de transfert défini.

  Vous pouvez définir des seuils pour chaque point de distribution cloud pendant l'installation du point de distribution ou modifier les propriétés de chaque point de distribution cloud après son installation.

- **Alertes** : vous pouvez configurer Configuration Manager de manière à déclencher des alertes pour les transferts de données à destination et en provenance de chaque point de distribution cloud, en fonction des seuils de transfert de données que vous spécifiez. Ces alertes vous aident à surveiller les transferts de données, à décider quand arrêter le service cloud, à ajuster le contenu que vous stockez sur le point de distribution ou à modifier les clients pouvant utiliser les points de distribution cloud.

  Dans un cycle horaire, le site principal qui surveille le point de distribution cloud télécharge des données transactionnelles à partir d'Azure et les stocke dans le fichier CloudDP-<nom_service>.log sur le serveur de site. Configuration Manager évalue ensuite ces informations par rapport aux quotas de stockage et de transfert pour chaque point de distribution du cloud. Lorsque le transfert de données atteint ou dépasse le volume défini pour les avertissements ou alertes critiques, Configuration Manager génère l'alerte appropriée.

  > **WARNING**
  > Comme les informations sur les transferts de données sont téléchargées depuis Azure toutes les heures, cette utilisation des données peut dépasser un seuil d'avertissement ou critique avant même que Configuration Manager n'accède aux données et n'émette une alerte.

> **NOTE**
>
> Les alertes pour un point de distribution cloud dépendent des statistiques d'utilisation fournies par Azure, un délai qui peut aller jusqu'à 24 heures. Pour plus d'informations sur Storage Analytics pour Azure et la fréquence de mise à jour des statistiques d'utilisation, consultez Storage Analytics dans la bibliothèque MSDN Library.

- **Arrêter ou démarrer le service cloud à la demande**: vous pouvez choisir d'arrêter un service cloud à tout moment pour empêcher les clients de l'utiliser en continu. Lorsque vous arrêtez le service cloud, vous empêchez immédiatement les clients de télécharger tout autre contenu à partir du service. Vous pouvez redémarrer le service cloud pour restaurer l'accès aux clients. Par exemple, vous pouvez choisir d'arrêter un service cloud lorsque les seuils de données sont atteints.

  Lorsque vous arrêtez un service cloud, le service cloud ne supprime pas le contenu du point de distribution et n'empêche pas le serveur de site de transférer du contenu supplémentaire vers le point de distribution cloud.

  Pour arrêter un service cloud, dans la console Configuration Manager, sélectionnez le point de distribution dans le nœud **Points de distribution cloud**, sous **Services cloud**dans l'espace de travail **Administration**. Ensuite, cliquez sur **Arrêter le service** pour arrêter le service cloud qui s'exécute dans Azure.

## À propos des abonnements et certificats pour les points de distribution cloud

Les points de distribution cloud ont besoin de certificats pour permettre à Configuration Manager de gérer le service cloud qui héberge le point de distribution et aux clients d'accéder au contenu à partir du point de distribution. Vous trouverez ci-dessous des informations générales sur ces certificats. Pour plus d'informations, consultez Configuration requise des certificats PKI pour Configuration Manager.

**Certificats**

- **Certificat de gestion pour la communication entre un serveur de site et un point de distribution** : le certificat de gestion établit la relation de confiance entre l'API de gestion Azure et Configuration Manager. Cette authentification permet à Configuration Manager d'appeler l'API Azure quand vous effectuez des tâches comme le déploiement de contenu ou le démarrage et l'arrêt du service cloud. Azure permet aux clients de créer leurs propres certificats de gestion, qu'il s'agisse de certificats auto-signés ou de certificats émis par une Autorité de certification (AC) :

  - Fournissez le fichier .cer du certificat de gestion à Azure quand vous configurez Azure pour Configuration Manager. Le fichier .cer contient la clé publique pour le certificat de gestion. Avant d'installer un point de distribution cloud, vous devez charger ce certificat dans Azure. Il permet à Configuration Manager d'accéder à l'API Azure.

  - Fournissez le fichier .pfx du certificat de gestion à Configuration Manager lorsque vous installez le point de distribution cloud. Le fichier .pfx contient la clé privée pour le certificat de gestion. Configuration Manager stocke ce certificat dans la base de données du site. Comme le fichier .pfx contient la clé privée, vous devez fournir le mot de passe pour importer ce fichier de certificat dans la base de données Configuration Manager.

  Si vous créez un certificat auto-signé, vous devez d'abord l'exporter au format .cer puis au format .pfx.

  Vous pouvez éventuellement spécifier un fichier **.publishsettings** version 1 du Kit de développement logiciel (SDK) Azure 1.7. Pour plus d'informations sur les fichiers .publishsettings, consultez la documentation d'Azure.

Pour plus d'informations, consultez Vue d'ensemble des certificats pour Azure Cloud Services et How to add a management certificate to an Azure subscription (Comment ajouter un certificat de gestion à un abonnement Azure) dans la section de la bibliothèque MSDN consacrée à la plateforme Azure.

- **Certificat de service pour la communication entre le client et le point de distribution** : le certificat de service du point de distribution cloud Configuration Manager établit une relation de confiance entre les clients Configuration Manager et le point de distribution cloud, puis sécurise les données que les clients téléchargent à partir de ce point de distribution grâce au protocole SSL (Secure Socket Layer) sur HTTPS.

  > **IMPORTANT**
  > Le nom commun dans la zone d'objet de certificat du certificat de service doit être unique dans votre domaine et ne correspondre à aucun appareil joint à un domaine.

  Pour obtenir un exemple de déploiement de ce certificat, consultez la section **Déployer le certificat de service pour les points de distribution cloud** dans la rubrique Exemple de déploiement pas à pas des certificats PKI pour System Center Configuration Manager : autorité de certification Windows Server 2008.

## Tâches de gestion courantes pour les points de distribution cloud

- **Communication entre un serveur de site et un point de distribution cloud**: quand vous installez un point de distribution cloud, vous devez affecter un site principal pour gérer le transfert de contenu vers le service cloud. Le principe est le même que lorsque vous installez le rôle de système de site du point de distribution sur un site spécifique.
- **Communication entre un client et un point de distribution cloud**: quand le paramètre client permettant l'utilisation d'un point de distribution cloud est activé pour un appareil ou un utilisateur d'appareil, l'appareil en question peut recevoir le point de distribution cloud comme emplacement de contenu valide :
  - Lorsqu'un client évalue les emplacements de contenu disponibles, un point de distribution cloud est considéré comme un point de distribution distant.
  - Les clients connectés via l'intranet utilisent uniquement les points de distribution cloud comme solution de secours si les points de distribution sur site ne sont pas disponibles.

  Même si vous installez les points de distribution cloud dans des zones spécifiques d'Azure, les clients qui utilisent les points de distribution cloud ne connaissent pas ces régions Azure et sélectionnent un point de distribution cloud de façon non déterministe.

Par conséquent, si vous installez des points de distribution cloud dans plusieurs régions et qu'un client reçoit plusieurs points de distribution cloud comme emplacements de contenu, le client peut ne pas utiliser un point de distribution cloud de la même zone Azure que le client.

Pour effectuer des demandes d'emplacement de contenu, les clients qui utilisent des points de distribution cloud respectent la séquence suivante :

1. Un client qui est configuré pour utiliser des points de distribution cloud commence toujours par essayer d'obtenir le contenu auprès d'un point de distribution préféré.
2. Lorsque le point de distribution préféré n'est pas disponible, le client utilise un point de distribution distant si le déploiement le permet et si un tel point est disponible.
3. Lorsqu'un point de distribution préféré ou un point de distribution distant n'est pas disponible, le client cherche alors à obtenir le contenu auprès d'un point de distribution cloud.

Lorsqu'un client utilise un point de distribution cloud comme emplacement de contenu, il s'authentifie auprès du point de distribution cloud en utilisant un jeton d'accès Configuration Manager. Si le client approuve le certificat de point de distribution cloud Configuration Manager, il peut ensuite télécharger le contenu demandé.

- **Surveillance des points de distribution cloud**: vous pouvez surveiller le contenu que vous déployez sur chaque point de distribution cloud, ainsi que le service cloud qui héberge le point de distribution.

  - **Contenu** : vous surveillez le contenu que vous déployez sur un point de distribution cloud comme lorsque vous déployez du contenu sur des points de distribution locaux.

  - **Service cloud** : Configuration Manager vérifie périodiquement le service Azure et émet une alerte si ce dernier est inactif ou si un problème d'abonnement ou de certificat est détecté. Vous pouvez également afficher des informations sur le point de distribution dans le nœud **Points de distribution cloud** sous **Services cloud** dans l'espace de travail **Administration** de la console Configuration Manager. À partir de cet emplacement, vous pouvez consulter les informations générales sur le point de distribution. Vous pouvez également sélectionner un point de distribution et modifier ses propriétés.

  Quand vous modifiez les propriétés d'un point de distribution cloud, vous pouvez :

  - ajuster les seuils de données pour le stockage et les alertes ;

  - gérer le contenu comme pour un point de distribution local.

  Enfin, pour chaque point de distribution cloud, vous pouvez afficher, sans toutefois modifier, l'ID d'abonnement, le nom du service et d'autres informations associées qui sont définies lors de l'installation de la distribution cloud.

- **Sauvegarde et récupération de points de distribution cloud**: quand vous utilisez un point de distribution cloud de votre hiérarchie, aidez-vous des informations suivantes pour planifier la sauvegarde ou la récupération du point de distribution :

  - Lorsque vous utilisez la tâche de maintenance prédéfinie **Serveur de site de sauvegarde**, Configuration Manager inclut automatiquement les configurations du point de distribution cloud.

  - Il est recommandé de sauvegarder et d'enregistrer une copie du certificat de gestion et du certificat de service utilisés avec un point de distribution cloud. En cas de restauration du site principal Configuration Manager qui gère le point de distribution cloud sur un autre ordinateur, vous devez réimporter les certificats pour continuer de les utiliser.

- **Désinstaller un point de distribution cloud** : pour désinstaller un point de distribution cloud, sélectionnez-le dans la console Configuration Manager, puis sélectionnez **Supprimer**.

  Lorsque vous supprimez un point de distribution cloud d'une hiérarchie, Configuration Manager supprime le contenu du service cloud dans Azure.

# Utiliser un point de distribution d'extraction avec System Center Configuration Manager

22/06/2018 • 17 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Un point de distribution d'extraction pour System Center Configuration Manager est un point de distribution standard qui obtient le contenu distribué en le téléchargeant à partir d'un emplacement source tel qu'un client, au lieu de recevoir le contenu du serveur de site.

Lorsque vous déployez du contenu sur un grand nombre de points de distribution au niveau d'un site, les points de distribution d'extraction contribuent à réduire la charge de traitement du serveur de site et accélèrent le transfert du contenu vers chaque point de distribution. Pour cela, vous devez décharger le processus de transfert du contenu sur chaque point de distribution à partir du processus du gestionnaire de distribution sur le serveur de site.

- Vous configurez des points de distribution comme des points de distribution d'extraction.
- Pour chaque point de distribution d'extraction, vous devez spécifier un ou plusieurs points de distribution sources à partir desquels il peut obtenir des déploiements. (Un point de distribution d'extraction ne peut obtenir du contenu qu'à partir d'un point de distribution spécifié comme point de distribution source.)
- Quand vous distribuez du contenu vers un point de distribution d'extraction, le serveur de site avertit ce point de distribution, qui lance alors le téléchargement (transfert) du contenu à partir d'un point de distribution source. Chaque point de distribution d'extraction gère individuellement le transfert du contenu en téléchargeant le contenu à partir d'un point de distribution qui possède déjà une copie du contenu.

Les points de distribution d'extraction prennent en charge les mêmes configurations et fonctionnalités que les points de distribution classiques de Configuration Manager. Par exemple, un point de distribution configuré en tant que point de distribution d'extraction prend en charge l'utilisation de configurations de multidiffusion et PXE, la validation de contenu et la distribution de contenu à la demande. Un point de distribution d'extraction prend en charge les communications des clients HTTP ou HTTPS, gère les mêmes options de certificat que les autres points de distribution et peut être géré individuellement ou en tant que membre d'un groupe de points de distribution.

> **IMPORTANT**
> Bien qu'un point de distribution d'extraction prenne en charge les communications par HTTP et HTTPS, lorsque vous utilisez Configuration Manager, vous ne pouvez spécifier que des points de distribution sources configurés pour HTTP. Le Kit de développement logiciel (SDK) Configuration Manager permet de spécifier un point de distribution source configuré pour le protocole HTTPS.

**Quand vous distribuez du contenu vers un point de distribution d'extraction, la séquence d'événements est la suivante :**

- Dès que du contenu est distribué à un point de distribution d'extraction, sur le serveur de site, le composant Package Transfer Manager vérifie la base de données de site pour confirmer si le contenu est disponible sur un point de distribution source. Si Package Transfer Manager ne peut pas confirmer que le contenu se trouve sur un point de distribution source pour le point de distribution d'extraction, la vérification est répétée toutes les 20 minutes jusqu'à ce que le contenu soit disponible.
- Une fois la disponibilité du contenu confirmée par Package Transfer Manager, une notification est adressée au point de distribution d'extraction pour télécharger le contenu. Si cette notification échoue, il réessayera en

fonction des **Paramètres de nouvelle tentative** du composant de distribution de logiciels pour les points de distribution d'extraction. Après avoir reçu cette notification, le point de distribution d'extraction tente de télécharger le contenu auprès de ses points de distribution source.

- Pendant que le point de distribution d'extraction télécharge le contenu, Package Transfer Manager interroge l'état en fonction des **Paramètres d'interrogation de l'état** du composant de distribution de logiciels pour les points de distribution d'extraction. Une fois le téléchargement du contenu terminé, le point de distribution d'extraction soumet cet état à un point de gestion.

**Vous pouvez configurer un point de distribution d'extraction** pendant l'installation du point de distribution ou après son installation en modifiant les propriétés du rôle de système de site du point de distribution.

**Vous pouvez supprimer la configuration de point de distribution d'extraction** en modifiant les propriétés du point de distribution. Lorsque vous supprimez la configuration de point de distribution d'extraction, le point de distribution reprend un fonctionnement normal et les prochains transferts de contenu vers le point de distribution sont alors gérés par le serveur de site.

## Pour configurer le composant de distribution de logiciels pour les points de distribution d'extraction

1. Dans la console Configuration Manager, choisissez **Administration** > **Sites**.
2. Sélectionnez le site de votre choix, puis sélectionnez **Configurer les composants de site** > **Distribution de logiciels**.
3. Sélectionnez l'onglet **Point de distribution d'extraction**.
4. Dans la liste **Paramètres de nouvelle tentative**, configurez les valeurs suivantes :
   - **Nombre de tentatives** : nombre de fois où Package Transfer Manager tente de notifier le point de distribution d'extraction pour télécharger le contenu. Si ce nombre est dépassé, Package Transfer Manager annule le transfert.
   - **Délai avant une nouvelle tentative (en minutes)** : nombre de minutes d'attente de Package Transfer Manager entre les tentatives.
5. Dans la liste **Paramètres d'interrogation de l'état**, configurez les valeurs suivantes :
   - **Nombre d'interrogations** : nombre de fois où Package Transfer Manager contacte le point de distribution d'extraction pour recevoir l'état de la tâche. Si ce nombre est dépassé avant l'achèvement de la tâche, Package Transfer Manager annule le transfert.
   - **Délai avant une nouvelle tentative (en minutes)** : nombre de minutes d'attente de Package Transfer Manager entre les tentatives.

> **NOTE**
> Quand Package Transfer Manager annule une tâche en raison du dépassement du nombre de tentatives d'interrogation de l'état, le point de distribution d'extraction continue à télécharger le contenu. Quand il a terminé, le message d'état approprié est envoyé à Package Transfer Manager et la console reflète le nouvel état.

## Limitations des points de distribution d'extraction

- Un point de distribution cloud ne peut pas être configuré en tant que point de distribution d'extraction.
- Un point de distribution sur un serveur de site ne peut pas être configuré en tant que point de distribution d'extraction.

- **La configuration de contenu préparé se substitue à la configuration du point de distribution d'extraction**. Un point de distribution d'extraction configuré pour du contenu préparé attend le contenu. Il n'extrait pas de contenu d'un point de distribution source et, comme un point de distribution standard avec la configuration de contenu préparé, il ne reçoit pas de contenu du serveur de site.
- **Un point de distribution d'extraction n'utilise pas de configurations pour la planification ou les limites de taux de transfert** lors du transfert de contenu. Si vous configurez un point de distribution précédemment installé comme point de distribution d'extraction, les configurations de la planification et des limites de taux de transfert sont enregistrées, mais pas utilisées. Si, par la suite, vous supprimez la configuration du point de distribution d'extraction, les configurations de la planification et des limites de taux de transfert sont implémentées selon la configuration précédente.

  > **NOTE**
  > Quand un point de distribution est configuré comme point de distribution d'extraction, les onglets **Planification** et **Limites du taux de transfert** ne sont pas disponibles dans les propriétés du point de distribution.

- Les points de distribution d'extraction n'utilisent pas les paramètres de l'onglet **Général** des **Propriétés du composant de distribution de logiciels** de chaque site. Cela inclut les paramètres de **distribution simultanée** et de **nouvelle tentative de multidiffusion**. Utilisez l'onglet **Point de distribution d'extraction** pour configurer les paramètres des points de distribution d'extraction.
- Pour transférer du contenu depuis un point de distribution source dans une forêt distante, un client Configuration Manager doit être installé sur l'ordinateur qui héberge le point de distribution d'extraction. Un compte d'accès réseau qui peut accéder au point de distribution source doit être configuré.
- Sur un ordinateur configuré comme point de distribution d'extraction et exécutant un client Configuration Manager, la version du client doit correspondre à celle du site Configuration Manager qui installe le point de distribution d'extraction. Le point de distribution d'extraction doit impérativement utiliser le composant CCMFramework qui est commun au point de distribution d'extraction et au client Configuration Manager.

## À propos des points de distribution sources

Quand vous configurez le point de distribution d'extraction, vous devez spécifier un ou plusieurs points de distribution sources :

- Seuls les points de distribution considérés comme points de distribution source possibles sont affichés.
- Un point de distribution d'extraction peut être spécifié en tant que point de distribution source d'un autre point de distribution d'extraction.
- Si vous utilisez Configuration Manager, seuls les points de distribution prenant en charge le protocole HTTP peuvent être spécifiés comme des points de distribution sources.
- Le Kit de développement logiciel (SDK) Configuration Manager permet de spécifier un point de distribution source configuré pour le protocole HTTPS. Pour utiliser un point de distribution source configuré pour le protocole HTTPS, le point de distribution d'extraction doit se trouver sur l'ordinateur qui exécute le client Configuration Manager.

Une priorité peut être attribuée à chaque point de distribution figurant dans la liste de points de distribution sources utilisée par le point de distribution d'extraction :

- Vous pouvez affecter une priorité distincte à chaque point de distribution source ou affecter la même priorité à plusieurs points de distribution source.
- La priorité détermine l'ordre dans lequel le point de distribution d'extraction demande du contenu auprès de

ses points de distribution source.

- Les points de distribution d'extraction contactent initialement le point de distribution source présentant la valeur de priorité la plus basse. Si plusieurs points de distribution source présentent la même priorité, le point de distribution d'extraction sélectionne de façon non déterminante l'un des points de distribution source partageant cette priorité.
- Si le contenu n'est pas disponible sur une source sélectionnée, le point de distribution d'extraction tente de télécharger le contenu à partir d'un autre point de distribution présentant le même niveau de priorité.
- Si le contenu n'est pas disponible sur les points de distribution présentant la priorité donnée, le point de distribution d'extraction essaie de télécharger le contenu auprès du point de distribution présentant le niveau de priorité suivant et continue ainsi jusqu'à trouver le contenu, ou bien le point de distribution d'extraction se met en veille pendant 30 minutes et recommence le processus.

Quand un point de distribution d'extraction télécharge du contenu à partir d'un point de distribution source, il est considéré comme un client dans la colonne **Client consulté (unique)** du rapport **Résumé de l'utilisation des points de distribution** .

Par défaut, un point de distribution d'extraction utilise son **compte d'ordinateur** pour transférer le contenu d'un point de distribution source. Toutefois, lorsque le point de distribution d'extraction transfère du contenu à partir d'un point de distribution source qui se trouve dans une forêt distante, il utilise toujours le compte d'accès réseau. Ce processus nécessite que le client Configuration Manager soit installé sur l'ordinateur et qu'un compte d'accès réseau soit configuré pour utiliser le point de distribution source et ait accès à celui-ci.

## À propos des transferts de contenu

Pour gérer le transfert de contenu, les points de distribution d'extraction utilisent le composant **CCMFramework** du logiciel client Configuration Manager.

- Cette infrastructure est installée par **Pulldp.msi** lors de la configuration du point de distribution comme point de distribution d'extraction. Elle n'a pas besoin du client Configuration Manager.
- Une fois le point de distribution d'extraction installé, le service CCMExec doit être opérationnel sur l'ordinateur du point de distribution pour permettre au point de distribution d'extraction de fonctionner.
- Lorsque le point de distribution d'extraction (pull) transfère du contenu, il le fait à l'aide du **Service de transfert intelligent en arrière-plan** (BITS) intégré au système d'exploitation Windows. Un point de distribution d'extraction (pull) ne requiert par l'installation de la fonctionnalité BITS IIS Server Extension facultative.
- Le point de distribution d'extraction (pull) journalise ses opérations dans les fichiers **datatransferservice.log** et **pulldp.log** sur l'ordinateur du point de distribution.

## Voir aussi

Concepts fondamentaux de la gestion de contenu dans System Center Configuration Manager

# Bibliothèque de contenu System Center Configuration Manager

22/06/2018 • 6 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

La bibliothèque de contenu est l'emplacement de stockage SIS (Single-Instance Store) utilisé par Configuration Manager pour réduire la taille globale de l'ensemble du contenu que vous distribuez. Elle stocke tous les fichiers de contenu des mises à jour logicielles, des applications, des déploiements de système d'exploitation, etc.

- Une copie de la bibliothèque de contenu est automatiquement créée et gérée sur chaque **serveur de site** et chaque **point de distribution**.
- Avant de télécharger les fichiers de contenu vers le serveur de site ou de copier les fichiers sur les points de distribution, Configuration Manager vérifie si chaque fichier de contenu se trouve déjà dans la bibliothèque de contenu.
- Si le fichier de contenu est disponible, Configuration Manager ne le copie pas et associe le fichier de contenu existant à l'application ou au package.

Sur les ordinateurs sur lesquels vous installez un point de distribution, vous pouvez configurer les éléments suivants :

- un ou plusieurs lecteurs de disque sur lesquels vous voulez créer la bibliothèque de contenu ;
- une priorité pour chaque lecteur que vous utilisez.

Lorsque Configuration Manager copie des fichiers de contenu, il les copie sur le lecteur ayant la plus haute priorité, sauf si ce lecteur dispose d'une quantité d'espace libre inférieure à la quantité minimale spécifiée.

- Vous configurez les paramètres de lecteur lors de l'installation du point de distribution.
- Vous ne pouvez pas configurer les paramètres de lecteur dans les propriétés du point de distribution, une fois l'installation terminée.

Pour plus d'informations sur la configuration des paramètres de lecteur pour le point de distribution, consultez Gérer le contenu et l'infrastructure de contenu pour System Center Configuration Manager.

> **IMPORTANT**
> Pour déplacer la bibliothèque de contenu vers un autre emplacement sur un point de distribution après l'installation, utilisez l'**outil Content Library Transfer** dans la boîte à outils de System Center 2012 R2 Configuration Manager. Vous pouvez télécharger les outils depuis le Centre de téléchargement Microsoft.

## À propos de la bibliothèque de contenu sur le site d'administration centrale

Par défaut, Configuration Manager crée une bibliothèque de contenu sur le site d'administration centrale, lors de l'installation du site. La bibliothèque de contenu est placée sur le lecteur du serveur de site possédant l'espace disponible le plus important. Comme vous ne pouvez pas installer un point de distribution sur le site d'administration centrale, vous ne pouvez pas attribuer une priorité aux lecteurs à utiliser pour la bibliothèque de contenu. Comme la bibliothèque de contenu sur d'autres serveurs de site ou sur des points de distribution, lorsque le lecteur contenant la bibliothèque de contenu n'a plus d'espace disponible, la bibliothèque de contenu

s'étend sur le lecteur disponible suivant.

Configuration Manager utilise la bibliothèque de contenu sur le site d'administration centrale dans les scénarios suivants :

- Lorsque vous créez un contenu sur le site d'administration centrale.
- Lorsque vous migrez le contenu depuis un autre site Configuration Manager et désignez le site d'administration centrale comme site de gestion du contenu.

> **NOTE**
> Lorsque vous créez un contenu sur un site principal, puis le distribuez à un autre site principal ou à un site secondaire sous un autre site principal, le site d'administration centrale stocke temporairement ce contenu dans la boîte de réception du planificateur sur le site d'administration centrale, sans toutefois ajouter ce contenu à sa bibliothèque de contenu.

Utilisez les options suivantes pour gérer la bibliothèque de contenu sur le site d'administration centrale :

- Pour empêcher l'installation de la bibliothèque de contenu sur un lecteur spécifique, créez un fichier vide nommé **no_sms_on_drive.sms** et copiez-le dans le dossier racine du lecteur avant la création de la bibliothèque de contenu.
- Une fois la bibliothèque de contenu créée, utilisez l'**outil Content Library Transfer** de la boîte à outils System Center 2012 R2 Configuration Manager pour gérer l'emplacement de la bibliothèque de contenu. Vous pouvez télécharger les outils depuis le Centre de téléchargement Microsoft.

# Outil de nettoyage de la bibliothèque de contenu pour System Center Configuration Manager

22/06/2018 • 9 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

À partir de la version 1702, vous pouvez utiliser un outil en ligne de commande (**ContentLibraryCleanup.exe**) pour supprimer le contenu qui n'est plus associé à un package ni une application à partir d'un point de distribution (contenu orphelin). Cet outil , nommé outil de nettoyage de la bibliothèque de contenu, remplace les anciennes versions des outils similaires distribuées pour les anciens produits Configuration Manager.

L'outil affecte uniquement le contenu du point de distribution spécifié à l'exécution de l'outil. L'outil ne peut pas supprimer le contenu de la bibliothèque de contenu sur le serveur de site.

Vous trouverez **ContentLibraryCleanup.exe** dans le dossier *%CM_Installation_Path%\cd.latest\SMSSETUP\TOOLS\ContentLibraryCleanup* sur le serveur du site d'administration centrale ou du site principal.*

## spécifications

L'outil ne peut s'exécuter que sur un seul point de distribution à la fois.

- Il peut s'exécuter directement sur l'ordinateur qui héberge le point de distribution à nettoyer, ou à distance à partir d'un autre serveur.
- Le compte d'utilisateur qui exécute l'outil doit avoir directement des autorisations d'administration basée sur des rôles qui correspondent à un administrateur complet dans la hiérarchie Configuration Manager. L'outil ne fonctionne pas quand le compte reçoit ces autorisations comme membre d'un groupe de sécurité Windows qui dispose des autorisations d'administrateur complet.

## Modes opératoires

Vous pouvez exécuter l'outil dans les deux modes suivants. Nous vous recommandons d'exécuter l'outil en mode *Simulation* afin de pouvoir consulter les résultats avant d'exécuter l'outil en *mode Suppression* :

1. **Mode de simulation** :
   Si vous ne spécifiez pas le commutateur **/delete**, l'outil s'exécute en mode de simulation et identifie le contenu qui serait supprimé à partir du point de distribution.
   - Dans ce mode, l'outil ne supprime aucune donnée.
   - Les informations sur le contenu qui serait supprimé sont écrites dans le fichier journal de l'outil, et vous n'êtes pas invité à confirmer chaque suppression potentielle.
2. **Mode Suppression** :
   Quand vous exécutez l'outil avec le commutateur **/delete**, l'outil s'exécute en mode de suppression.
   - Dans ce mode, le contenu orphelin qui se trouve sur le point de distribution spécifié peut être supprimé de la bibliothèque de contenu du point de distribution.
   - Avant de supprimer chaque fichier, vous devez confirmer que le fichier doit être supprimé. Vous pouvez sélectionner **Y** pour oui, **N** pour non, ou **Oui pour tout** pour ignorer les autres invites et supprimer tout le contenu orphelin.

Quand l'outil s'exécute dans l'un de ces modes, il crée automatiquement un journal avec un nom qui inclut le mode

d'exécution de l'outil, le nom du point de distribution et la date et l'heure de l'opération. Le fichier journal s'ouvre automatiquement quand l'exécution de l'outil est terminée.

Par défaut, le fichier journal est écrit dans le dossier temporaire du compte d'utilisateur qui exécute l'outil, sur le même ordinateur. Vous pouvez utiliser le commutateur **/log** pour rediriger le fichier journal vers un autre emplacement, y compris un partage réseau.

## Exécution de l'outil

Pour exécuter l'outil :

1. Ouvrez une invite de commandes d'administration dans un dossier qui contient **ContentLibraryCleanup.exe**.
2. Entrez ensuite une ligne de commande qui inclut les commutateurs de ligne de commande obligatoires ainsi que les commutateurs facultatifs que vous souhaitez utiliser.

**Problème connu** : lorsque l'outil s'exécute, une erreur de ce type peut être renvoyée si un package ou un déploiement, quel qu'il soit, a échoué ou est en cours :

- *System.InvalidOperationException: This content library cannot be cleaned up right now because package is not fully installed.*

**Solution de contournement :** aucune. L'outil ne peut pas identifier de façon fiable les fichiers orphelins lorsque du contenu est en cours de déploiement ou n'a pas pu être déployé. Par conséquent, l'outil ne vous autorisera pas à nettoyer le contenu tant que ce problème ne sera pas résolu.

**Commutateurs de ligne de commande**

Les commutateurs de ligne de commande suivants peuvent être utilisés dans n'importe quel ordre.

| COMMUTATEUR | DÉTAILS |
|---|---|
| **/delete** | **Facultatif**<br>Utilisez ce commutateur quand vous souhaitez supprimer le contenu à partir du point de distribution. Vous êtes invité à confirmer que le contenu doit être supprimé.<br><br>Quand ce commutateur n'est pas utilisé, l'outil enregistre les résultats sur le contenu qui serait supprimé, mais ne supprime pas de contenu du point de distribution.<br><br>Exemple : ***ContentLibraryCleanup.exe /dp server1.contoso.com /delete*** |
| **/q** | **Facultatif**<br>Ce commutateur exécute l'outil dans un mode silencieux qui supprime toutes les invites (telles que les invites pour supprimer du contenu), et n'ouvre pas automatiquement le fichier journal.<br><br>Exemple : ***ContentLibraryCleanup.exe /q /dp server1.contoso.com*** |
| **/dp <nom de domaine complet du point de distribution>** | **Obligatoire**<br>Spécifiez le nom de domaine complet du point de distribution que vous souhaitez nettoyer.<br><br>Exemple : ***ContentLibraryCleanup.exe /dp server1.contoso.com*** |

| COMMUTATEUR | DÉTAILS |
| --- | --- |
| **/ps <nom de domaine complet du site principal>** | **Facultatif** lors du nettoyage du contenu à partir d'un point de distribution sur un site principal.<br>**Obligatoire** lors du nettoyage du contenu à partir d'un point de distribution sur un site secondaire.<br><br>L'outil se connecte au site parent principal pour exécuter des requêtes sur SMS_Provider. Ces requêtes permettent à l'outil de déterminer le contenu qui doit être sur le point de distribution, afin de pouvoir identifier le contenu qui est orphelin et peut être supprimé. Cette connexion au site parent principal doit être établie pour les points de distribution sur un site secondaire, car les détails nécessaires ne sont pas accessibles directement à partir du site secondaire.<br><br>Spécifiez le nom de domaine complet du site principal auquel le point de distribution appartient, ou du site principal parent quand le point de distribution est sur un site secondaire.<br><br>Exemple : ***ContentLibraryCleanup.exe /dp server1.contoso.com /ps siteserver1.contoso.com*** |
| **/sc <code du site principal>** | **Facultatif** lors du nettoyage du contenu à partir d'un point de distribution sur un site principal.<br>**Obligatoire** lors du nettoyage du contenu à partir d'un point de distribution sur un site secondaire.<br><br>Spécifiez le code du site principal auquel le point de distribution appartient, ou du site principal parent quand le point de distribution est sur un site secondaire.<br><br>Exemple : ***ContentLibraryCleanup.exe /dp server1.contoso.com /sc ABC*** |
| **/log** | **Facultatif**<br>Spécifiez l'emplacement d'écriture du fichier journal par l'outil. Il peut s'agir d'un lecteur local ou d'un emplacement sur un partage réseau.<br><br>Lorsque ce commutateur n'est pas utilisé, le fichier journal est placé dans le dossier temporaire de l'utilisateur, sur l'ordinateur où s'exécute l'outil.<br><br>Exemple de lecteur local : ***ContentLibraryCleanup.exe /dp server1.contoso.com /log C:\Users\Administrator\Desktop***<br><br>Exemple de partage réseau : ***ContentLibraryCleanup.exe /dp server1.contoso.com /log \<partage><dossier>*** |

# Gérer les comptes pour accéder au contenu dans System Center Configuration Manager

22/06/2018 • 12 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Avant de déployer du contenu dans System Center Configuration Manager, déterminez de quelle façon les clients accèderont à ce contenu à partir des points de distribution. Cet article décrit les comptes suivants utilisés à cette fin :

- **Compte d'accès réseau**. Utilisé par les clients pour se connecter à un point de distribution et accéder au contenu. Par défaut, les clients essaient d'abord d'utiliser leur compte d'ordinateur.

  Ce compte est également utilisé par les points de distribution d'extraction pour obtenir le contenu d'un point de distribution source dans une forêt distante.

- **Compte d'accès au package**. Par défaut, Configuration Manager octroie aux comptes intégrés appelés **Utilisateurs** et **Administrateurs** l'accès au contenu d'un point de distribution. Vous pouvez configurer des autorisations supplémentaires pour limiter l'accès.

- **Compte de connexion multidiffusion**. Utilisé pour les déploiements de système d'exploitation.

## Compte d'accès réseau

Les ordinateurs clients utilisent le compte d'accès réseau quand ils ne peuvent pas utiliser leur compte d'ordinateur local pour accéder au contenu sur les points de distribution. Par exemple, cela s'applique aux clients du groupe de travail et aux ordinateurs de domaines non approuvés. Ce compte peut également être utilisé pendant le déploiement du système d'exploitation si l'ordinateur qui installe le système d'exploitation ne possède pas encore de compte d'ordinateur sur le domaine.

- Les clients utilisent le compte d'accès réseau uniquement pour accéder aux ressources du réseau.

- Sur chaque site principal, vous pouvez configurer plusieurs comptes à utiliser comme compte d'accès réseau.

- Les clients tentent d'abord d'accéder au contenu sur un point de distribution à l'aide de leur compte *nom_ordinateur*$. Si l'accès avec ce compte n'est pas possible, ils tentent alors d'utiliser un compte d'accès réseau. Les clients continuent d'essayer d'utiliser le compte d'accès réseau, même en cas d'échec antérieur.

**Autorisations**

Accordez les autorisations minimales appropriées à ce compte, pour qu'il puisse accéder au logiciel pour le contenu que nécessite le client.

- Le compte doit avoir le droit **Accéder à cet ordinateur à partir du réseau** sur le point de distribution.

- Créez le compte dans n'importe quel domaine fournissant l'accès nécessaire aux ressources. Le compte d'accès réseau doit toujours inclure un nom de domaine. La sécurité directe n'est pas prise en charge pour ce compte. Si vous disposez de points de distribution dans plusieurs domaines, créez le compte dans un domaine approuvé.

**TIP**

Pour éviter les verrouillages de compte, ne modifiez pas le mot de passe d'un compte d'accès réseau existant. Au lieu de cela, créez un compte et configurez le nouveau compte dans Configuration Manager. Après un délai suffisant pendant lequel tous les clients ont reçu les informations du nouveau compte, supprimez l'ancien compte des dossiers partagés du réseau et supprimez le compte.

**IMPORTANT**

N'accordez pas à ce compte des autorisations d'ouverture de session interactive.

N'accordez pas à ce compte le droit de joindre les ordinateurs au domaine. Si vous devez joindre les ordinateurs au domaine au cours d'une séquence de tâches, utilisez le compte de jonction de domaine de l'Éditeur de séquence de tâches.

**Pour configurer le compte d'accès réseau**

1. Dans la console Configuration Manager, choisissez **Administration** > **Configuration du site** > **Sites**, puis sélectionnez le site.
2. Dans le groupe **Paramètres**, choisissez **Configurer les composants de site** > **Distribution de logiciels**.
3. Choisissez l'onglet **Compte d'accès réseau**. Configurez un ou plusieurs comptes, puis choisissez **OK**.

## Comptes d'accès aux packages

Les comptes d'accès au package vous permettent de définir des autorisations NTFS pour spécifier les utilisateurs et les groupes d'utilisateurs qui peuvent accéder à un contenu de package sur des points de distribution. Par défaut, Configuration Manager n'accorde cet accès qu'aux comptes génériques **Utilisateurs** et **Administrateurs**. Vous pouvez cependant contrôler l'accès pour les ordinateurs clients à l'aide d'autres comptes ou groupes Windows. Les appareils mobiles n'utilisent pas les comptes d'accès au package, car ces appareils récupèrent toujours le contenu du package de façon anonyme.

Par défaut, quand Configuration Manager copie les fichiers de contenu d'un package sur un point de distribution, il accorde un accès en **Lecture** au groupe **Utilisateurs** local et un **Contrôle intégral** au groupe **Administrateurs** local. Les autorisations requises dépendent du package. Si vous avez des clients dans des groupes de travail ou dans des forêts non approuvées, ceux-ci utiliseront le compte d'accès réseau pour accéder au contenu du package. Assurez-vous que le compte d'accès réseau bénéficie d'autorisations sur le package à l'aide des comptes d'accès au package définis.

Utilisez des comptes dans un domaine susceptible d'accéder aux points de distribution. Si vous créez ou modifiez le compte une fois le package créé, vous devez redistribuer le package. La mise à jour du package ne modifie pas les autorisations de système de fichiers NTFS sur le package.

Il est inutile d'ajouter le compte d'accès réseau comme un compte d'accès au package, car l'appartenance au groupe **Utilisateurs** l'ajoute automatiquement. Le fait de restreindre le compte d'accès au package au compte d'accès réseau uniquement n'empêche pas les clients d'accéder au package.

**Pour gérer les comptes d'accès**

1. Dans la console Configuration Manager, choisissez **Bibliothèque de logiciels**.
2. Dans l'espace de travail **Bibliothèque de logiciels**, déterminez le type de contenu dont vous souhaitez gérer les comptes d'accès et suivez les étapes indiquées :
   - **Applications** : développez **Gestion d'applications**, choisissez **Applications**, puis sélectionnez les applications dont vous souhaitez gérer les comptes d'accès.

- **Packages** : développez **Gestion d'applications**, choisissez **Packages**, puis sélectionnez les packages dont vous souhaitez gérer les comptes d'accès.
- **Packages de déploiement** : développez **Mises à jour logicielles**, choisissez **Packages de déploiement**, puis sélectionnez les packages de déploiement dont vous souhaitez gérer les comptes d'accès.
- **Packages de pilotes** : développez **Systèmes d'exploitation**, choisissez **Packages de pilotes**, puis sélectionnez les packages de pilotes dont vous souhaitez gérer les comptes d'accès.
- **Images du système d'exploitation** : développez **Systèmes d'exploitation**, choisissez **Images du système d'exploitation**, puis sélectionnez les images du système d'exploitation dont vous souhaitez gérer les comptes d'accès.
- **Programmes d'installation de système d'exploitation** : développez **Systèmes d'exploitation**, choisissez **Programmes d'installation de système d'exploitation**, puis sélectionnez les programmes d'installation de système d'exploitation dont vous souhaitez gérer les comptes d'accès.
- **Images de démarrage** : développez **Systèmes d'exploitation**, choisissez **Images de démarrage**, puis sélectionnez les images de démarrage dont vous souhaitez gérer les comptes d'accès.

3. Cliquez avec le bouton droit sur l'objet sélectionné, puis choisissez **Gérer des comptes d'accès**.
4. Dans la boîte de dialogue **Ajouter un compte**, spécifiez le type du compte auquel les droits d'accès au contenu seront accordés, puis indiquez les droits d'accès associés au compte.

> **NOTE**
> Quand vous ajoutez un nom d'utilisateur au compte et que Configuration Manager trouve un compte d'utilisateur local et un compte d'utilisateur de domaine portant ce nom, Configuration Manager définit les droits d'accès du compte d'utilisateur de domaine.

## Compte de connexion multidiffusion

Le compte de connexion multidiffusion est utilisé par des points de distribution qui sont configurés pour la multidiffusion pour lire les informations de la base de données de site.

- Vous spécifiez un compte à utiliser quand vous configurez des connexions de base de données Configuration Manager pour la multidiffusion.
- Le compte d'ordinateur du point de distribution est utilisé par défaut, mais vous pouvez configurer un compte d'utilisateur à la place.
- Chaque fois que la base de données de site est dans une forêt non approuvée, vous devez spécifier un compte d'utilisateur.
- Le compte doit avoir des autorisations **d'accès en lecture** à la base de données de site.

Par exemple, si votre centre de données dispose d'un réseau de périmètre dans une forêt autre que celle du serveur de site et de la base de données du site, vous pouvez utiliser ce compte pour lire les informations sur la multidiffusion à partir de la base de données du site.

Si vous créez ce compte, créez-le en tant que compte local doté de droits limités sur l'ordinateur qui exécute Microsoft SQL Server.

**IMPORTANT**

N'accordez pas à ce compte des autorisations d'ouverture de session interactive.

# Cache d'homologue pour les clients Configuration Manager

22/06/2018 • 13 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez le **cache d'homologue** pour gérer le déploiement de contenu sur les clients distants. Le cache d'homologue est une solution Configuration Manager intégrée qui permet aux clients de partager du contenu avec d'autres clients directement à partir de leur cache local.

> **TIP**
> Cette fonctionnalité a été introduite dans la version 1610 en tant que fonctionnalité en préversion. À compter de la version 1710, cette fonctionnalité n'est plus une fonctionnalité en préversion.

> **NOTE**
> Par défaut, Configuration Manager n'active pas cette fonctionnalité facultative. Vous devez activer cette fonctionnalité avant de l'utiliser. Pour plus d'informations, consultez Activer les fonctionnalités facultatives des mises à jour.

## Vue d'ensemble

Un client de cache d'homologue est un client Configuration Manager qui est activé pour utiliser le cache d'homologue. Un client de cache d'homologue qui a du contenu qu'il peut partager avec d'autres clients est une source de cache d'homologue.

- Vous utilisez des paramètres du client pour permettre aux clients d'utiliser le cache d'homologue.
- Pour partager du contenu en tant que source de cache d'homologue, un client de cache d'homologue :
  - Les appareils doivent être joints à un domaine. Toutefois, un client qui n'est pas joint à un domaine peut obtenir du contenu à partir d'une source de cache d'homologue jointe à un domaine.
  - Il doit être un membre du groupe de limites actuel du client qui recherche le contenu. Quand un client utilise une action de secours pour rechercher du contenu dans un groupe de limites voisin, la liste des emplacements sources de contenu n'inclut pas un client de cache d'homologue dans un groupe de limites voisin. Pour plus d'informations sur les groupes de limites actuels et voisins, consultez Groupes de limites.
- Le client Configuration Manager délivre chaque type de contenu dans le cache à d'autres clients en utilisant le cache d'homologue. Ce contenu comprend des fichiers Office 365 et représente des fichiers d'installation.
- Le cache d'homologue ne remplace pas l'utilisation d'autres solutions, comme BranchCache. Le cache d'homologue fonctionne avec d'autres solutions pour vous donner plus d'options permettant d'étendre les solutions traditionnelles de déploiement de contenu, comme les points de distribution. Le cache d'homologue est une solution personnalisée qui ne dépend pas de BranchCache. Si vous n'activez pas ou n'utilisez pas Windows BranchCache, le cache d'homologue fonctionne quand même.

### Opérations

Pour activer le cache d'homologue, déployez les paramètres client sur un regroupement. Les membres de ce regroupement se comportent ensuite comme une source de contenu d'homologue pour d'autres clients du même groupe de limites.

- Un client qui agit en tant que source de contenu homologue envoie une liste des contenus mis en cache disponibles à son point de gestion.
- Quand le client suivant de ce groupe de limites demande ce contenu, chaque source du cache d'homologue qui a ce contenu et qui est en ligne est retournée dans la liste des sources potentielles de contenu. Cette liste inclut également les points de distribution et d'autres emplacements de source de contenu dans ce groupe de limites.
- Dans le processus normal, le client qui demande le contenu sélectionne une source dans la liste fournie. Le client essaie ensuite d'obtenir le contenu.

> **NOTE**
> Si le client a recours à un groupe de limites voisin pour le contenu, il n'ajoute pas les emplacements sources de contenu du cache d'homologue du groupe de limites voisin à la liste des emplacements de sources de contenu potentiels.

La bonne pratique consiste à choisir uniquement les clients les plus appropriés comme sources de cache d'homologue. Évaluez l'adéquation des clients en fonction d'attributs comme le type de châssis, l'espace disque et la connectivité réseau. Pour plus d'informations vous permettant de sélectionner les meilleurs clients à utiliser pour le cache d'homologue, consultez ce blog rédigé par un consultant Microsoft.

**Accès limité à une source de cache d'homologue**
À compter de la version 1702, un ordinateur source de cache d'homologue rejette les demandes de contenu quand il remplit une des conditions suivantes :

- Il est en mode de batterie faible.
- La charge de l'UC dépasse 80 % au moment où le contenu est demandé.
- Les E/S disque ont une valeur *AvgDiskQueueLength* supérieure à 10.
- Il n'y a plus de connexion disponible vers l'ordinateur.

Configurez ces paramètres à l'aide de la classe WMI du serveur de configuration du client pour la fonctionnalité de source d'homologue (*SMS_WinPEPeerCacheConfig*) dans le SDK System Center.

Quand l'ordinateur rejette une demande de contenu, l'ordinateur demandeur continue à rechercher le contenu dans la liste des emplacements de sources de contenu disponibles.

**Analyse**
Pour vous aider à comprendre l'utilisation du cache d'homologue, vous pouvez afficher le tableau de bord Sources de données du client. Consultez la section relative au tableau de bord Sources de données du client.

À partir de la version 1702, vous pouvez utiliser trois rapports pour afficher l'utilisation du cache d'homologue. Dans la console, accédez à **Surveillance** > **Comptes rendus** > **Rapports**. Tous les rapports ont le type **Contenu de distribution de logiciels** :

1. **Rejet du contenu de la source de cache d'homologue** :
   Utilisez ce rapport pour comprendre la fréquence à laquelle les sources de cache d'homologue d'un groupe de limites rejettent une demande de contenu.
   - **Problème connu :** lorsque vous descendez dans la hiérarchie pour accéder à des résultats comme *MaxCPULoad* ou *MaxDiskIO*, il se peut que vous receviez une erreur qui indique que le rapport ou les détails sont introuvables. Pour contourner ce problème, utilisez les deux rapports suivants, qui montrent directement les résultats.
2. **Rejet conditionnel du contenu de la source de cache d'homologue** :
   Utilisez ce rapport pour comprendre les détails du rejet pour un groupe de limites ou un type de rejet donné. Vous pouvez spécifier :
   - **Problème connu :** vous ne pouvez pas choisir parmi une liste de paramètres disponibles ; vous devez les entrer manuellement. Entrez les valeurs *Nom de groupe de limites* et *Type de rejet* comme dans le

premier rapport. Par exemple, pour *Type de rejet*, vous pouvez entrer *MaxCPULoad* ou *MaxDiskIO*.

3. **Détails du rejet du contenu de la source de cache d'homologue** :
   Utilisez ce rapport pour comprendre quel était le contenu demandé par le client au moment du rejet.

   - **Problème connu :** vous ne pouvez pas choisir parmi une liste de paramètres disponibles ; vous devez les entrer manuellement. Entrez la valeur pour *Type de rejet* telle qu'elle apparaît dans le rapport **Rejet du contenu par une source de cache d'homologue**. Entrez ensuite *l'ID de ressource* pour la source de contenu sur laquelle vous voulez plus d'informations. Pour trouver l'ID de ressource de la source de contenu :

     a. Recherchez le nom de l'ordinateur qui s'affiche comme *Source de cache d'homologue* dans les résultats du rapport **Rejet conditionnel du contenu de la source de cache d'homologue**.
     b. Ensuite, accédez à **Biens et conformité** > **Appareils**, puis recherchez ce nom d'ordinateur. Utilisez la valeur de la colonne ID de ressource.

## Exigences et considérations relatives au cache d'homologue

- Le cache d'homologue est pris en charge sur tout système d'exploitation Windows pris en charge en tant que client Configuration Manager. Les systèmes d'exploitation autres que Windows ne sont pas pris en charge pour le cache d'homologue.

- Des clients ne peuvent transférer du contenu qu'à partir de clients de cache d'homologue qui se trouvent dans leur groupe de limites actuel.

- Avant la version 1706, chaque site où les clients utilisent le cache d'homologue doit être configuré avec un compte d'accès réseau. Depuis la version 1706, ce compte n'est plus nécessaire, sauf dans le cas suivant : un client autorisé à utiliser le cache d'homologue exécute une séquence de tâches depuis le Centre logiciel, et cette séquence de tâches redémarre à partir d'une image de démarrage. Dans ce scénario, le client nécessite toujours le compte d'accès réseau. Quand le client est sur Windows PE, il utilise le compte d'accès réseau pour obtenir du contenu de la source de cache d'homologue.

  Quand c'est nécessaire, le cache d'homologue utilise le compte d'accès réseau pour authentifier les demandes de téléchargement provenant de pairs. Pour cela, ce compte a seulement besoin des autorisations d'utilisateur de domaine.

- Le dernier envoi de l'inventaire matériel du client détermine la limite d'une source de contenu de cache d'homologue. Un client qui passe à un groupe de limites différent peut toujours être membre de son groupe de limites précédent pour les besoins liés au cache d'homologue. Ce comportement fait qu'un client peut se voir proposer une source de contenu de cache d'homologue qui ne se trouve pas à proximité de son emplacement réseau. Nous vous recommandons d'empêcher les clients qui adoptent souvent cette configuration de participer à une source de cache d'homologue.

- Depuis la version 1706, le client de cache homologue vérifie d'abord que la source de contenu du cache d'homologue est en ligne avant d'essayer de télécharger le contenu.

## Pour configurer les paramètres client du cache d'homologue du client

Pour plus d'informations sur la configuration des paramètres client, consultez Paramètres du cache des clients. Pour plus d'informations, consultez Guide pratique pour configurer les paramètres client.

Sur les clients autorisés à utiliser le cache d'homologue qui utilisent le pare-feu Windows, Configuration Manager configure les ports du pare-feu que vous spécifiez dans les paramètres des clients.

# Package Transfer Manager dans System Center Configuration Manager

22/06/2018 • 12 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Dans un site System Center Configuration Manager, Package Transfer Manager est un composant du service SMS_Executive qui gère le transfert de contenu d'un ordinateur serveur de site sur les points de distribution distants d'un site. (Un point de distribution est dit distant s'il ne se trouve pas sur l'ordinateur serveur de site.) Le composant Package Transfer Manager ne prend pas en charge les configurations effectuées par l'administrateur, mais le fait de comprendre comment il fonctionne peut vous aider à planifier votre infrastructure de gestion de contenu. Il peut également vous aider à résoudre les problèmes de distribution de contenu.

Quand vous distribuez du contenu à un ou plusieurs points de distribution distants sur un site, le **gestionnaire de distribution** crée une tâche de transfert de contenu. Il indique ensuite à Package Transfer Manager sur les serveurs de site principal et secondaire de transférer le contenu sur les points de distribution distants.

Package Transfer Manager consigne ses actions dans le fichier **pkgxfermgr.log** sur le serveur de site. Le fichier journal est le seul emplacement où vous pouvez voir les activités du Package Transfer Manager.

> **NOTE**
> Dans les versions précédentes de Configuration Manager, le gestionnaire de distribution gère le transfert de contenu à destination d'un point de distribution distant. Le gestionnaire de distribution gère également le transfert de contenu entre sites. Avec System Center Configuration Manager, le gestionnaire de distribution continue de gérer le transfert de contenu entre deux sites. Cependant, Package Transfer Manager gère désormais le transfert de contenu sur un grand nombre de points de distribution. Cela permet d'améliorer les performances générales de déploiement de contenu à la fois entre les sites et sur les points de distribution au sein d'un site.

Pour transférer du contenu vers un point de distribution standard, Package Transfer Manager fonctionne de la même façon que le gestionnaire de distribution des versions précédentes de Configuration Manager. En d'autres termes, il gère activement le transfert de fichiers pour chaque point de distribution distant. Cependant, pour distribuer du contenu sur un point de distribution d'extraction, Package Transfer Manager indique au point de distribution d'extraction que du contenu est disponible. Le point de distribution d'extraction se charge ensuite du processus de transfert.

Les informations suivantes expliquent comment Package Transfer Manager gère le transfert de contenu sur les points de distribution standard et les points de distribution configurés comme points de distribution d'extraction :

1. **L'administrateur déploie le contenu sur un ou plusieurs points de distribution sur un site.**
   - **Point de distribution standard** : le gestionnaire de distribution crée un travail de transfert de contenu pour ce contenu.
   - **Point de distribution d'extraction** : le gestionnaire de distribution crée un travail de transfert de contenu pour ce contenu.
2. **Le gestionnaire de distribution exécute des vérifications préliminaires.**
   - **Point de distribution standard** : le gestionnaire de distribution exécute une vérification de base pour s'assurer que chaque point de distribution est prêt à recevoir le contenu. Après cette vérification, le gestionnaire de distribution instruit Package Transfer Manager de démarrer le

transfert de contenu vers le point de distribution.

- **Point de distribution d'extraction** : le gestionnaire de distribution démarre Package Transfer Manager, qui informe le point de distribution d'extraction qu'il existe un nouveau travail de transfert de contenu. Le gestionnaire de distribution ne vérifie pas l'état des points de distribution distants qui sont des points de distribution d'extraction, car chaque point de distribution d'extraction gère ses propres transferts de contenu.

3. **Package Transfer Manager prépare le transfert du contenu.**

   - **Point de distribution standard** : Package Transfer Manager examine le magasin de contenu à instance unique de chaque point de distribution distant spécifié. Cette opération a pour but d'identifier les fichiers qui se trouvent déjà sur ce point de distribution. Ensuite, Package Transfer Manager met en file d'attente le transfert uniquement des fichiers qui ne sont pas déjà présents.

     > **NOTE**
     > Pour copier chaque fichier dans la distribution sur le point de distribution, même si les fichiers sont déjà présents dans le magasin d'instances uniques du point de distribution, utilisez l'action **Redistribuer** pour le contenu.

   - **Point de distribution d'extraction** : pour chaque point de distribution d'extraction de la distribution, Package Transfer Manager vérifie les points de distribution source des points de distribution d'extraction pour confirmer que le contenu est disponible.

     - Quand le contenu est disponible sur au moins un point de distribution source, Package Transfer Manager envoie une notification à ce point de distribution d'extraction. La notification indique à ce point de distribution de commencer le processus de transfert de contenu. La notification inclut les noms de fichiers et les tailles, les attributs et les valeurs de hachage.
     - Lorsque le contenu n'est pas encore disponible, Package Transfer Manager n'envoie pas de notification au point de distribution. Il répète la vérification toutes les 20 minutes jusqu'à ce que le contenu soit disponible. Puis, lorsque le contenu est disponible, Package Transfer Manager envoie la notification à ce point de distribution d'extraction.

     > **NOTE**
     > Pour que le point de distribution d'extraction copie chaque fichier dans la distribution sur le point de distribution, même si les fichiers sont déjà présents dans le magasin d'instances uniques du point de distribution d'extraction, utilisez l'action **Redistribuer** pour le contenu.

4. **Le transfert du contenu commence.**

   - **Point de distribution standard** : Package Transfer Manager copie les fichiers sur chaque point de distribution distant. Lors du transfert vers un point de distribution standard :

     - Par défaut, Package Transfer Manager peut traiter simultanément trois packages uniques et les distribuer à cinq points de distribution en parallèle. Ceux-ci sont collectivement appelés « **paramètres de distribution simultanée** ». Pour configurer la distribution simultanée, dans les **Propriétés du composant de distribution de logiciels** de chaque site, accédez à l'onglet **Général**.
     - Package Transfer Manager utilise les configurations de la bande passante réseau et de la planification de chaque point de distribution lors du transfert de contenu vers ce point de distribution. Pour configurer ces paramètres, dans les **Propriétés** de chaque point de distribution distant, accédez aux onglets **Planification** et **Limites du taux de transfert**. Pour

plus d'informations, consultez Gérer le contenu et l'infrastructure de contenu pour System Center Configuration Manager.

- **Point de distribution d'extraction** : quand un point de distribution d'extraction reçoit un fichier de notification, le point de distribution commence le processus de transfert du contenu. Le processus de transfert s'exécute indépendamment sur chaque point de distribution d'extraction :

  a. La distribution d'extraction identifie les fichiers dans la distribution de contenu qui ne se trouvent pas déjà dans son magasin d'instances uniques et prépare le téléchargement de ce contenu depuis un de ses points de distribution source.

  b. Ensuite, le point de distribution d'extraction vérifie chacun de ses points de distribution source, dans l'ordre, jusqu'à ce qu'il trouve un point de distribution source disposant du contenu. Lorsque le point de distribution d'extraction identifie un point de distribution source avec le contenu, il commence le téléchargement de ce contenu.

  > **NOTE**
  > Le processus de téléchargement de contenu du point de distribution d'extraction est le même que celui des clients Configuration Manager. Pour le transfert de contenu par le point de distribution d'extraction, les paramètres de transfert simultané ne sont pas utilisés. Les options de planification et de limitation de bande passante que vous configurez pour les points de distribution standard ne sont pas non plus utilisées.

5. **Fin du transfert de contenu.**

   - **Point de distribution standard** : une fois que Package Transfer Manager a terminé le transfert de fichiers sur chaque point de distribution distant désigné, il vérifie le hachage du contenu sur le point de distribution. Puis il informe le gestionnaire de distribution que la distribution est terminée.
   - **Point de distribution d'extraction** : une fois que le point de distribution d'extraction a terminé le téléchargement du contenu, le point de distribution vérifie le hachage du contenu. Puis il envoie un message d'état au point de gestion des sites pour indiquer que l'opération a abouti. Si cet état n'est pas reçu après 60 minutes, Package Transfer Manager ressort du mode veille. Il consulte le point de distribution d'extraction pour déterminer s'il a téléchargé le contenu. Si le téléchargement du contenu est en cours, Package Transfer Manager se remet en veille pendant 60 minutes avant de reconsulter le point de distribution d'extraction. Ce cycle se répète jusqu'à ce que le point de distribution d'extraction termine le transfert du contenu.

# Gérer la bande passante réseau pour le contenu

22/06/2018 • 12 minutes to read • Edit Online

Pour mieux gérer la bande passante réseau utilisée pour le processus de gestion du contenu de System Center Configuration Manager, vous pouvez utiliser les commandes Configuration Manager intégrées de planification et de limitation de bande passante. Vous pouvez également utiliser le contenu préparé. Les sections suivantes décrivent ces options plus en détail.

## Planification et limitation de bande passante

Lorsque vous créez un package, modifiez le chemin source du contenu ou mettez à jour le contenu sur le point de distribution, les fichiers sont copiés depuis le chemin source vers la bibliothèque de contenu sur le serveur de site. Ensuite, le contenu est copié depuis la bibliothèque de contenu sur le serveur de site vers la bibliothèque de contenu sur les points de distribution. Si des fichiers sources de contenu sont mis à jour et que ces fichiers ont déjà été distribués, Configuration Manager récupère uniquement les fichiers nouveaux ou mis à jour, puis il les envoie au point de distribution.

Vous pouvez utiliser les commandes de planification et de limitation de bande passante pour la communication entre sites, ainsi que pour la communication entre un serveur de site et un point de distribution distant. Si vous constatez que la bande passante réseau est limitée même après avoir configuré les commandes de planification et de limitation de bande passante, vous pouvez envisager de préparer le contenu sur le point de distribution.

Dans Configuration Manager, vous pouvez configurer un calendrier et spécifier des paramètres de limitation de bande passante sur des points de distribution distants qui déterminent quand et comment s'effectue la distribution du contenu. Chaque point de distribution distant peut avoir différentes configurations qui permettent de répondre aux limitations de la bande passante réseau à partir du serveur de site pour le point de distribution distant. Les commandes de programmation et de limitation de bande passante sur le point de distribution sont similaires aux paramètres d'une adresse d'expéditeur standard. Dans ce cas, les paramètres sont utilisés par un nouveau composant appelé Package Transfer Manager.

Package Transfer Manager distribue le contenu à partir d'un serveur de site, site principal ou secondaire, vers un point de distribution qui est installé sur un système de site. Les paramètres de limitation de bande passante sont spécifiés sous l'onglet **Limites du taux de transfert**, et les paramètres de planification sont spécifiés sous l'onglet **Calendrier** pour un point de distribution qui ne se trouve pas sur un serveur de site. Les paramètres d'heure sont basés sur le fuseau horaire du site émetteur, et non sur le point de distribution.

> **IMPORTANT**
> Les onglets **Limites du taux de transfert** et **Calendrier** sont affichés uniquement dans les propriétés des points de distribution qui ne sont pas installés sur un serveur de site.

Pour plus d'informations, consultez Installer et configurer des points de distribution pour System Center Configuration Manager.

## Contenu préparé

Vous pouvez préparer du contenu pour ajouter les fichiers de contenu à la bibliothèque de contenu sur un serveur de site ou sur un point de distribution avant de distribuer le contenu. Comme les fichiers de contenu figurent déjà dans la bibliothèque de contenu, ils ne sont pas transférés sur le réseau quand vous distribuez le contenu. Vous pouvez préparer des fichiers de contenu pour les applications et les packages.

Dans la console Configuration Manager, sélectionnez le contenu à préparer, puis utilisez l'**Assistant Création du fichier de contenu préparé**. Cette opération crée un fichier de contenu compressé et préparé qui contient les fichiers et les métadonnées associées pour le contenu. Vous pouvez ensuite importer manuellement le contenu au niveau d'un serveur de site ou d'un point de distribution. Notez les points suivants :

- Lorsque vous importez le fichier de contenu préparé sur un serveur de site, les fichiers de contenu sont ajoutés à la bibliothèque de contenu sur le serveur de site, puis enregistrés dans la base de données du serveur de site.
- Quand vous importez le fichier de contenu préparé sur un point de distribution, les fichiers de contenu sont ajoutés à la bibliothèque de contenu sur le point de distribution. Un message d'état est envoyé au serveur de site pour indiquer au site que le contenu est disponible sur le point de distribution.

Vous pouvez éventuellement configurer le point de distribution comme **préparé** pour faciliter la gestion de la distribution de contenu. Ensuite, quand vous distribuez le contenu, choisissez l'option souhaitée :

- Toujours préparer le contenu sur le point de distribution.
- Préparer le contenu initial pour le package, puis utiliser le processus de distribution de contenu standard quand des mises à jour du contenu sont disponibles.
- Toujours utiliser le processus de distribution de contenu standard pour le contenu du package.

**Déterminer si vous devez préparer du contenu**

Envisagez de préparer du contenu pour les applications et les packages dans les cas suivants :

- **Pour résoudre le problème de bande passante réseau limitée entre le serveur de site et un point de distribution.** Si la planification et la limitation de bande passante ne suffisent pas à répondre à vos besoins en matière de bande passante, songez à préparer le contenu sur le point de distribution. Chaque point de distribution est associé au paramètre **Activer ce point de distribution pour le contenu préparé** que vous pouvez choisir dans les propriétés du point de distribution. Lorsque vous activez cette option, le point de distribution est identifié comme un point de distribution préparé et vous pouvez choisir comment gérer le contenu pour chaque package.

  Les paramètres suivants sont disponibles dans les propriétés relatives à une application, un package, un package de pilotes, une image de démarrage, un programme d'installation de système d'exploitation et une image. Ils vous permettent de choisir le mode de gestion de la distribution du contenu sur les points de distribution distants qui sont identifiés comme préparés :

  - **Télécharger automatiquement le contenu lorsque des packages sont affectés à des points de distribution** : utilisez cette option quand vous disposez de packages plus petits, et que les paramètres de planification et de limitation de bande passante offrent suffisamment de contrôle pour la distribution de contenu.
  - **Télécharger uniquement les modifications de contenu vers le point de distribution** : utilisez cette option si vous prévoyez que la taille des futures mises à jour du contenu du package sera normalement inférieure à celle du package initial. Par exemple, vous pouvez préparer une application telle que Microsoft Office, car la taille du package initial est supérieure à 700 Mo et trop volumineuse pour être envoyée sur le réseau. Toutefois, les mises à jour du contenu pour ce package peuvent être inférieures à 10 Mo et distribuables sur le réseau. Citons aussi l'exemple d'un package de pilotes : sa taille initiale peut être importante, mais les ajouts de pilotes incrémentiels au package peuvent être de petite taille.
  - **Copier manuellement le contenu de ce package vers le point de distribution** : utilisez cette option quand vous disposez de packages volumineux, avec du contenu tel qu'un système d'exploitation et n'utilisez jamais le réseau pour distribuer le contenu sur le point de distribution. Lorsque vous sélectionnez cette option, vous devez préparer le contenu sur le point de distribution.

> **IMPORTANT**
>
> Les options précédentes sont applicables pour chaque package et ne sont utilisées que si un point de distribution est identifié comme préparé. Les points de distribution qui n'ont pas été identifiés comme préparés ignorent ces paramètres. Dans ce cas, le contenu est toujours distribué via le réseau à partir du serveur de site vers les points de distribution.

- **Pour restaurer la bibliothèque de contenu sur un serveur de site.** lors de la défaillance d'un serveur de site, les informations sur les packages et applications inclus dans la bibliothèque de contenu sont restaurées vers la base de données de site dans le cadre du processus de restauration, mais les fichiers de la bibliothèque de contenu ne sont pas restaurés dans le cadre du processus. Si vous ne disposez pas d'une sauvegarde du système de fichiers pour restaurer la bibliothèque de contenu, vous pouvez créer un fichier de contenu préparé à partir d'un autre site contenant les packages et applications que vous devez avoir. Vous pouvez ensuite extraire le fichier de contenu préparé sur le serveur de site récupéré. Pour plus d'informations sur la sauvegarde et la récupération du serveur de site, consultez Sauvegarde et récupération pour System Center Configuration Manager.

# Sécurité et confidentialité pour la gestion du contenu dans System Center Configuration Manager

22/06/2018 • 13 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cette rubrique contient des informations de sécurité et de confidentialité pour la gestion du contenu dans System Center Configuration Manager. Lisez-le conjointement aux rubriques suivantes :

- Sécurité et confidentialité pour la gestion des applications dans System Center Configuration Manager
- Sécurité et confidentialité pour les mises à jour logicielles dans System Center Configuration Manager
- Sécurité et confidentialité du déploiement de systèmes d'exploitation dans System Center Configuration Manager

## Meilleures pratiques de sécurité pour la gestion de contenu

Utilisez les meilleures pratiques de sécurité suivantes pour la gestion de contenu :

**Pour les points de distribution sur l'intranet, prenez en considération les avantages et les inconvénients liés à l'utilisation de HTTP et de HTTPS** : dans la plupart des cas, l'utilisation du protocole HTTP et des comptes d'accès aux packages pour l'autorisation est plus sécurisée que l'utilisation du protocole HTTPS avec chiffrement mais sans autorisation. Toutefois, si des données sensibles se trouvent dans votre contenu que vous souhaitez chiffrer lors du transfert, utilisez le protocole HTTPS.

- **Quand vous utilisez HTTPS pour un point de distribution**, Configuration Manager n'utilise pas les comptes d'accès aux packages pour autoriser l'accès au contenu, mais le contenu est chiffré pendant son transfert sur le réseau.
- **Quand vous utilisez HTTP pour un point de distribution**, vous pouvez utiliser des comptes d'accès aux packages pour l'autorisation, mais le contenu n'est pas chiffré pendant son transfert sur le réseau.

**Si vous utilisez un certificat d'authentification de client PKI plutôt qu'un certificat auto-signé pour le point de distribution, protégez le fichier de certificat (.pfx) avec un mot de passe fort. Si vous stockez le fichier sur le réseau, sécurisez le canal de réseau quand vous importez le fichier dans Configuration Manager** : Quand vous avez besoin d'un mot de passe pour importer le certificat d'authentification du client permettant au point de distribution de communiquer avec les points de gestion, vous pouvez ainsi protéger le certificat contre les utilisateurs malveillants. Utilisez la signature SMB (Server Message Block) ou IPsec entre l'emplacement réseau et le serveur de site pour empêcher une personne malveillante de falsifier le fichier de certificat.

**Supprimez le rôle de point de distribution du serveur de site** : Par défaut, un point de distribution est installé sur le même serveur que le serveur de site. Les clients n'ont pas besoin de communiquer directement avec le serveur de site, ainsi, pour réduire la surface d'attaque, attribuez le rôle de point de distribution à d'autres systèmes de site et retirez-le du serveur de site.

**Sécurisez le contenu au niveau de l'accès aux packages** : Le partage de point de distribution permet un accès en lecture pour tous les utilisateurs. Pour restreindre les utilisateurs pouvant accéder au contenu, utilisez les comptes d'accès aux packages lorsque le point de distribution est configuré pour le protocole HTTP. Cette consigne ne s'applique pas aux points de distribution cloud, qui ne prennent pas en charge les comptes d'accès aux packages. Pour plus d'informations sur le compte d'accès aux packages, consultez Gérer les comptes pour accéder au

contenu.

**Si Configuration Manager installe IIS au moment où vous ajoutez un rôle de système de site de point de distribution, désactivez la redirection HTTP ou les scripts et outils de gestion IIS une fois l'installation du point de distribution terminée** : Le point de distribution n'a pas besoin de la redirection HTTP ni des scripts et outils de gestion IIS. Pour réduire la surface d'attaque, supprimez ces services de rôle pour le rôle de serveur Web (IIS). Pour plus d'informations sur les services de rôle pour le rôle de serveur web (IIS) pour les points de distribution, voir Prérequis des sites et systèmes de site.

**Définissez les autorisations d'accès au package au moment de la création du package** : Comme les modifications apportées aux comptes d'accès sur les fichiers de package ne sont mises en place qu'une fois le package redistribué, définissez les autorisations d'accès au package avec précaution quand vous créez le package pour la première fois. Cela est particulièrement important lorsque le package est volumineux ou distribués à de nombreux points de distribution, et lorsque la capacité de la bande passante réseau pour la distribution de contenu est limitée.

**Implémentez des contrôles d'accès pour protéger les supports qui contiennent le contenu préparé** : Le contenu préparé est compressé mais pas chiffré. Une personne malveillante pourrait alors lire et modifier les fichiers qui sont téléchargés vers des appareils. Les clients Configuration Manager rejettent le contenu qui a été falsifié, mais ils le téléchargent malgré tout.

**Importez le contenu préparé en utilisant uniquement l'outil en ligne de commande ExtractContent (ExtractContent.exe) qui est fourni avec Configuration Manager, et vérifiez qu'il est signé par Microsoft** : Pour éviter toute falsification et une élévation de privilèges, utilisez uniquement l'outil en ligne de commande autorisé fourni avec Configuration Manager.

**Sécurisez le canal de communication entre le serveur de site et l'emplacement source du package** : Utilisez une signature SMB ou IPsec entre le serveur de site et l'emplacement source du package quand vous créez des applications et des packages. Cela permet d'empêcher un individu mal intentionné de falsifier les fichiers sources.

**Si vous modifiez l'option de configuration du site pour utiliser un site web personnalisé plutôt que le site web par défaut après l'installation de rôles de point de distribution, supprimez les répertoires virtuels par défaut** : Quand vous passez du site web par défaut à un site web personnalisé, Configuration Manager ne supprime pas les anciens répertoires virtuels. Supprimez les répertoires virtuels que Configuration Manager a créés initialement sous le site web par défaut :

- SMS_DP_SMSPKG$
- SMS_DP_SMSSIG$
- NOCERT_SMS_DP_SMSPKG$
- NOCERT_SMS_DP_SMSSIG$

**Pour les points de distribution cloud, protégez vos informations d'abonnement et vos certificats** : Quand vous utilisez des points de distribution cloud, protégez les éléments importants, notamment le nom d'utilisateur et le mot de passe de votre abonnement Azure, le certificat de gestion Azure et le certificat de service de point de distribution cloud. Stockez les certificats en lieu sûr. Si vous y accédez via le réseau lors de la configuration du point de distribution cloud, utilisez une authentification IPsec ou SMB entre le serveur de système de site et l'emplacement source.

**Pour assurer la continuité de service des points de distribution cloud, surveillez la date d'expiration des certificats** : Configuration Manager ne vous avertit pas quand les certificats importés pour la gestion des services de point de distribution cloud sont sur le point d'expirer. Vous devez donc surveiller les dates d'expiration indépendamment de Configuration Manager et penser à renouveler, puis à importer les nouveaux certificats avant la date d'expiration. Cette opération est particulièrement importante si vous faites l'acquisition d'un certificat de

service de point de distribution cloud Configuration Manager auprès d'une autorité de certification externe, car l'obtention d'un certificat renouvelé peut prendre plus de temps.

En cas d'expiration d'un certificat, le gestionnaire de services cloud génère l'ID de message d'état **9425**. Une entrée contenant la date d'expiration exprimée au format UTC est alors ajoutée au fichier CloudMgr.log pour indiquer que le certificat **a expiré**.

## Considérations de sécurité pour la gestion de contenu

Tenez compte des points suivants au moment de planifier la gestion de contenu :

- Les clients ne valident pas le contenu jusqu'au téléchargement de celui-ci.

  Les clients Configuration Manager ne valident le hachage du contenu qu'après le téléchargement de celui-ci dans leur cache client. Si un individu mal intentionné falsifie la liste des fichiers à télécharger ou le contenu lui-même, le processus de téléchargement peut consommer une quantité importante de bande passante réseau pour que le client supprime ensuite le contenu quand il rencontre le hachage non valide.

- Quand vous utilisez des points de distribution cloud, l'accès au contenu est automatiquement limité à votre entreprise, et vous ne pouvez pas le limiter de façon plus précise en sélectionnant des utilisateurs ou des groupes.

- Quand vous utilisez des points de distribution cloud, les clients sont authentifiés par le point de gestion, puis ils utilisent un jeton Configuration Manager pour accéder aux points de distribution cloud. Le jeton reste valide pendant huit heures. Par conséquent, si vous bloquez un client parce qu'il n'est plus approuvé, il peut continuer à télécharger du contenu à partir d'un point de distribution cloud, jusqu'à la fin de la période de validité de ce jeton. À ce stade, le point de gestion n'émettra pas d'autre jeton pour le client, puisque celui-ci aura été bloqué.

  Pour empêcher un client bloqué de télécharger du contenu pendant cette période de huit heures, vous pouvez arrêter le service cloud à partir du nœud **Cloud**, **Configuration de la hiérarchie**, dans l'espace de travail **Administration** de la console Configuration Manager.

## Informations de confidentialité pour la gestion de contenu

Configuration Manager n'inclut pas de données utilisateur dans les fichiers de contenu, même si un utilisateur administratif peut choisir d'en ajouter.

Avant de configurer la gestion de contenu, pensez à vos besoins en matière de confidentialité.

# Comprendre comment les clients recherchent des services et des ressources de site pour System Center Configuration Manager

22/06/2018 • 31 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les clients System Center Configuration Manager utilisent un processus appelé *emplacement du service* pour trouver les serveurs de système de site avec lesquels ils peuvent communiquer et qui leur fournissent les services dont ils ont besoin. Bien comprendre comment et quand les clients utilisent l'emplacement du service pour rechercher des ressources de site peut vous aider à configurer vos sites de manière appropriée pour prendre en charge les tâches des clients. Ces configurations peuvent nécessiter que le site interagisse avec des configurations de domaine et de réseau telles que AD DS et DNS. Elles peuvent également nécessiter la configuration d'alternatives plus complexes.

Exemples de rôles de système de site qui fournissent des services :

- Serveur de système de site principal pour les clients.
- Point de gestion.
- Serveurs de système de site supplémentaires avec lesquels le client peut communiquer, tels que les points de distribution et les points de mises à jour logicielles.

## Fundamentals of service location

Quand un client utilise l'emplacement du service pour rechercher un point de gestion avec lequel il peut communiquer, il évalue son emplacement réseau actuel, son protocole de communication préféré et son site attribué.

**Un client communique avec un point de gestion pour effectuer les opérations suivantes :**

- Télécharger des informations concernant d'autres points de gestion du site, afin de pouvoir générer une liste des points de gestion connus (ou *liste PG*) pour les cycles ultérieurs d'emplacement du service.
- Charger les informations de la configuration, comme l'inventaire et l'état.
- Télécharger une stratégie qui définit des configurations sur le client et peut informer celui-ci sur les logiciels qu'il peut ou doit installer, et d'autres tâches connexes.
- Demander des informations sur les autres rôles de système qui fournissent des services que le client a été configuré pour utiliser. Il peut s'agir des points de distribution des logiciels que le client peut installer ou un point de mise à jour logicielle à partir duquel obtenir les mises à jour.

**Un client Configuration Manager effectue une demande d'emplacement du service :**

- Toutes les 25 heures de fonctionnement continu.
- Quand il détecte une modification de sa configuration ou de son emplacement réseau.
- Quand le service **ccmexec.exe** de l'ordinateur (service client de base) démarre.
- Quand le client doit localiser un rôle de système de site qui fournit un service requis.

**Quand un client essaie de trouver des serveurs qui hébergent des rôles système de site**, il utilise l'emplacement du service pour rechercher un rôle de système de site prenant en charge son protocole (HTTP ou HTTPS). Par défaut, les clients utilisent la méthode la plus sûre à leur disposition. Considérez les points suivants :

- Pour utiliser le protocole HTTPS, vous devez disposer d'une infrastructure à clé publique (PKI) et installer des certificats PKI sur des clients et serveurs. Pour plus d'informations sur la façon d'utiliser des certificats, consultez Configuration requise des certificats PKI pour System Center Configuration Manager.
- Quand vous déployez un rôle de système de site qui utilise Internet Information Services (IIS) et prend en charge les communications des clients, vous devez spécifier si les clients se connectent au système de site à l'aide de HTTP ou HTTPS. Si vous utilisez le protocole HTTP, vous devez également envisager les options de signature et de chiffrement. Pour plus d'informations, consultez Planifier la signature et le chiffrement dans la rubrique Planifier la sécurité dans System Center Configuration Manager.

## Emplacement du service et façon dont les clients déterminent leur point de gestion attribué

Quand un client est attribué pour la première fois à un site principal, il sélectionne un point de gestion par défaut pour ce site. Les sites principaux prennent en charge plusieurs points de gestion, et chaque client identifie indépendamment un point de gestion comme son point de gestion par défaut. Ce point de gestion par défaut devient ensuite le point de gestion attribué de ce client. (Vous pouvez également utiliser les commandes d'installation du client pour définir le point de gestion attribué au client lors de l'installation.)

Un client sélectionne le point de gestion avec lequel communiquer en fonction de son emplacement réseau et de son groupe de limites configurés. Le point de gestion utilisé par le client n'est pas obligatoirement son point de gestion attribué.

> **NOTE**
> Un client utilise toujours le point de gestion attribué pour les messages d'enregistrement et certains messages de la stratégie, même quand d'autres communications sont envoyées à un point de gestion proxy ou local.

Vous pouvez utiliser des points de gestion préférés. Les points de gestion préférés sont ceux du site attribué au client qui sont associés à un groupe de limites que le client utilise pour rechercher des serveurs de système de site. L'association d'un point de gestion préféré à un groupe de limites en tant que serveur de système de site est similaire à l'association de points de distribution ou de points de migration d'état à un groupe de limites. Si vous activez les points de gestion préférés pour la hiérarchie, lorsqu'un client utilise un point de gestion à partir de son site attribué, il va tenter d'utiliser un point de gestion préféré avant d'utiliser d'autres points de gestion à partir de son site attribué.

Vous pouvez également utiliser les informations du blog Management point affinity (Affinité des points de gestion) sur TechNet.com pour configurer l'affinité des points de gestion. L'affinité des points de gestion remplace le comportement par défaut des points de gestion attribués et permet au client d'utiliser un ou plusieurs points de gestion spécifiques.

Chaque fois qu'un client doit contacter un point de gestion, il consulte la liste PG qu'il stocke localement dans Windows Management Instrumentation (WMI). Le client crée la liste PG lors de son installation. Il met à jour régulièrement cette liste avec des informations sur chaque point de gestion dans la hiérarchie.

Quand le client ne trouve pas de point de gestion valide dans sa liste PG, il étend sa recherche aux sources d'emplacement de service suivantes, dans l'ordre et jusqu'à trouver un point de gestion qu'il peut utiliser :

1. Point de gestion
2. AD DS
3. DNS
4. WINS

Dès qu'un client a localisé et contacté un point de gestion, il télécharge sa liste des points de gestion disponibles dans la hiérarchie et met à jour sa liste locale. Cela s'applique aussi bien aux clients qui appartiennent à un domaine qu'à ceux qui n'y appartiennent pas.

Par exemple, quand un client Configuration Manager sur Internet se connecte à un point de gestion basé sur Internet, ce dernier lui envoie la liste des points de gestion basés sur Internet disponibles sur le site. De même, les clients qui appartiennent à un domaine ou figurent dans des groupes de travail reçoivent également la liste des points de gestion qu'ils peuvent utiliser.

Un client qui n'est pas configuré pour Internet ne reçoit pas de points de gestion exclusivement accessibles sur Internet. Les clients de groupe de travail configurés pour Internet communiquent uniquement avec des points de gestion accessibles sur Internet.

## La liste PG

La liste PG est la source d'emplacements de service préférés du client. Elle hiérarchise les points de gestion précédemment identifiés par le client. Cette liste est triée par chaque client en fonction de son emplacement réseau au moment où il l'a met à jour, puis stockée localement sur le client dans WMI.

**Création de la liste PG initiale**

Lors de l'installation du client, les règles suivantes sont utilisées pour générer sa liste PG initiale :

- Cette liste initiale inclut les points de gestion spécifiés lors de l'installation du client (quand vous utilisez l'option **SMSMP**= ou **/MP**).
- Le client recherche les points de gestion publiés, dans AD DS. Pour que le point de gestion soit identifié à partir d'AD DS, il doit provenir du site attribué du client et avoir la même version de produit que celle du client.
- Si aucun point de gestion n'a été spécifié lors de l'installation du client et si le schéma Active Directory n'est pas étendu, le client recherche des points de gestion publiés dans les services DNS et WINS.
- Lorsque le client crée la liste initiale, les informations concernant certains points de gestion de la hiérarchie peuvent ne pas être connues.

**Organisation de la liste PG**

Les clients organisent leur liste de points de gestion selon les classifications suivantes :

- **Proxy** : un point de gestion proxy sur un site secondaire.
- **Local** : tout point de gestion associé à l'emplacement réseau actuel du client tel qu'il est défini par les limites de site. Gardez à l'esprit les informations suivantes sur les limites :
  - Quand un client appartient à plusieurs groupes de limites, la liste des points de gestion locaux est déterminée en réunissant toutes les limites qui incluent l'emplacement réseau actuel du client.
  - En règle générale, les points de gestion locaux sont un sous-ensemble des points de gestion attribués d'un client, sauf si ce dernier se trouve à un emplacement réseau associé à un autre site avec des points de gestion desservant ses groupes de limites.
- **Attribué** : tout point de gestion représentant un système de site pour le site attribué du client.

Vous pouvez utiliser des points de gestion préférés. Les points de gestion d'un site qui ne sont pas associés à un groupe de limites ou qui ne figurent pas dans un groupe de limites associé à un emplacement réseau actuel du client ne sont pas considérés comme préférés. Ils seront utilisés si le client ne peut pas identifier un point de gestion par défaut disponible.

**Sélection d'un point de gestion à utiliser**

Pendant une communication classique, un client tente d'utiliser un point de gestion appartenant aux classifications dans l'ordre suivant, en fonction de l'emplacement réseau du client :

1. Proxy
2. Local
3. Attribués

Toutefois, le client utilise toujours le point de gestion attribué pour les messages d'enregistrement et certains messages de la stratégie, même quand d'autres communications sont envoyées à un point de gestion proxy ou local.

Dans chaque classification (proxy, local ou attribué), le client tente d'utiliser un point de gestion en fonction de préférences, dans l'ordre suivant :

1. Compatible HTTPS dans une forêt approuvée ou locale (quand le client est configuré pour la communication HTTPS)
2. Compatible HTTPS dans une forêt non approuvée ou non locale (quand le client est configuré pour la communication HTTPS)
3. Compatible HTTP dans une forêt approuvée ou locale
4. Compatible HTTP hors d'une forêt approuvée ou locale

Dans l'ensemble des points de gestion triés par préférences, le client tente d'utiliser le premier point de gestion de la liste. Cette liste triée de points de gestion est aléatoire et ne peut pas être ordonnée. L'ordre de la liste peut varier chaque fois que le client met à jour sa liste PG.

Si un client ne parvient pas à contacter le premier point de gestion, il essaie chacun des points de gestion suivants dans sa liste. Il teste chaque point de gestion préféré de la classification avant d'essayer des points de gestion non préférés. Si un client ne parvient pas communiquer avec un point de gestion dans la classification, il tente de contacter un point de gestion préféré de la classification suivante, et ainsi de suite jusqu'à ce qu'il trouve un point de gestion à utiliser.

Une fois la communication établie avec un point de gestion, le client continue d'utiliser ce même point de gestion jusqu'à ce que :

- 25 heures soient écoulées.
- Le client ne puisse pas communiquer avec le point de gestion à l'issue des cinq tentatives sur une période de 10 minutes.

Le client sélectionne de manière aléatoire un nouveau point de gestion à utiliser.

## Active Directory

Les clients qui appartiennent à un domaine peuvent utiliser les services AD DS pour l'emplacement du service. Pour ce faire, les sites doivent publier des données dans Active Directory.

Un client peut utiliser AD DS comme emplacement du service quand l'une des conditions suivantes est remplie :

- Le schéma Active Directory est étendu ou a été étendu pour System Center 2012 Configuration Manager.
- La forêt Active Directory est configurée pour la publication, de même que les sites Configuration Manager.
- L'ordinateur client est membre d'un domaine Active Directory et peut accéder à un serveur de catalogue global.

Si un client ne peut pas trouver de point de gestion à utiliser comme emplacement du service dans AD DS, il tente d'utiliser DNS.

## DNS

Les clients se trouvant sur l'intranet peuvent utiliser DNS pour l'emplacement du service. Pour ce faire, au moins un site d'une hiérarchie doit publier des informations sur les points de gestion dans DNS.

Envisagez d'utiliser DNS pour l'emplacement du service quand l'une des conditions suivantes est remplie :

- Le schéma AD DS n'est pas étendu pour prendre en charge Configuration Manager.
- Les clients sur intranet se trouvent dans une forêt qui n'est pas activée pour la publication Configuration Manager.
- Des clients se trouvent sur des ordinateurs de groupes de travail et ne sont pas configurés pour la gestion des clients uniquement accessibles sur Internet. (Un client de groupe de travail configuré pour Internet communique uniquement avec des points de gestion accessibles sur Internet et n'utilise pas DNS comme emplacement du service.)
- Vous pouvez configurer les clients pour rechercher les points de gestion dans les services DNS.

Quand un site publie des enregistrements d'emplacement de service pour les points de gestion dans DNS :

- La publication est uniquement applicable aux points de gestion qui acceptent les connexions client à partir de l'intranet.
- La publication ajoute un enregistrement de ressource d'emplacement du service (SRV RR) dans la zone DNS de l'ordinateur du point de gestion. Une entrée hôte correspondante doit se trouver dans DNS pour cet ordinateur.

Par défaut, les clients appartenant à un domaine recherchent des enregistrements de point de gestion dans DNS à partir de leur domaine local. Vous pouvez configurer une propriété de client qui spécifie un suffixe pour un domaine qui publie des informations sur les points de gestion dans DNS.

Pour plus d'informations sur la configuration de la propriété cliente du suffixe DNS, consultez Guide pratique pour configurer des ordinateurs clients pour trouver des points de gestion à l'aide de la publication DNS dans System Center Configuration Manager.

Si un client ne trouve pas de point de gestion à utiliser pour l'emplacement du service dans DNS, il tente d'utiliser WINS.

**Publier des points de gestion dans DNS**

Pour publier des points de gestion dans DNS, les deux conditions suivantes doivent être vraies :

- Vos serveurs DNS prennent en charge les enregistrements de ressource d'emplacement de service, à l'aide d'une version de BIND qui est au moins la version 8.1.2.
- Les noms de domaine complets intranet spécifiés pour les points de gestion dans Configuration Manager ont des entrées d'hôte (par exemple, des enregistrements A) dans DNS.

> **IMPORTANT**
> La publication DNS Configuration Manager ne prend pas en charge un espace de noms disjoint. Si votre espace de noms est disjoint, vous pouvez publier manuellement des points de gestion dans DNS ou utiliser l'une des autres méthodes d'emplacement de service décrites dans cette section.

**Quand vos serveurs DNS prennent en charge les mises à jour automatiques**, vous pouvez configurer Configuration Manager pour qu'il publie automatiquement les points de gestion intranet dans DNS, ou vous pouvez publier manuellement ces enregistrements dans DNS. Lorsque des points de gestion sont publiés dans DNS, leur nom de domaine complet Intranet et leur numéro de port sont publiés dans l'enregistrement d'emplacement de service (SRV). Vous configurez la publication DNS sur un site dans les Propriétés du composant de point de gestion du site. Pour plus d'informations, consultez Composants de site pour System Center Configuration Manager.

**Quand la zone DNS est réglée sur « Secure only » (Sécurisées uniquement) pour les mises à jour dynamiques**, seul le premier point de gestion pouvant publier dans DNS peut effectuer cette action avec les autorisations par défaut.

Si un seul point de gestion peut publier et modifier son enregistrement DNS, et que le serveur de ce point de gestion est fonctionnel, les clients peuvent obtenir la liste complète de leurs points de gestion et trouver leur point de gestion préféré.

**Quand vos serveurs DNS ne prennent pas en charge les mises à jour automatiques, mais prennent en charge les enregistrements d'emplacement de service**, vous pouvez publier manuellement des points de gestion dans DNS. Pour cela, vous devez spécifier manuellement l'enregistrement de la ressource d'emplacement de service (SRV RR) dans DNS.

Configuration Manager prend en charge la norme RFC 2782 pour les enregistrements d'emplacement de service. Ces enregistrements présentent le format suivant : *_Service._Proto.Nom TTL Classe SRV Priorité Poids Port Cible*.

Pour publier un point de gestion sur Configuration Manager, spécifiez les valeurs suivantes :

- **_Service** : entrez **_mssms_mp**<*code_site*>, *où <code_site> est le code du site du point de gestion.*
- **._Proto**: spécifiez **._tcp**.
- **.Name**: entrez le suffixe DNS du point de gestion, par exemple **contoso.com**.
- **TTL**: entrez **14400**, ce qui correspond à quatre heures.
- **Class**: spécifiez **IN** (conformément à la norme RFC 1035).
- **Priorité** : Configuration Manager n'utilise pas ce champ.
- **Poids** : Configuration Manager n'utilise pas ce champ.
- **Port**: entrez le numéro de port que le point de gestion utilise, par exemple **80** pour HTTP et **443** pour HTTPS.

  > **NOTE**
  > Le port de l'enregistrement SRV doit correspondre au port de communication utilisé par le point de gestion. Par défaut, le port **80** est utilisé pour les communications HTTP et le port **443** pour les communications HTTPS.

- **Cible**: entrez le nom de domaine complet de l'intranet spécifié pour le système de site configuré avec le rôle de site de point de gestion.

Si vous utilisez le DNS Windows Server, vous pouvez utiliser la procédure suivante pour entrer cet enregistrement DNS pour les points de gestion intranet. Si vous utilisez une autre implémentation de DNS, utilisez les informations de cette section sur les valeurs de champ et consultez la documentation de ce DNS pour adapter cette procédure.

#### Pour configurer la publication automatique :

1. Dans la console Configuration Manager, développez **Administration** > **Configuration du site** > **Sites**.
2. Sélectionnez votre site, puis cliquez sur **Configurer les composants de site**.
3. Sélectionnez **Point de gestion**.
4. Sélectionnez les points de gestion à publier. (Cette sélection s'applique à la publication dans AD DS et DNS.)
5. Cochez la case pour publier dans DNS. Cette case :
   - Permet de sélectionner les points de gestion à publier dans DNS.
   - Ne configure pas la publication dans AD DS.

#### Pour publier manuellement des points de gestion dans DNS sur Windows Server

1. Dans la console Configuration Manager, spécifiez les noms de domaine complets d'intranet des systèmes de site.

2. Dans la console de gestion DNS, sélectionnez la zone DNS de l'ordinateur du point de gestion.
3. Vérifiez qu'il existe un enregistrement d'hôte (A ou AAAA) pour le nom de domaine complet d'intranet du système de site. Si cet enregistrement n'existe pas, créez-le.
4. À l'aide de l'option **New Other Records (Autres nouveaux enregistrements)**, cliquez sur **Emplacement du service (SRV)** dans la boîte de dialogue **Type d'enregistrement de ressource**, cliquez sur **Créer un enregistrement**, entrez les informations suivantes, puis choisissez **Terminé** :
   - **Domain**: si nécessaire, entrez le suffixe DNS du point de gestion, par exemple **contoso.com**.
   - **Service** : tapez **_mssms_mp**<*code_site*>, *où* <*code_site*> *est le code de site du point de gestion.*
   - **Protocol**: entrez **_tcp**.
   - **Priorité** : Configuration Manager n'utilise pas ce champ.
   - **Poids** : Configuration Manager n'utilise pas ce champ.
   - **Port**: entrez le numéro de port que le point de gestion utilise, par exemple **80** pour HTTP et **443** pour HTTPS.

     > **NOTE**
     > Le port de l'enregistrement SRV doit correspondre au port de communication utilisé par le point de gestion. Par défaut, le port **80** est utilisé pour les communications HTTP et le port **443** pour les communications HTTPS.

   - **Hôte offrant ce service** : entrez le nom de domaine complet de l'intranet, spécifié pour le système de site configuré avec le rôle de site du point de gestion.

Répétez ces étapes pour chaque point de gestion de l'intranet que vous souhaitez publier dans DNS.

## WINS

En cas d'échec d'autres mécanismes d'emplacement de service, les clients peuvent trouver un point de gestion initial en examinant WINS.

Par défaut, un site principal publie dans WINS le premier point de gestion du site configuré pour le protocole HTTP et le premier point de gestion configuré pour le protocole HTTPS.

Si vous ne souhaitez pas que les clients trouvent un point de gestion HTTP dans WINS, configurez les clients avec la propriété CCMSetup.exe Client.msi **SMSDIRECTORYLOOKUP=NOWINS**.

# Sécurité et confidentialité pour l'administration de site dans System Center Configuration Manager

22/06/2018 • 50 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cette rubrique contient des informations de sécurité et de confidentialité pour les sites System Center Configuration Manager et la hiérarchie.

## Bonnes pratiques de sécurité pour l'administration de site

Utilisez les bonnes pratiques de sécurité suivantes pour vous aider à sécuriser les sites System Center Configuration Manager et la hiérarchie.

**Exécutez le programme d'installation à partir d'une source approuvée et sécurisez le canal de communication entre le support d'installation et le serveur de site.**

Pour empêcher la falsification des fichiers sources, exécutez le programme d'installation à partir d'une source approuvée. Si vous stockez les fichiers sur le réseau, sécurisez l'emplacement réseau.

Si vous exécutez le programme d'installation à partir d'un emplacement réseau, pour empêcher une éventuelle personne malveillante de falsifier les fichiers lors de leur transmission sur le réseau, utilisez IPsec ou la signature SMB (Server Message Block) entre l'emplacement source des fichiers d'installation et le serveur de site.

De plus, si vous utilisez le téléchargeur d'installation pour télécharger les fichiers requis par le programme d'installation, veillez à sécuriser également l'emplacement de stockage de ces fichiers et sécurisez le canal de communication pour cet emplacement lorsque vous exécutez le programme d'installation.

**Développez le schéma Active Directory pour System Center Configuration Manager et publiez des sites vers les services de domaine Active Directory.**

Les extensions de schéma ne sont pas nécessaires pour exécuter System Center Configuration Manager, mais elles créent un environnement plus sécurisé car les serveurs de site et les clients Configuration Manager peuvent récupérer les informations à partir d'une source approuvée.

Si les clients se trouvent dans un domaine non approuvé, déployez les rôles de système de site suivants dans les domaines des clients :

- Point de gestion
- Point de distribution
- Point du site web du catalogue des applications

> **NOTE**
> Un domaine approuvé pour Configuration Manager requiert l'authentification Kerberos. Cela signifie que si des clients se trouvent dans une autre forêt qui ne dispose pas d'une approbation de forêt bidirectionnelle avec la forêt du serveur de site, ces clients sont considérés comme étant dans un domaine non approuvé. Dans ce cas, une approbation externe n'est pas suffisante.

**Utilisez IPsec pour sécuriser les communications entre les sites et serveurs de système de site.**

Bien que Configuration Manager sécurise les communications entre le serveur de site et l'ordinateur qui exécute SQL Server, Configuration Manager ne sécurise pas les communications entre les rôles de système de site et SQL Server. Seuls certains systèmes de site (le point d'inscription et le point de service Web du catalogue d'applications) peuvent être configurés pour le protocole HTTPS pour la communication intrasite.

Si vous n'utilisez pas de contrôles supplémentaires pour sécuriser ces canaux serveur à serveur, des personnes malveillantes peuvent utiliser différentes attaques d'usurpation ou de l'intercepteur contre les systèmes de site. Utilisez la signature SMB lorsque vous ne pouvez pas utiliser IPsec.

> **NOTE**
> Il est particulièrement important de sécuriser le canal de communication entre le serveur de site et le serveur de la source du package. Cette communication utilise SMB. Si vous ne pouvez pas utiliser IPsec pour sécuriser cette communication, utilisez la signature SMB afin de vous assurer que les fichiers ne sont pas falsifiés avant que les clients les téléchargent et les exécutent.

**Ne modifiez pas les groupes de sécurité créés et gérés par Configuration Manager pour la communication du système de site.**

Groupes de sécurité :

- **SMS_SiteSystemToSiteServerConnection_MP_<code_site>**
- **SMS_SiteSystemToSiteServerConnection_SMSProv_<code_site>**
- **SMS_SiteSystemToSiteServerConnection_Stat_<code_site>**

Configuration Manager crée et gère automatiquement ces groupes de sécurité. Cela inclut la suppression de comptes d'ordinateur lorsqu'un rôle de système de site est supprimé.

Pour garantir la continuité de service et des privilèges minimum, ne modifiez pas ces groupes manuellement.

**Si les clients ne peuvent pas interroger le serveur du catalogue global pour obtenir des informations Configuration Manager, gérez le processus de mise en service de la clé racine approuvée.**

Si les clients ne peuvent pas interroger le catalogue global pour obtenir des informations Configuration Manager, ils doivent s'appuyer sur la clé racine approuvée pour authentifier des points de gestion valides. La clé racine approuvée est stockée dans le Registre du client et peut être configurée à l'aide d'une stratégie de groupe ou d'une configuration manuelle.

Si le client ne dispose pas d'une copie de la clé racine approuvée avant de contacter un point de gestion pour la première fois, il approuve le premier point de gestion avec lequel il communique. Pour réduire le risque d'un acte de piraterie consistant à réacheminer les clients vers un point de gestion non autorisé, vous pouvez préparer la mise en service des clients avec la clé racine approuvée. Pour plus d'informations, voir Planification de la clé racine approuvée.

**Utilisez des numéros différents des numéros de port par défaut.**

L'utilisation de numéros de port différents des numéros par défaut peut vous permettre de bénéficier d'une sécurité supplémentaire, car les personnes malveillantes ont plus de difficulté à explorer l'environnement en vue d'une attaque. Si vous décidez d'utiliser des ports autres que les ports par défaut, planifiez-les avant d'installer Configuration Manager et utilisez-les de manière cohérente sur tous les sites de la hiérarchie. Les ports de demande client et l'éveil par appel réseau (Wake On LAN), notamment, permettent d'utiliser des numéros de port autres que les numéros par défaut.

**Utilisez la séparation des rôles sur les systèmes de site.**

Bien que vous puissiez installer tous les rôles de système de site sur un seul ordinateur, cette pratique est rarement utilisée sur les réseaux de production, car elle crée un point de défaillance unique.

**Réduisez le profil d'attaque.**

L'isolation de chaque rôle de système de site sur un serveur différent réduit le risque qu'une attaque contre les vulnérabilités d'un système de site puisse être utilisée contre un autre système de site. De nombreux rôles de système de site requièrent l'installation d'IIS (Internet Information Services) sur le système de site et cela augmente la surface d'attaque. Si vous devez combiner des rôles de système de site afin de réduire les dépenses en matériel, combinez les rôles de système de site IIS uniquement avec d'autres rôles de système de site nécessitant IIS.

> **IMPORTANT**
> Le rôle de point d'état de secours est une exception. Comme ce rôle de système de site accepte les données non authentifiées des clients, nous vous recommandons de ne jamais attribuer le rôle de point d'état de secours à un autre système de site Configuration Manager.

**Suivez les meilleures pratiques de sécurité pour Windows Server et exécutez l'Assistant Configuration de la sécurité sur tous les systèmes de site.**

L'Assistant Configuration de la sécurité (SCW) vous aide à créer une stratégie de sécurité que vous pouvez appliquer à n'importe quel serveur de votre réseau. Une fois que vous avez installé le modèle System Center Configuration Manager, l'Assistant Configuration de la sécurité reconnaît les applications, les services, les ports et les rôles de système de site Configuration Manager. Il autorise ensuite les communications requises pour Configuration Manager et bloque les communications non requises.

L'Assistant Configuration de la sécurité est inclus dans le kit de ressources pour System Center 2012 Configuration Manager, que vous pouvez télécharger dans le Centre de téléchargement Microsoft : System Center 2012 – Composants additionnels et extensions du composant Configuration Manager.

**Configurez des adresses IP statiques pour les systèmes de site.**

Les adresses IP statiques sont plus simples à protéger des attaques de résolution de noms.

Elles facilitent également la configuration d'IPsec. L'utilisation d'IPsec est une bonne pratique de sécurité pour sécuriser les communications entre des systèmes de site dans Configuration Manager.

**N'installez pas d'autres applications sur des serveurs de système de site.**

Lorsque vous installez d'autres applications sur des serveurs de système de site, vous augmentez la surface d'attaque pour Configuration Manager et risquez des problèmes d'incompatibilité.

**Exigez la signature et autorisez le cryptage comme une option de site.**

Activez les options de signature et de cryptage pour le site. Assurez-vous que tous les clients peuvent prendre en charge l'algorithme de hachage SHA-256, puis activez l'option **Exiger SHA-256**.

**Limitez et surveillez les utilisateurs administratifs Configuration Manager et utilisez l'administration basée sur les rôles pour accorder à ces utilisateurs les autorisations minimales dont ils ont besoin.**

Accordez un accès administratif à Configuration Manager uniquement aux utilisateurs auxquels vous faites confiance, puis accordez-leur les autorisations minimales en utilisant les rôles de sécurité intégrés ou en personnalisant les rôles de sécurité. Les utilisateurs administratifs qui peuvent créer, modifier et déployer des applications, des séquence de tâches, des mises à jour logicielles, des éléments de configuration et des références de configuration, peuvent potentiellement contrôler des appareils dans la hiérarchie Configuration Manager.

Auditez régulièrement les affectations d'utilisateur administratifs et leur niveau d'autorisation pour vérifier les modifications requises.

Pour plus d'informations sur la configuration de l'administration basée sur des rôles, voir la section Configure role-

based administration for System Center Configuration Manager.

**Sécurisez les sauvegardes Configuration Manager et le canal de communication lors de la sauvegarde et de la restauration.**

Lorsque vous sauvegardez Configuration Manager, ces informations incluent des certificats et d'autres données sensibles qui pourraient être utilisées par une personne malveillante pour l'emprunt d'identité.

Utilisez la signature SMB ou IPsec lorsque vous transférez ces données sur le réseau et sécurisez l'emplacement de sauvegarde.

**Lorsque vous exportez ou importez des objets à partir de la console Configuration Manager vers un emplacement réseau, sécurisez l'emplacement et le canal de réseau.**

Veillez à restreindre l'accès au dossier réseau.

Utilisez la signature SMB ou IPsec entre l'emplacement réseau et le serveur de site, et entre l'ordinateur qui exécute la console Configuration Manager et le serveur de site pour empêcher une personne malveillante de falsifier les données exportées. Utilisez IPsec pour chiffrer les données sur le réseau afin d'éviter la divulgation d'informations.

**Si un système de site n'est pas désinstallé correctement ou cesse de fonctionner et ne peut pas être restauré, supprimez manuellement les certificats Configuration Manager pour ce serveur à partir des autres serveurs Configuration Manager.**

Pour supprimer la confiance entre homologues initialement établie avec le système de site et les rôles de système de site, supprimez manuellement les certificats Configuration Manager pour le serveur en échec dans le magasin de certificats **Personnes autorisées** sur d'autres serveurs de système de site. Ceci est particulièrement important si vous adaptez le serveur sans le reformater.

Pour plus d'informations sur ces certificats, consultez la section **Contrôles de chiffrement pour la communication du serveur** dans Informations techniques de référence sur les contrôles de chiffrement pour System Center Configuration Manager.

**Ne configurez pas les systèmes de site basés sur Internet pour relier le réseau de périmètre et l'Intranet.**

Ne configurez pas les serveurs de système de site comme multi-résidents, afin qu'ils se connectent au réseau de périmètre et à l'intranet. Bien que cette configuration autorise les systèmes de site basés sur Internet à accepter les connexions client à partir d'Internet et de l'Intranet, elle élimine une limite de sécurité entre le réseau de périmètre et l'Intranet.

**Si le serveur de système de site se trouve sur un réseau non approuvé (tel qu'un réseau de périmètre), configurez le serveur de site pour établir des connexions avec le système de site.**

Par défaut, les systèmes de site établissent des connexions avec le serveur de site pour transférer des données, ce qui peut constituer un risque pour la sécurité lorsque la connexion est établie depuis un réseau non approuvé vers le réseau approuvé. Lorsque des systèmes de site acceptent des connexions depuis Internet ou résident dans une forêt non approuvée, configurez l'option du système de site **Exiger que le serveur de site établisse des connexions vers ce système de site** afin que toutes les connexions soient établies depuis le réseau approuvé une fois que le système de site et tout rôle de système de site a été installé.

**Si vous utilisez un serveur proxy Web pour la gestion des clients basés sur Internet, utilisez le pontage SSL vers SSL à l'aide de la terminaison avec authentification.**

Lorsque vous configurez la terminaison SSL au niveau du serveur Web proxy, les paquets provenant d'Internet sont inspectés avant d'être transférés au réseau interne. Le serveur Web proxy authentifie la connexion du client, l'arrête, puis ouvre une nouvelle connexion authentifiée vers les systèmes de site basés sur Internet.

Lorsque les ordinateurs clients Configuration Manager utilisent un serveur web proxy pour se connecter à des systèmes de site basés sur Internet, l'identité du client (GUID client) est contenue, en toute sécurité, dans la charge

utile du paquet pour que le point de gestion ne considère pas le serveur web proxy comme le client. Si votre serveur Web proxy ne peut pas prendre en charge la configuration requise pour le pontage SSL, le tunnel SSL est également pris en charge. Il s'agit d'une option moins sûre car les paquets SSL d'Internet sont transférés aux systèmes de site sans terminaison et ne peuvent donc pas être inspectés à la recherche de contenu malveillant.

Si votre serveur Web proxy ne peut pas prendre en charge la configuration requise pour le pontage SSL, vous pouvez utiliser le tunnel SSL. Toutefois, il s'agit d'une option moins sûre car les paquets SSL d'Internet sont transférés aux systèmes de site sans terminaison et ne peuvent donc pas être inspectés à la recherche de contenu malveillant.

> **WARNING**
> Les appareils mobiles qui sont inscrits par Configuration Manager ne peuvent pas utiliser le pontage SSL et doivent utiliser le tunnel SSL uniquement.

**Configurations à utiliser si vous configurez le site pour qu'il réveille les ordinateurs afin d'installer le logiciel :**

- Si vous utilisez des paquets de mise en éveil traditionnels, utilisez la monodiffusion plutôt que des diffusions dirigées vers le sous-réseau.
- Si vous devez utiliser des diffusions dirigées vers le sous-réseau, configurez les routeurs de sorte à autoriser les diffusions vers IP uniquement à partir du serveur de site et uniquement sur un numéro de port autre que le port par défaut.

Pour plus d'informations sur les différentes technologies Wake On LAN, consultez Planification de l'éveil des clients dans System Center Configuration Manager.

**Si vous utilisez la notification par courrier électronique, configurez un accès authentifié au serveur de messagerie SMTP.**

Dans la mesure du possible, utilisez un serveur de courrier qui prend en charge l'accès authentifié et le compte d'ordinateur du serveur de site pour l'authentification. Si vous devez spécifier un compte d'utilisateur pour l'authentification, utilisez un compte qui dispose des privilèges minimum.

## Bonnes pratiques de sécurité pour le serveur de site

Utilisez les bonnes pratiques de sécurité suivantes pour mieux sécuriser le serveur de site Configuration Manager.

**Installez Configuration Manager sur un serveur membre plutôt que sur un contrôleur de domaine.**

Le serveur de site Configuration Manager et les systèmes de site ne nécessitent pas d'installation sur un contrôleur de domaine. Un contrôleur de domaine ne possède pas de base de données SAM (Security Accounts Management) locale autre que la base de données du domaine. Lorsque vous installez Configuration Manager sur un serveur membre, vous pouvez gérer les comptes Configuration Manager dans la base de données SAM locale plutôt que dans la base de données du domaine.

Cette pratique réduit également la surface d'attaque sur vos contrôleurs de domaine.

**Installez des sites secondaires en évitant de copier les fichiers vers le serveur de site secondaire sur le réseau.**

Lorsque vous exécutez le programme d'installation et créez un site secondaire, ne sélectionnez pas l'option de copie des fichiers depuis le site parent vers le site secondaire, et n'utilisez pas un emplacement réseau source. Lorsque vous copiez des fichiers sur le réseau, un attaquant doué pourrait pirater le package d'installation du site secondaire et falsifier les fichiers avant qu'ils soient installés, bien qu'il soit difficile de programmer cette attaque. Cette attaque peut être atténuée à l'aide d'IPsec ou de SMB lorsque vous transférez les fichiers.

Au lieu de copier les fichiers sur le réseau, sur le serveur de site secondaire, copiez les fichiers sources du dossier multimédia vers un dossier local. Ensuite, lorsque vous exécutez le programme d'installation pour créer un site secondaire, dans la page **Fichiers sources d'installation**, sélectionnez **Utiliser les fichiers sources dans l'emplacement local suivant sur l'ordinateur de site secondaire (le plus sûr)**, et spécifiez ce dossier.

Pour plus d'informations, consultez Install a secondary site (Installer un site secondaire) dans la rubrique Use the Setup Wizard to install sites (Utiliser l'Assistant Configuration pour installer des sites).

## Bonnes pratiques de sécurité pour SQL Server

Configuration Manager utilise SQL Server comme base de données principale. Si la base de données est compromise, des personnes malveillantes pourraient contourner Configuration Manager et accéder directement à SQL Server afin de lancer des attaques via Configuration Manager. Considérez les attaques contre SQL Server comme présentant un risque élevé et traitez-les en conséquence.

Utilisez les bonnes pratiques de sécurité suivantes pour mieux sécuriser SQL Server pour Configuration Manager.

**N'utilisez pas le serveur de base de données de site Configuration Manager pour exécuter d'autres applications SQL Server.**

L'augmentation du nombre d'accès au serveur de base de données de site Configuration Manager augmente le risque auquel sont exposées vos données Configuration Manager. Si la base de données du site Configuration Manager est compromise, les autres applications sur le même ordinateur SQL Server présentent également des risques.

**Configurez SQL Server pour utiliser l'authentification Windows.**

Configuration Manager accède au site de base de données à l'aide d'un compte Windows et de l'authentification Windows, mais vous pouvez également configurer SQL Server de sorte qu'il utilise le mode mixte SQL Server. Le mode mixte SQL Server vous permet de configurer des connexions SQL supplémentaires afin d'accéder à la base de données, mais cela n'est pas nécessaire et augmente la surface d'attaque.

**Prenez des mesures supplémentaires pour assurer que les sites secondaires qui utilisent SQL Server Express disposent des dernières mises à jour logicielles.**

Lorsque vous installez un site principal, Configuration Manager télécharge SQL Server Express depuis le Centre de téléchargement Microsoft, puis copie les fichiers sur le serveur de site principal. Lorsque vous installez un site secondaire et sélectionnez l'option d'installation de SQL Server Express, Configuration Manager installe la version téléchargée précédemment et ne vérifie pas si de nouvelles versions sont disponibles. Pour vous assurer que le site secondaire dispose des dernières versions, effectuez l'une des tâches suivantes :

- Une fois le site secondaire installé, exécutez Windows Update sur le serveur de site secondaire.
- Avant d'installer le site secondaire, installez SQL Server Express manuellement sur l'ordinateur qui va exécuter le serveur de site secondaire et assurez-vous d'installer la version la plus récente, ainsi que toutes les mises à jour logicielles. Installez ensuite le site secondaire et sélectionnez l'option pour utiliser une instance existante de SQL Server.

Exécutez régulièrement Windows Update sur ces sites et sur toutes les versions installées de SQL Server pour vous assurer qu'ils disposent des dernières mises à jour logicielles.

**Suivez les meilleures pratiques pour SQL Server.**

Identifiez et suivez les meilleures pratiques pour votre version de SQL Server. Prenez toutefois en compte les impératifs suivants pour Configuration Manager :

- Le compte d'ordinateur du serveur de site doit être membre du groupe Administrateurs sur l'ordinateur exécutant SQL Server. Si vous suivez la recommandation SQL Server « Définir des administrateurs de

manière explicite », le compte utilisé pour exécuter l'installation sur le serveur de site doit être membre du groupe Utilisateurs SQL.

- Si vous installez SQL Server à l'aide d'un compte utilisateur de domaine, vous devez configurer un nom principal de service (SPN) pour le compte d'ordinateur de domaine dans les services de domaine Active Directory. Sans le nom de principal du service, l'authentification Kerberos échoue, de même que l'installation de Configuration Manager.

## Bonnes pratiques de sécurité pour les systèmes de site exécutant IIS

Plusieurs rôles de système de site dans Configuration Manager requièrent IIS. Le processus de sécurisation IIS permet à Configuration Manager de fonctionner correctement et réduit les risques d'attaques de sécurité. Dans la mesure du possible, réduisez le nombre de serveurs qui requièrent IIS. Par exemple, exécutez uniquement le nombre de points de gestion dont vous avez besoin pour prendre en charge votre base de clients, en tenant compte de la haute disponibilité et de l'isolation du réseau pour la gestion des clients basée sur Internet.

Utilisez les meilleures pratiques de sécurité suivantes pour contribuer à sécuriser les systèmes de site qui exécutent IIS.

**Désactivez les fonctions IIS dont vous n'avez pas besoin.**

Installez uniquement les fonctionnalités IIS minimales pour le rôle de système de site que vous installez. Pour plus d'informations, consultez Prérequis des sites et systèmes de site.

**Configurez les rôles de système de site pour exiger HTTPS.**

Lorsque les clients se connectent à un système de site à l'aide du protocole HTTP au lieu de HTTPS, ils utilisent l'authentification Windows, qui peut avoir recours à l'authentification NTLM plutôt qu'à l'authentification Kerberos. Avec l'authentification NTLM, les clients risquent de se connecter à un serveur non autorisé.

Les points de distribution peuvent présenter l'exception à cette meilleure pratique de sécurité dans la mesure où les comptes d'accès aux packages ne fonctionnent pas lorsque ces points de distribution sont configurés pour le protocole HTTPS. Les comptes d'accès aux packages fournissent des autorisations d'accès au contenu, vous permettant de limiter les utilisateurs disposant des droits d'accès au contenu. Pour plus d'informations, voir Bonnes pratiques de sécurité pour la gestion de contenu.

**Configurez une liste de certificats de confiance dans IIS pour les rôles système de site.**

Rôles des systèmes de site :

- Point de distribution configuré pour le protocole HTTPS
- Point de gestion configuré pour le protocole HTTPS et pour la prise en charge des appareils mobiles

Une liste de certificats de confiance est une liste définie d'autorités de certification racine de confiance. Utilisée avec une stratégie de groupe et un déploiement d'infrastructure à clé publique (PKI), une liste de certificats de confiance vous permet de compléter les autorités de certification racine de confiance déjà configurées sur votre réseau, notamment celles installées automatiquement avec Microsoft Windows ou ajoutées par le biais des autorités de certification racine d'entreprise Windows. Toutefois, lorsqu'une liste de certificats de confiance est configurée dans IIS, elle définit un sous-ensemble des autorités de certification racine de confiance.

Ce dernier vous confère un contrôle accru de la sécurité car la liste de certificats de confiance limite l'acceptation des certificats clients à ceux qui sont publiés à partir de la liste des autorités de certification de la liste de certificats de confiance. Par exemple, Windows est fourni avec différents certificats d'autorités de certification tierces renommées, telles que VeriSign et Thawte.

Par défaut, l'ordinateur qui exécute les services Internet (IIS) approuve les certificats liés à ces autorités de certification connues. Si vous ne configurez pas IIS avec une liste de certificats de confiance pour les rôles de

système de site répertoriés, tout appareil doté d'un certificat client publié par ces autorités de certification est accepté comme client Configuration Manager valide. Si vous configurez les services Internet (IIS) avec une liste de certificats de confiance qui ne comprend pas ces autorités de certification, les connexions de clients sont rejetées si le certificat requis était lié à ces autorités de certification. Cependant, pour que les clients Configuration Manager soient acceptés dans les rôles de système de site répertoriés, vous devez configurer IIS avec une liste de certificats de confiance qui spécifie les autorités de certification utilisées par les clients Configuration Manager.

> **NOTE**
> Seuls les rôles de système de site répertoriés exigent que vous configuriez une liste de certificats de confiance dans IIS. La liste d'émetteurs de certificats utilisée par Configuration Manager pour les points de gestion fournit la même fonctionnalité aux ordinateurs clients lorsqu'ils se connectent aux points de gestion HTTPS.

Pour plus d'informations sur la façon de configurer une liste d'autorités de certification approuvées dans IIS, consultez la documentation de IIS.

**N'installez pas le serveur de site sur un ordinateur comportant IIS.**

La séparation des rôles permet de réduire le profil d'attaque et d'optimiser la récupération. De plus, le compte d'ordinateur du serveur de site dispose généralement des privilèges d'administrateur sur tous les rôles de système de site (et probablement sur les clients Configuration Manager, si vous utilisez l'installation poussée du client).

**Utilisez des serveurs IIS dédiés pour Configuration Manager.**

Il est possible d'héberger plusieurs applications basées sur le web sur les serveurs IIS utilisés par Configuration Manager, mais cela peut augmenter considérablement votre surface d'attaque. Une application mal configurée peut permettre à un attaquant d'acquérir le contrôle d'un système de site Configuration Manager, puis d'étendre son contrôle à la hiérarchie.

Si vous devez exécuter d'autres applications basées sur le web sur des systèmes de site Configuration Manager, créez un site web personnalisé pour les systèmes de site Configuration Manager.

**Utilisez un site web personnalisé.**

Pour les systèmes de site exécutant IIS, vous pouvez configurer Configuration Manager pour utiliser un site web personnalisé en lieu et place du site web par défaut pour IIS. Si vous devez exécuter d'autres applications basées sur le Web sur le système de site, vous devez utiliser un site web personnalisé. Ce paramètre s'applique à l'ensemble du site plutôt qu'à un système de site spécifique.

En plus de fournir une sécurité supplémentaire, vous devez utiliser un site Web personnalisé si vous exécutez d'autres applications Web sur le système de site.

**Si vous passez du site Web par défaut à un site Web personnalisé après l'installation des rôles de point de distribution, supprimez les répertoires virtuels par défaut.**

Lorsque vous utilisez un site web personnalisé à la place du site web par défaut, Configuration Manager ne supprime pas les anciens répertoires virtuels. Supprimez les répertoires virtuels que Configuration Manager a créés initialement sous le site web par défaut.

Par exemple, les répertoires virtuels à supprimer pour un point de distribution sont les suivants :

- SMS_DP_SMSPKG$
- SMS_DP_SMSSIG$
- NOCERT_SMS_DP_SMSPKG$
- NOCERT_SMS_DP_SMSSIG$

**Suivez les meilleures pratiques relatives au serveur IIS.**

Identifiez et suivez les meilleures pratiques relatives à votre version du serveur IIS. Toutefois, prenez en considération les spécifications de Configuration Manager relatives à certains rôles de système de site spécifiques. Pour plus d'informations, consultez Prérequis des sites et systèmes de site.

## Bonnes pratiques de sécurité pour le point de gestion

Les points de gestion représentent l'interface principale entre les appareils et Configuration Manager. Toute attaque contre le point de gestion et le serveur sur lequel il s'exécute doit être considérée comme représentant un risque élevé et doit être traitée en conséquence. Appliquez toutes les bonnes pratiques de sécurité et surveillez toute activité inattendue.

Utilisez les bonnes pratiques suivantes pour mieux sécuriser un point de gestion dans Configuration Manager.

**Lorsque vous installez un client Configuration Manager sur le point de gestion, attribuez-le au site de ce point de gestion.**

Évitez le scénario où un client Configuration Manager sur un système de site de point de gestion est attribué à un site autre que le site du point de gestion.

Si vous migrez vers System Center Configuration Manager à partir d'une version antérieure, migrez dès que possible le logiciel client sur le point de gestion vers System Center Configuration Manager.

## Bonnes pratiques de sécurité pour le point d'état de secours

Utilisez les bonnes pratiques de sécurité suivantes si vous installez un point d'état de secours dans Configuration Manager.

Pour plus d'informations sur les considérations relatives à la sécurité, voir Determine Whether You Require a Fallback Status Point.

**N'exécutez pas d'autres rôles de système de site sur le système de site et n'installez pas le point d'état de secours sur un contrôleur de domaine.**

Le point d'état de secours est conçu pour accepter les communications non authentifiées provenant de n'importe quel ordinateur. De ce fait, l'exécution de ce rôle de système de site avec d'autres rôles de système de site ou sur un contrôleur de domaine augmente considérablement le risque auquel est exposé le serveur.

**Lorsque vous utilisez des certificats PKI pour la communication client dans Configuration Manager, installez le point d'état de secours avant d'installer les clients.**

Si les systèmes de site Configuration Manager n'acceptent pas la communication client HTTP, vous pouvez ne pas être au courant que des clients ne sont pas gérés en raison de problèmes liés aux certificats PKI. Toutefois, si les clients sont affectés à un point d'état de secours, ces problèmes de certificat sont signalés par le point d'état de secours.

Pour des raisons de sécurité, vous ne pouvez pas affecter un point d'état de secours aux clients une fois qu'ils sont installés. Au lieu de cela, vous ne pouvez attribuer ce rôle que pendant l'installation des clients.

**Évitez d'utiliser le point d'état de secours dans le réseau de périmètre.**

Le point d'état de secours est conçu pour accepter les données provenant de n'importe quel client. Un point d'état de secours sur le réseau de périmètre facilite le dépannage des clients basés sur Internet, mais il convient d'évaluer les avantages liés au dépannage par rapport aux risques pouvant être engendrés par un système de site qui accepte les données non authentifiées sur un réseau accessible au public.

Si vous installez le point d'état de secours sur le réseau de périmètre ou sur tout réseau non approuvé, configurez

le serveur de site de sorte qu'il initialise les transferts de données au lieu du paramètre par défaut qui autorise le point d'état de secours à se connecter au serveur de site.

## Problèmes de sécurité pour l'administration de site

Passez en revue les problèmes de sécurité suivants pour Configuration Manager :

- Configuration Manager ne possède aucune défense contre un utilisateur administratif autorisé qui utilise Configuration Manager pour attaquer le réseau. Les utilisateurs administratifs non autorisés représentent un risque élevé pour la sécurité et peuvent lancer de nombreuses attaques, dont notamment les stratégies suivantes :

  - l'utilisation de la fonction de déploiement de logiciels pour installer et exécuter automatiquement un logiciel malveillant sur tous les clients Configuration Manager de l'entreprise ;
  - l'utilisation du contrôle distant pour prendre à distance le contrôle d'un client Configuration Manager sans autorisation ;
  - la configuration d'intervalles d'interrogation rapides et d'un grand nombre d'inventaires afin de créer des attaques par déni de service contre les clients et les serveurs ;
  - l'utilisation d'un site de la hiérarchie pour écrire des données dans un autre site Active Directory.

  La hiérarchie du site constitue la limite de sécurité. Considérez le sites comme des limites de gestion uniquement.

  Analysez toutes les opérations de l'utilisateur administratif et consultez régulièrement les journaux d'audit. Il est impératif de vérifier les antécédents professionnels des utilisateurs administratifs Configuration Manager avant de les recruter, puis de les soumettre régulièrement à des vérifications.

- Si le point d'inscription est compromis, un attaquant peut obtenir des certificats pour authentification et voler les informations d'identification des utilisateurs qui inscrivent leurs appareils mobiles.

  Le point d'inscription communique avec une autorité de certification et peut créer, modifier et supprimer des objets Active Directory. N'installez jamais le point d'inscription dans le réseau de périmètre et surveillez toute activité inattendue.

- Si vous autorisez des stratégies d'utilisateur pour la gestion des clients basés sur Internet ou configurez le point du site Web du catalogue d'applications pour les utilisateurs lorsqu'ils sont sur Internet, vous augmentez votre profil d'attaque.

  En plus des certificats PKI pour les connexions client à serveur, ces configurations requièrent l'authentification Windows, qui peut avoir recours à l'authentification NTLM plutôt qu'à l'authentification Kerberos. L'authentification NTLM est vulnérable aux attaques par relecture et emprunt d'identité. Pour authentifier correctement un utilisateur sur Internet, vous devez autoriser une connexion d'un serveur de système de site basé sur Internet à un contrôleur de domaine.

- Le partage Admin$ est requis sur les serveurs de système de site.

  Le serveur de site Configuration Manager utilise le partage Admin$ pour se connecter aux systèmes de site et y effectuer des opérations de service. Ne désactivez pas ou ne supprimez pas le partage Admin$.

- Configuration Manager utilise des services de résolution de noms pour se connecter à d'autres ordinateurs. Ces services sont difficiles à sécuriser contre des attaques de sécurité telles que l'usurpation, l'altération, la répudiation, la divulgation d'informations, le déni de service et l'élévation de privilèges.

  Identifiez et suivez les meilleures pratiques de sécurité pour la version de DNS et WINS que vous utilisez pour la résolution de noms.

# Informations de confidentialité pour la découverte

La découverte crée des enregistrements pour les ressources réseau et les stocke dans la base de données System Center Configuration Manager. Les enregistrements de données de découverte contiennent des informations sur les ordinateurs, telles que les adresses IP, les systèmes d'exploitation et les noms des ordinateurs. Les méthodes de découverte Active Directory peuvent également être configurées pour découvrir toute information stockée dans les services de domaine Active Directory.

La seule méthode de découverte activée par défaut est la découverte par pulsations d'inventaire, mais cette méthode découvre uniquement les ordinateurs sur lesquels le logiciel client System Center Configuration Manager est installé.

Les informations de découverte ne sont pas envoyées à Microsoft. Au lieu de cela, elles sont stockées dans la base de données Configuration Manager. Les informations sont conservées dans la base de données jusqu'à leur suppression, tous les 90 jours, par la tâche de maintenance du site **Supprimer les données de découverte anciennes**.

Avant de configurer d'autres méthodes de découverte ou d'étendre la découverte Active Directory, pensez aux conditions requises en termes de confidentialité.

# Configurer les pare-feu, les ports et les domaines pour System Center Configuration Manager

17/07/2018 • 3 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Pour préparer votre réseau à prendre en charge System Center Configuration Manager, prévoyez de configurer l'infrastructure, notamment les pare-feu, pour autoriser les communications Configuration Manager.

| CONSIDÉRATION | DÉTAILS |
| --- | --- |
| **Ports et protocoles** utilisés par les différentes fonctionnalités de Configuration Manager. Certains ports sont exigés, tandis que d'autres **domaines et services** sont personnalisables. | La plupart des communications Configuration Manager utilisent des ports courants, comme le port 80 pour HTTP ou le port 443 pour HTTPS. Toutefois, certains rôles de système de site prennent en charge l'utilisation de sites web personnalisés et de ports personnalisés.<br><br>**Avant de déployer Configuration Manager**, identifiez les ports que vous souhaitez utiliser et configurez les pare-feu de manière appropriée.<br><br>**Si vous avez besoin de modifier un port** après avoir installé Configuration Manager, n'oubliez pas de mettre à jour les pare-feu sur les appareils et sur le réseau, et également de modifier la configuration du port dans Configuration Manager.<br><br>Pour plus d'informations, consultez :<br>- Guide pratique pour configurer les ports de communication des clients<br>- Ports utilisés dans Configuration Manager<br>- Conditions requises pour l'accès Internet pour le point de connexion de service |
| **Domaines et services** que les serveurs et clients de site sont susceptibles d'utiliser. | Certaines fonctionnalités de Configuration Manager peuvent nécessiter que les clients et les serveurs de site accèdent à des services et domaines spécifiques sur Internet, comme Windowsudpate.microsoft.com ou le service Microsoft Intune.<br><br>Si vous souhaitez utiliser Microsoft Intune pour gérer des appareils mobiles, vous devez également configurer l'accès aux ports et domaines exigés par Intune. |
| **Serveurs proxy** pour les serveurs de système de site et les communications client. Vous pouvez spécifier des serveurs proxy distincts pour les différents clients et serveurs du système de site. | Étant donné que ces configurations sont effectuées lors de l'installation d'un rôle de système de site ou d'un client, il vous suffit de connaître les configurations de serveur proxy pour référence ultérieure lorsque vous configurerez des rôles de système de site et des clients.<br><br>Si vous ne savez pas si votre déploiement nécessite l'utilisation de serveurs proxy, consultez Prise en charge des serveurs proxy dans System Center Configuration Manager pour en savoir plus sur les rôles de système de site et les actions de client susceptibles d'utiliser un serveur proxy. |
| | |

# Préparer Active Directory pour la publication de site

22/06/2018 • 8 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Quand vous étendez le schéma Active Directory pour System Center Configuration Manager, les nouvelles structures que vous introduisez dans Active Directory sont utilisées par les sites System Center Configuration Manager pour publier des informations importantes, à un emplacement sécurisé facilement accessible par les clients.

Si vous gérez localement des clients, nous vous conseillons d'utiliser Configuration Manager avec un schéma Active Directory étendu. Un schéma étendu peut simplifier le processus de déploiement et de configuration des clients. Un schéma étendu permet également aux clients de localiser efficacement des ressources comme les serveurs de contenu et d'autres services fournis par les différents rôles de système de site Configuration Manager.

- Si vous ne savez pas si vous avez intérêt à utiliser un schéma étendu pour le déploiement dans Configuration Manager, consultez Extensions de schéma pour System Center Configuration Manager pour vous aider à prendre cette décision.
- Si vous n'utilisez pas de schéma étendu, vous pouvez configurer d'autres méthodes, telles que DNS et WINS, pour rechercher des services et des serveurs de système de site. Ces méthodes d'emplacement de service nécessitent des configurations supplémentaires et ne sont pas la méthode préférée pour l'emplacement du service par les clients. Pour en savoir plus, consultez Comprendre comment les clients recherchent des services et des ressources de site pour System Center Configuration Manager.
- Si votre schéma Active Directory a déjà été étendu pour Configuration Manager 2007 ou System Center 2012 Configuration Manager, vous n'avez pas d'autres tâches à effectuer. Les extensions de schéma demeurent inchangées et sont déjà en place.

L'extension du schéma est une opération qui s'effectue une seule fois pour n'importe quelle forêt. Pour étendre le schéma Active Directory étendu, puis l'utiliser, procédez comme suit :

## Étape 1. Étendre le schéma

Pour étendre le schéma pour Configuration Manager, vous devez :

- Utiliser un compte qui est membre du groupe de sécurité Administrateurs du schéma.
- Être connecté à un contrôleur de domaine principal du schéma.
- Exécuter l'outil **Extadsch.exe** , ou utiliser l'utilitaire de ligne de commande LDIFDE avec le fichier **ConfigMgr_ad_schema.ldf** . L'outil et le fichier se trouvent dans le dossier **SMSSETUP\BIN\X64** sur le média d'installation de Configuration Manager.

#### Option A : utiliser Extadsch.exe

1. Exécutez le fichier **extadsch.exe** pour ajouter les nouvelles classes et les nouveaux attributs au schéma Active Directory.

   > **TIP**
   > Exécutez cet outil à partir de la ligne de commande pour afficher les commentaires pendant son exécution.

2. Pour vérifier que l'extension du schéma a réussi, examinez extadsch.log à la racine du lecteur du système.

#### Option B : utiliser le fichier LDIF

1. Modifiez le fichier **ConfigMgr_ad_schema.ldf** pour définir le domaine racine Active Directory à étendre :
   - Remplacez toutes les instances du texte **DC=x** dans le fichier par le nom complet du domaine à étendre.
   - Par exemple, si le nom complet du domaine à étendre est widgets.microsoft.com, remplacez toutes les instances de DC=x dans le fichier par **DC=widgets, DC=microsoft, DC=com**.
2. À l'aide de l'utilitaire de ligne de commande LDIFDE, importez le contenu du fichier **ConfigMgr_ad_schema.ldf** dans Active Directory Domain Services :
   - Par exemple, la ligne de commande suivante importe les extensions de schéma dans Active Directory Domain Services, active la journalisation détaillée et crée un fichier journal pendant l'importation : **ldifde -i -f ConfigMgr_ad_schema.ldf -v -j <emplacement_de_stockage_du_fichier_journal>**.
3. Pour vérifier si l'extension du schéma a réussi, examinez le fichier journal créé par la ligne de commande exécutée à l'étape précédente.

## Étape 2. Créer le conteneur System Management et accorder des autorisations de sites au nouveau conteneur

Après avoir étendu le schéma, vous devez créer un conteneur nommé **System Management** dans Active Directory Domain Services (AD DS) :

- Vous créez ce conteneur une fois pour toutes dans chaque domaine comportant un site principal ou secondaire qui publiera des données dans Active Directory.
- Pour chaque conteneur, vous accordez des autorisations au compte d'ordinateur de chaque serveur de site principal et secondaire appelé à publier les données sur ce domaine. Chaque compte doit avoir un **contrôle total** sur le conteneur avec l'autorisation avancée **Appliquer à** égale à **cet objet et tous ceux descendants**.

#### Pour ajouter le conteneur

1. Utilisez un compte possédant l'autorisation **Créer tous les objets enfants** sur le conteneur **Système** dans les services de domaine Active Directory.
2. Exécutez **ADSI Edit** (adsiedit.msc) et connectez-vous au domaine du serveur de site.
3. Créez le conteneur :
   - Développez **Domaine** <nom_de_domaine_complet_ordinateur>, développez <nom_unique>, cliquez avec le bouton droit sur **CN=System**, choisissez **Nouveau**, puis **Objet**.
   - Dans la boîte de dialogue **Créer un objet**, choisissez **Conteneur**, puis **Suivant**.
   - Dans la zone **Valeur**, entrez **System Management**, puis choisissez **Suivant**.
4. Accordez les autorisations appropriées :

> **NOTE**
> Si vous préférez, vous pouvez utiliser d'autres outils, tels que l'outil d'administration Utilisateurs et ordinateurs Active Directory (DSA.msc) pour ajouter des autorisations au conteneur.

   - Cliquez avec le bouton droit sur **CN=System Management**, puis choisissez **Propriétés**.

- Choisissez l'onglet **Sécurité**, **Ajouter**, puis ajoutez le compte d'ordinateur de serveur de site avec l'autorisation **Contrôle intégral**.
- Choisissez **Avancé**, choisissez le compte d'ordinateur du serveur de site, puis choisissez **Modifier**.
- Dans la liste **Appliquer à**, choisissez **cet objet et tous ceux descendants**.

5. Choisissez **OK** pour fermer la console et enregistrer la configuration.

## Étape 3. Configurer les sites pour la publication de données sur Active Directory Domain Services

Après avoir configuré le conteneur, accordé les autorisations appropriées et installé un site principal Configuration Manager, vous pouvez configurer ce site pour la publication de données dans Active Directory.

Pour plus d'informations sur la publication, consultez Publier des données de site pour System Center Configuration Manager.

# Extensions de schéma pour System Center Configuration Manager

22/06/2018 • 10 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez étendre le schéma Active Directory pour prendre en charge Configuration Manager. Cette opération modifie le schéma Active Directory d'une forêt pour ajouter un nouveau conteneur et plusieurs attributs grâce auxquels les sites Configuration Manager peuvent publier dans Active Directory des informations clés utilisables par les clients de manière sécurisée. Ces informations peuvent simplifier le déploiement et la configuration des clients et aider ces derniers à localiser les ressources du site, comme les serveurs sur lesquels le contenu a été déployé ou qui fournissent différents services aux clients.

- Il est conseillé d'étendre le schéma Active Directory, mais ceci n'est pas obligatoire.

Avant d' étendre le schéma Active Directory, vous devez être familiarisé avec les services de domaine Active Directory et la modification du schéma Active Directory.

## Considérations relatives à l'extension du schéma Active Directory pour Configuration Manager

- Les extensions de schéma Active Directory pour System Center Configuration Manager sont identiques à celles utilisées par Configuration Manage 2007 et Configuration Manager 2012. Si vous avez déjà étendu le schéma pour l'une de ces versions, vous n'avez plus besoin de l'étendre.
- L'extension du schéma est une action irréversible, unique et à l'échelle de la forêt.
- Seul un utilisateur membre du groupe Administrateurs du schéma ou disposant d'autorisations suffisantes pour modifier le schéma peut étendre ce dernier.
- Bien que vous puissiez étendre le schéma avant ou après l'exécution du programme d'installation de Configuration Manager, nous vous conseillons d'étendre le schéma avant de commencer à configurer vos sites et vos paramètres de hiérarchie. Ce procédé simplifie la plupart des étapes de configuration ultérieures.
- Une fois le schéma étendu, le catalogue global Active Directory est répliqué dans toute la forêt. Ainsi, choisissez une période calme, afin de ne pas affecter d'autres processus dépendant du réseau :
  - Dans les forêts Windows 2000, l'extension du schéma entraîne une synchronisation complète du catalogue global.
  - À partir des forêts Windows 2003, seuls les attributs ajoutés récemment sont répliqués.

**Appareils et clients qui n'utilisent pas le schéma Active Directory :**

- Appareils mobiles gérés par le connecteur du serveur Exchange Server
- Client des ordinateurs Mac
- Client des serveurs Linux et UNIX
- Appareils mobiles inscrits par Configuration Manager
- Appareils mobiles inscrits par Microsoft Intune

- Clients d'appareil mobile hérités
- Clients Windows configurés pour être gérés uniquement via Internet
- Clients Windows détectés par Configuration Manager comme étant connectés à Internet

## Fonctionnalités qui bénéficient de l'extension du schéma

**Installation de l'ordinateur client et attribution de site** : quand un ordinateur Windows installe un nouveau client, ce dernier recherche des propriétés d'installation dans Active Directory Domain Services.

- **Solutions de contournement** : si vous n'étendez pas le schéma, utilisez l'une des options suivantes pour fournir les détails de configuration que les ordinateurs doivent installer :
  - **Utiliser l'installation poussée du client**. Avant d'utiliser une méthode d'installation du client, vérifiez que tous les prérequis sont remplis. Pour plus d'informations, consultez la section « Dépendances liées aux méthodes d'installation » dans Prérequis au déploiement de clients sur des ordinateurs Windows.
  - **Installer les clients manuellement** et fournir les propriétés d'installation du client en utilisant les propriétés de ligne de commande d'installation CCMSetup. Ces méthodes doivent inclure :
    - Spécifiez un point de gestion ou un chemin source à partir duquel l'ordinateur peut télécharger les fichiers d'installation en utilisant la propriété CCMSetup **/mp:<nom_ordinateur_nom_point_de_gestion>** ou **/source:<chemin_fichiers_sources_client>** sur la ligne de commande CCMSetup lors de l'installation du client.
    - Spécifiez une liste de points de gestion initiale pour le client pour qu'il puisse les attribuer au site et ensuite télécharger les paramètres de stratégie client et du site. Pour ce faire, utilisez la propriété CCMSetup Client.msi de SMSMP.
  - **Publier le point de gestion dans DNS ou WINS** et configurer des clients pour utiliser cette méthode d'emplacement de service.

**Configuration du port pour la communication client à serveur** : quand un client est installé, il est configuré avec les informations du port stockées dans Active Directory. Si vous modifiez ultérieurement le port de communication client à serveur pour un site, un client peut obtenir ce nouveau paramètre de port par les services de domaine Active Directory.

- **Solutions de contournement :** si vous n'étendez pas le schéma, utilisez l'une des options suivantes pour fournir de nouvelles configurations de port aux clients existants :
  - **Réinstaller les clients** à l'aide d'options qui configurent le nouveau port.
  - **Déployer sur les clients un script personnalisé qui met à jour les informations de port**. Si les clients ne peuvent pas communiquer avec un site en raison d'une modification du port, vous ne pouvez pas utiliser Configuration Manager pour déployer ce script. Vous pouvez par exemple utiliser la Stratégie de groupe.

**Scénarios de déploiement de contenu** : quand vous créez du contenu sur un site et que vous déployez ce contenu vers un autre site de la hiérarchie, le site récepteur doit être capable de vérifier la signature des données du contenu signé. Cela nécessite un accès à la clé publique du site source dans lequel vous créez ces données. Quand vous étendez le schéma Active Directory pour Configuration Manager, la clé publique d'un site est accessible à tous les sites de la hiérarchie.

- **Solutions de contournement :** si vous n'étendez pas le schéma, utilisez l'outil de maintenance de hiérarchie, **preinst.exe**, pour échanger les informations de la clé sécurisées entre les sites.

Par exemple, si vous envisagez de créer du contenu sur un site principal et le déployer sur un site secondaire inférieur à un site principal différent, vous devez soit étendre le schéma Active Directory pour permettre au site secondaire d'obtenir la clé publique de la source des sites principaux, soit utiliser preinst.exe pour partager les clés directement entre les deux sites.

## Classes et attributs Active Directory

Quand vous étendez le schéma pour System Center Configuration Manager, les classes et les attributs suivants sont ajoutés au schéma et sont accessibles à tous les sites Configuration Manager dans cette forêt Active Directory.

- Attributs :
  - cn=mS-SMS-Assignment-Site-Code
  - cn=mS-SMS-Capabilities
  - cn=MS-SMS-Default-MP
  - cn=mS-SMS-Device-Management-Point
  - cn=mS-SMS-Health-State
  - cn=MS-SMS-MP-Address
  - cn=MS-SMS-MP-Name
  - cn=MS-SMS-Ranged-IP-High
  - cn=MS-SMS-Ranged-IP-Low
  - cn=MS-SMS-Roaming-Boundaries
    sur
  - cn=MS-SMS-Site-Boundaries
  - cn=MS-SMS-Site-Code
  - cn=mS-SMS-Source-Forest
  - cn=mS-SMS-Version
- Classes :
  - cn=MS-SMS-Management-Point
  - cn=MS-SMS-Roaming-Boundary-Range
  - cn=MS-SMS-Server-Locator-Point
  - cn=MS-SMS-Site

> **NOTE**
>
> Les extensions de schéma peuvent inclure des attributs et des classes issus de versions précédentes du produit, qui ne sont plus utilisés par System Center Configuration Manager. Par exemple :
>
> - Attribut : cn=MS-SMS-Site-Boundaries
>   - Classe : cn=MS-SMS-Server-Locator-Point

Vous pouvez vous assurer que les listes précédentes sont à jour en consultant le fichier

**ConfigMgr_ad_schema.LDF**, situé dans le dossier **\SMSSETUP\BIN\x64** du support d'installation de System Center Configuration Manager.

# Préparer des serveurs Windows pour prendre en charge System Center Configuration Manager

22/06/2018 • 10 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Pour pouvoir l'utiliser comme serveur de site ou serveur de système de site pour System Center Configuration Manager, l'ordinateur doit remplir les conditions requises.

- Ces conditions incluent souvent un ou plusieurs rôles ou fonctionnalités Windows, qui sont activés à l'aide du Gestionnaire de serveur des ordinateurs.
- Étant donné que la méthode d'activation des rôles et fonctionnalités Windows varie selon les systèmes d'exploitation, consultez la documentation de votre système d'exploitation pour en savoir plus sur la configuration appropriée.

Les informations contenues dans cet article offrent une vue d'ensemble des différents types de configurations Windows nécessaires à la prise en charge des systèmes de site Configuration Manager. Pour plus d'informations sur la configuration de certains rôles de système de site, consultez Prérequis des sites et systèmes de site pour System Center Configuration Manager.

## Rôles et fonctionnalités Windows

Quand vous configurez des rôles et des fonctionnalités Windows sur un ordinateur, il se peut que vous deviez redémarrer l'ordinateur pour terminer la configuration. Il est donc judicieux d'identifier les ordinateurs qui hébergeront certains rôles de système de site avant d'installer un site ou un serveur de système de site Configuration Manager.

**Fonctionnalités**

Les fonctionnalités Windows suivantes sont nécessaires sur certains serveurs de système de site et doivent être configurées pour pouvoir installer un rôle de système de site sur cet ordinateur.

- **.NET Framework** : incluant
  - ASP.NET
  - Activation HTTP
  - Activation non-HTTP
  - Services WCF (Windows Communication Foundation)

  Différents rôles de système de site requièrent différentes versions de .NET Framework.

  Comme Microsoft .NET Framework 4.0 et les versions ultérieures n'offrent pas de compatibilité descendante pour remplacer les versions 3.5 et antérieures, si différentes versions sont requises, vous devez prévoir d'activer chaque version sur le même ordinateur.
- **Service de transfert intelligent en arrière-plan (BITS)** : les points de gestion ont besoin du service BITS (et des options sélectionnées automatiquement) pour prendre en charge la communication avec les appareils gérés.
- **BranchCache** : vous pouvez configurer les points de distribution avec BranchCache pour prendre en charge les clients qui utilisent cette fonctionnalité.
- **Déduplication des données** : vous pouvez configurer les points de distribution avec la déduplication des

données pour tirer parti de cette fonctionnalité.

- **Compression différentielle à distance (RDC)** : chaque ordinateur qui héberge un serveur de site ou un point de distribution a besoin de la compression différentielle à distance.
  Celle-ci est utilisée pour générer des signatures de package et effectuer des comparaisons de signatures.

**Rôles**

Les rôles Windows suivants sont requis pour prendre en charge des fonctionnalités spécifiques, telles que les mises à jour logicielles et les déploiements de système d'exploitation. IIS est requis par les principaux rôles de système de site.

- **Service d'inscription de périphérique réseau** (sous Services de certificats Active Directory) : ce rôle Windows est requis pour pouvoir utiliser des profils de certificat dans Configuration Manager.
- **Serveur web (IIS)**, avec notamment :
  - Fonctionnalités HTTP communes >
    - Redirection HTTP
  - Développement d'applications >
    - Extensibilité .NET
    - ASP.NET
    - Extensions ISAPI
    - Filtres ISAPI
  - Outils de gestion >
    - IIS 6 Management Compatibility
    - Compatibilité avec la métabase de données IIS 6
    - Compatibilité avec IIS 6 Windows Management Instrumentation (WMI)
  - Sécurité >
    - Filtrage des demandes
    - Authentification Windows

  Les rôles de système de site suivants utilisent une ou plusieurs des configurations IIS répertoriées :

  - Point de service web du catalogue des applications
  - Point du site web du catalogue des applications
  - Point de distribution
  - Point d'inscription
  - Point proxy d'inscription
  - Point d'état de secours
  - Point de gestion
  - Point de mise à jour logicielle
  - Point de migration d'état

  La version minimale d'IIS requise est la version fournie avec le système d'exploitation du serveur de site.

  En plus de ces configurations IIS, il se peut que vous deviez configurer le Filtrage des demandes IIS pour les points de distribution.

- **Services de déploiement Windows** : ce rôle est utilisé pour le déploiement de système d'exploitation.
- **Windows Server Update Services** : ce rôle est nécessaire pour le déploiement de mises à jour logicielles.

## Filtrage des demandes IIS pour les points de distribution

Par défaut, IIS utilise le filtrage des demandes pour bloquer l'accès par HTTP ou HTTPS à plusieurs extensions de

nom de fichier et emplacements de dossier. Sur un point de distribution, cela empêche les clients de télécharger des packages contenant des extensions ou des emplacements de dossier bloqués.

Si vos fichiers sources de package contiennent des extensions qui sont bloquées dans IIS par votre configuration de filtrage des demandes, vous devez les autoriser dans le filtrage des demandes. Pour cela, vous devez configurer le filtrage des demandes dans le Gestionnaire des services IIS sur vos ordinateurs de point de distribution.

Par ailleurs, Configuration Manager utilise les extensions de nom de fichier suivantes pour les packages et les applications. Vérifiez que vos configurations de filtrage des demandes ne bloquent pas les extensions de fichier suivantes :

- .PCK
- .PKG
- .STA
- .TAR

Par exemple, dans le cadre d'un déploiement logiciel, vous pouvez avoir des fichiers sources incluant un dossier nommé **bin** ou contenant un fichier avec l'extension **.mdb**.

- Par défaut, le filtrage des demandes IIS bloque l'accès à ces éléments (**bin** est bloqué en tant que segment masqué et **.mdb** est bloqué en tant qu'extension de nom de fichier).
- Quand vous utilisez la configuration IIS par défaut sur un point de distribution, les clients qui utilisent BITS ne peuvent pas télécharger ce déploiement logiciel à partir du point de distribution et indiquent qu'ils attendent du contenu.
- Pour permettre aux clients de télécharger ce contenu, sur chaque point de distribution applicable, modifiez l'option **Filtrage des demandes** dans le Gestionnaire des services IIS pour autoriser l'accès aux extensions de fichier et aux dossiers contenus dans les packages et applications que vous déployez.

> **IMPORTANT**
>
> Les modifications apportées au filtre de demande peuvent augmenter la surface exposée aux attaques de l'ordinateur.
>
> - Les modifications apportées au niveau du serveur s'appliquent à tous les sites web sur le serveur.
>   - Les modifications apportées à un site web particulier s'appliquent uniquement à ce site web.
>
>   La bonne pratique à suivre sur le plan de la sécurité consiste à exécuter Configuration Manager sur un serveur web dédié. Si vous devez exécuter d'autres applications sur le serveur web, utilisez un site web personnalisé pour Configuration Manager. Pour plus d'informations, consultez Sites web pour les serveurs de système de site dans System Center Configuration Manager.

## Verbes HTTP

**Points de gestion** : pour garantir une communication fonctionnelle entre les clients et un point de gestion, sur le serveur de point de gestion, vérifiez que les verbes HTTP suivants sont autorisés :

- GET
- POST
- CCM_POST
- HEAD
- PROPFIND

**Points de distribution** : les points de distribution exigent l'autorisation des verbes HTTP suivants :

- GET

- HEAD
- PROPFIND

Pour plus d'informations sur la configuration du filtrage des demandes, consultez Configurer le filtrage des demandes dans IIS sur TechNet ou une documentation similaire applicable à la version de Windows Server qui héberge votre point de gestion.

# Sites web pour les serveurs de système de site dans System Center Configuration Manager

22/06/2018 • 10 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Plusieurs rôles de système de site Configuration Manager nécessitent l'utilisation de Microsoft Internet Information Services (IIS) et utilisent le site web IIS par défaut pour héberger les services du système de site. Si vous devez exécuter d'autres applications web sur le même serveur et que les paramètres ne sont pas compatibles avec Configuration Manager, utilisez plutôt un site web personnalisé pour Configuration Manager.

> **TIP**
> Une bonne pratique en matière de sécurité consiste à dédier un serveur aux systèmes de site Configuration Manager nécessitant IIS. Quand vous exécutez d'autres applications sur un système de site Configuration Manager, vous augmentez la surface exposée aux attaques de cet ordinateur.

## Informations à connaître avant d'utiliser des sites web personnalisés

Par défaut, les rôles de système de site utilisent le **site web par défaut** dans IIS. Ceci est automatiquement configuré lors de l'installation du rôle de système de site. Toutefois, sur les sites principaux, vous pouvez choisir d'utiliser des sites web personnalisés à la place. Quand vous utilisez des sites web personnalisés :

- Les sites web personnalisés sont activés pour l'ensemble du site, et non pas individuellement pour des serveurs ou rôles du système de site.
- Sur les sites principaux, chaque ordinateur qui hébergera un rôle de système de site applicable doit être configuré avec un site web personnalisé nommé **SMSWEB**. Tant que ce site web n'aura pas été créé et que les rôles de système de site sur l'ordinateur n'auront pas été configurés pour utiliser le site web personnalisé, les clients ne pourront peut-être pas communiquer avec les rôles de système de site sur cet ordinateur.
- Du fait que les sites secondaires sont automatiquement configurés pour utiliser un site web personnalisé quand leur site parent principal est configuré pour cela, vous devez également créer des sites web personnalisés dans IIS sur chaque serveur de système de site secondaire qui nécessite IIS.

**Configuration requise pour l'utilisation de sites web personnalisés :**

Avant d'activer l'option pour utiliser des sites web personnalisés sur un site, vous devez effectuer les opérations suivantes :

- Créez un site web personnalisé nommé **SMSWEB** dans IIS sur chaque serveur de système de site qui nécessite les services IIS. Effectuez cette opération sur le site principal et sur tous les sites secondaires enfants.
- Configurez le site web personnalisé pour répondre sur le même port que celui configuré pour la communication client Configuration Manager (port de demande client).
- Pour chaque site web personnalisé ou site web par défaut qui utilise un dossier personnalisé, placez une copie du type de document par défaut que vous utilisez dans le dossier racine qui héberge le site web. Par exemple, sur un ordinateur Windows Server 2008 R2 avec des configurations par défaut, **iisstart.htm** est

l'un des types de documents par défaut disponibles. Ce fichier se trouve à la racine du site web par défaut. Vous pouvez en placer une copie (ou une copie du type de document par défaut que vous utilisez) dans le dossier racine qui héberge le site web personnalisé SMSWEB. Pour plus d'informations sur les types de documents par défaut, consultez Document par défaut <defaultDocument> pour IIS.

**À propos de la configuration requise pour IIS : Les rôles de système de site suivants nécessitent IIS et un site web pour héberger les services de système de site :**

- Point de service web du catalogue des applications
- Point du site web du catalogue des applications
- Point de distribution
- Point d'inscription
- Point proxy d'inscription
- Point d'état de secours
- Point de gestion
- Point de mise à jour logicielle
- Point de migration d'état

Autres éléments à prendre en considération

- Quand un site principal comporte des sites web personnalisés activés, les clients attribués à ce site sont configurés pour communiquer avec les sites web personnalisés plutôt qu'avec les sites web par défaut sur les serveurs de système de site concernés.
- Si vous activez des sites web personnalisés pour un site principal, envisagez d'utiliser des sites web personnalisés pour tous les sites principaux de votre hiérarchie afin d'assurer la bonne itinérance des clients dans la hiérarchie. (L'itinérance désigne le déplacement d'un ordinateur client vers un nouveau segment de réseau qui est géré par un autre site. L'itinérance peut avoir une incidence sur les ressources auxquelles un client peut accéder localement au lieu d'y accéder sur une liaison WAN).
- Les rôles de système de site qui utilisent les services IIS mais n'acceptent pas les connexions clientes, comme le point de Reporting Services, utilisent également le site web SMSWEB au lieu du site web par défaut.
- Les sites web personnalisés vous permettent d'attribuer des numéros de port différents de ceux utilisés par le site web par défaut des ordinateurs. Un site web par défaut et le site web personnalisé ne peuvent pas s'exécuter simultanément s'ils tentent tous les deux d'utiliser les mêmes ports TCP/IP.
- Les ports TCP/IP que vous configurez dans IIS pour le site web personnalisé doivent correspondre aux ports de demande client pour le site.

## Basculer entre un site web par défaut et un site web personnalisé

Vous pouvez cocher ou décocher la case relative à l'utilisation de sites web personnalisés sur un site principal à tout moment (la case à cocher se trouve sous l'onglet Général des propriétés des sites), mais effectuez cette modification avec prudence. Si cette configuration est modifiée, tous les rôles de système de site applicables sur le site principal et sur les sites secondaires enfants doivent être désinstallés, puis réinstallés :

Les rôles suivants sont **réinstallés automatiquement**:

- Point de gestion

- Point de distribution
- Point de mise à jour logicielle
- Point d'état de secours
- Point de migration d'état

Les rôles suivants doivent être **réinstallés manuellement**:

- Point de service web du catalogue des applications
- Point du site web du catalogue des applications
- Point d'inscription
- Point proxy d'inscription

En outre :

- Quand vous utilisez un site web personnalisé à la place du site web par défaut, Configuration Manager ne supprime pas les anciens répertoires virtuels. Si vous souhaitez supprimer les fichiers utilisés par Configuration Manager, vous devez supprimer manuellement les répertoires virtuels créés sous le site web par défaut.
- Si vous modifiez le site pour utiliser des sites web personnalisés, les clients qui sont déjà attribués au site doivent ensuite être reconfigurés pour utiliser les nouveaux ports de demande client pour les sites web personnalisés. Consultez Guide pratique pour configurer les ports de communication des clients dans System Center Configuration Manager.

## Configurer des sites web personnalisés

Du fait que les procédures de création d'un site web personnalisé varient selon la version du système d'exploitation, reportez-vous à la documentation de votre version de système d'exploitation pour connaître les procédures exactes à suivre. Toutefois, suivez les indications ci-dessous, le cas échéant :

- Le site web doit être appelé **SMSWEB**.
- Si vous configurez le protocole HTTPS, vous devez spécifier un certificat SSL pour pouvoir enregistrer la configuration.
- Après avoir créé le site web personnalisé, supprimez les ports de sites web personnalisés que vous utilisez à partir d'autres sites web dans IIS :

  1. Modifiez les **liaisons** des autres sites web pour supprimer les ports qui correspondent à ceux attribués au site web **SMSWEB**.
  2. Démarrez le site web **SMSWEB**.
  3. Redémarrez le service **SMS_SITE_COMPONENT_MANAGER** sur le serveur de site du site.

# Configuration requise des certificats PKI pour System Center Configuration Manager

10/07/2018 • 42 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les certificats d'infrastructure à clé publique (PKI) dont vous pouvez avoir besoin pour System Center Configuration Manager sont répertoriés dans les tableaux suivants. Ces informations présupposent une connaissance élémentaire des certificats PKI. Pour obtenir des instructions pas à pas pour le déploiement, consultez Exemple détaillé de déploiement des certificats PKI pour Configuration Manager : Autorité de certification Windows Server 2008.

Pour plus d'informations sur les services de certificats Active Directory, consultez la documentation suivante :

- Pour Windows Server 2012 : Vue d'ensemble des services de certificats Active Directory
- Pour Windows Server 2008 : Services de certificats Active Directory dans Windows Server 2008

Pour plus d'informations sur l'utilisation des certificats Cryptography API : Next Generation (CNG) avec Configuration Manager, consultez Vue d'ensemble des certificats CNG.

> **IMPORTANT**
> System Center Configuration Manager prend en charge les certificats (SHA-2) (Secure Hash Algorithm 2). Les certificats SHA-2 apportent un avantage important en termes de sécurité. Par conséquent, nous vous recommandons ce qui suit :
>
> - Émettez de nouveaux certificats d'authentification serveur et client signés avec SHA-2 (qui inclut entre autres SHA-256 et SHA-512).
> - Tous les services doivent utiliser un certificat SHA-2. Par exemple, si vous achetez un certificat public pour une utilisation avec une passerelle de gestion cloud, vérifiez qu'il s'agit d'un certificat SHA-2.
>
> À compter du 14 février 2017, Windows ne fait plus confiance à certains certificats signés avec SHA-1. En général, nous vous recommandons d'émettre de nouveaux certificats d'authentification serveur et client signés avec SHA-2 (qui inclut entre autres SHA-256 et SHA-512). Nous vous recommandons aussi d'utiliser un certificat SHA-2 pour tout service Internet. Par exemple, si vous achetez un certificat public pour une utilisation avec une passerelle de gestion cloud, vérifiez qu'il s'agit d'un certificat SHA-2.»
>
> Dans la plupart des cas, le passage à des certificats SHA-2 n'a pas d'impact sur les opérations. Pour plus d'informations, consultez cet article sur l'application Windows des certificats SHA1.

À l'exception des certificats clients inscrits par System Center Configuration Manager sur les appareils mobiles et les ordinateurs Mac, des certificats créés automatiquement par Windows Intune pour la gestion des appareils mobiles et des certificats installés par System Center Configuration Manager sur les ordinateurs AMT, vous pouvez utiliser n'importe quelle infrastructure PKI pour créer, déployer et gérer les certificats suivants. Toutefois, lorsque vous utilisez des services de certificats Active Directory et des modèles de certificat, cette solution d'infrastructure à clé publique Microsoft peut faciliter la gestion des certificats. Utilisez la colonne **Modèle de certificat Microsoft à utiliser** des tableaux ci-dessous pour identifier le modèle de certificat qui correspond le plus aux spécifications du certificat. Seule une autorité de certification d'entreprise exécutée sur l'édition Enterprise ou Datacenter du système d'exploitation serveur, par exemple Windows Server 2008 Enterprise et Windows Server 2008 Datacenter, peut utiliser des certificats basés sur des modèles.

**IMPORTANT**

Lorsque vous utilisez une autorité de certification d'entreprise et des modèles de certificats, n'utilisez pas les modèles de la version 3. Ces modèles de certificat créent des certificats incompatibles avec System Center Configuration Manager. Utilisez plutôt les modèles de la version 2 en suivant les instructions suivantes :

- Pour une autorité de certification sur Windows Server 2012 : sous l'onglet **Compatibilité** des propriétés du modèle de certificat, spécifiez **Windows Server 2003** pour l'option **Autorité de certification** et **Windows XP/Server 2003** pour l'option **Destinataire du certificat** .
  - Pour une autorité de certification sur Windows Server 2008 : quand vous dupliquez un modèle de certificat, conservez la sélection par défaut de **Windows Server 2003 Enterprise** quand vous y êtes invité par la boîte de dialogue **Dupliquer le modèle**. Ne sélectionnez pas **Windows Server 2008, Enterprise Edition**.

Utilisez les sections suivantes pour afficher les spécifications du certificat.

## Certificats PKI pour serveurs

| COMPOSANT SYSTEM CENTER CONFIGURATION MANAGER | RÔLE DU CERTIFICAT | MODÈLE DE CERTIFICAT MICROSOFT À UTILISER | INFORMATIONS SPÉCIFIQUES DU CERTIFICAT | MODE D'UTILISATION DU CERTIFICAT DANS SYSTEM CENTER CONFIGURATION MANAGER |
|---|---|---|---|---|
| Systèmes de site qui exécutent Internet Information Services (IIS) et qui sont configurés pour les connexions clientes HTTPS :<br><br>• Point de gestion<br>• Point de distribution<br>• Point de mise à jour logicielle<br>• Point de migration d'état<br>• Point d'inscription<br>• Point proxy d'inscription<br>• Point de service web du catalogue des applications<br>• Point du site web du catalogue des applications<br>• Point d'enregistrement de certificat | Authentification du serveur | **Serveur Web** | **Utilisation avancée de la clé** : la valeur de ce paramètre doit contenir **Authentification du serveur (1.3.6.1.5.5.7.3.1)**.<br><br>Si le système du site accepte les connexions en provenance d'Internet, Nom d'objet ou Autre nom de l'objet doit correspondre au nom de domaine Internet complet (FQDN).<br><br>Si le système de site accepte les connexions en provenance de l'intranet, Nom d'objet ou Autre nom de l'objet doit correspondre soit au nom de domaine complet de l'intranet (recommandé), soit au nom de l'ordinateur, selon la configuration du système de site.<br><br>Si le système de site accepte les connexions | Ce certificat doit se trouver dans le magasin personnel du magasin de certificats de l'ordinateur.<br><br>Ce certificat de serveur web est utilisé pour authentifier ces serveurs sur le client et pour chiffrer toutes les données transférées entre le client et ces serveurs à l'aide du protocole SSL (Secure Sockets Layer). |

| COMPOSANT SYSTEM CENTER CONFIGURATION MANAGER | RÔLE DU CERTIFICAT | MODÈLE DE CERTIFICAT MICROSOFT À UTILISER | INFORMATIONS SPÉCIFIQUES DU CERTIFICAT | MODE D'UTILISATION DU CERTIFICAT DANS SYSTEM CENTER CONFIGURATION MANAGER |
|---|---|---|---|---|
| | | | entrantes Internet et intranet, il est nécessaire de spécifier le nom de domaine Internet complet et le nom de domaine complet de l'intranet (ou le nom de l'ordinateur) en les séparant par une esperluette (&.<br><br>**Remarque** : quand le point de mise à jour logicielle accepte des connexions client uniquement à partir d'Internet, le certificat doit contenir à la fois le nom de domaine complet (FQDN) Internet et le nom de domaine complet (FQDN) intranet.<br><br>L'algorithme de hachage SHA-2 est pris en charge.<br><br>System Center Configuration Manager ne spécifie pas de longueur de clé maximale prise en charge pour ce certificat. Pour tout problème lié à la taille de clé pour ce certificat, consultez votre PKI et la documentation IIS. | |

| COMPOSANT SYSTEM CENTER CONFIGURATION MANAGER | RÔLE DU CERTIFICAT | MODÈLE DE CERTIFICAT MICROSOFT À UTILISER | INFORMATIONS SPÉCIFIQUES DU CERTIFICAT | MODE D'UTILISATION DU CERTIFICAT DANS SYSTEM CENTER CONFIGURATION MANAGER |
|---|---|---|---|---|
| Point de distribution cloud | Authentification du serveur | **Serveur Web** | **Utilisation avancée de la clé** : la valeur de ce paramètre doit contenir **Authentification du serveur (1.3.6.1.5.5.7.3.1)**.<br><br>Le nom d'objet doit contenir un nom de service défini par le client et un nom de domaine sous forme de nom de domaine complet, servant de nom commun pour l'instance spécifique du point de distribution cloud.<br><br>La clé privée doit être exportable.<br><br>L'algorithme de hachage SHA-2 est pris en charge.<br><br>Longueurs de clé prises en charge : 2 048 bits. | Ce certificat de service permet d'authentifier le service du point de distribution cloud auprès des clients Configuration Manager et de chiffrer l'intégralité des données transférées entre ces clients par le biais du protocole SSL (Secure Sockets Layer). Ce certificat doit être exporté au format Public Key Certificate Standard (PKCS #12), et le mot de passe doit être connu, de sorte qu'il puisse être importé lors de la création d'un point de distribution cloud.<br><br>**Remarque :** ce certificat est utilisé conjointement avec le certificat de gestion Windows Azure. |
| serveurs de système de site exécutant Microsoft SQL Server | Authentification du serveur | **Web server** | **Utilisation avancée de la clé** : la valeur de ce paramètre doit contenir **Authentification du serveur (1.3.6.1.5.5.7.3.1)**.<br><br>Le nom du sujet doit contenir le nom de domaine complet (FQDN) de l'intranet.<br><br>L'algorithme de hachage SHA-2 est pris en charge.<br><br>La longueur maximale de la clé est de 2 048 bits. | Ce certificat doit se trouver dans le magasin personnel du magasin de certificats de l'ordinateur. System Center Configuration Manager le copie automatiquement dans le magasin des personnes autorisées pour les serveurs de la hiérarchie System Center Configuration Manager qui peuvent avoir besoin d'établir une relation de confiance avec le serveur.<br><br>Ces certificats sont utilisés pour l'authentification de serveur à serveur. |

| COMPOSANT SYSTEM CENTER CONFIGURATION MANAGER | RÔLE DU CERTIFICAT | MODÈLE DE CERTIFICAT MICROSOFT À UTILISER | INFORMATIONS SPÉCIFIQUES DU CERTIFICAT | MODE D'UTILISATION DU CERTIFICAT DANS SYSTEM CENTER CONFIGURATION MANAGER |
|---|---|---|---|---|
| Cluster SQL Server : serveurs de système de site exécutant Microsoft SQL Server | Authentification du serveur | **Web server** | **Utilisation avancée de la clé** : la valeur de ce paramètre doit contenir **Authentification du serveur (1.3.6.1.5.5.7.3.1)**.<br><br>Le nom d'objet doit contenir le nom de domaine complet (FQDN) de l'intranet du cluster.<br><br>La clé privée doit être exportable.<br><br>Le certificat doit avoir une période de validité d'au moins deux ans quand vous configurez System Center Configuration Manager de sorte qu'il utilise le cluster SQL Server.<br><br>L'algorithme de hachage SHA-2 est pris en charge.<br><br>La longueur maximale de la clé est de 2 048 bits. | Après avoir demandé et installé ce certificat sur un nœud du cluster, exportez le certificat et importez-le dans les autres nœuds du cluster SQL Server.<br><br>Ce certificat doit se trouver dans le magasin personnel du magasin de certificats de l'ordinateur. System Center Configuration Manager le copie automatiquement dans le magasin des personnes autorisées pour les serveurs de la hiérarchie System Center Configuration Manager qui peuvent avoir besoin d'établir une relation de confiance avec le serveur.<br><br>Ces certificats sont utilisés pour l'authentification de serveur à serveur. |

| COMPOSANT SYSTEM CENTER CONFIGURATION MANAGER | RÔLE DU CERTIFICAT | MODÈLE DE CERTIFICAT MICROSOFT À UTILISER | INFORMATIONS SPÉCIFIQUES DU CERTIFICAT | MODE D'UTILISATION DU CERTIFICAT DANS SYSTEM CENTER CONFIGURATION MANAGER |
|---|---|---|---|---|
| Surveillance de système de site pour les rôles de système de site suivants :<br><br>• Point de gestion<br>• Point de migration d'état | Authentification du client | **Authentification de station de travail** | **Utilisation avancée de la clé** : la valeur de ce paramètre doit contenir **Authentification du client (1.3.6.1.5.5.7.3.2)**.<br><br>Les ordinateurs doivent présenter une valeur unique dans les champs Nom de l'objet ou Autre nom de l'objet.<br><br>**Remarque :** si vous indiquez plusieurs valeurs pour Autre nom de l'objet, seule la première est utilisée.<br><br>L'algorithme de hachage SHA-2 est pris en charge.<br><br>La longueur maximale de la clé est de 2 048 bits. | Ce certificat est requis sur les serveurs de système de site répertoriés, même si le client System Center Configuration Manager n'est pas installé. Cette configuration permet de surveiller et de signaler au site l'intégrité de ces rôles de système de site.<br><br>Le certificat de ces systèmes de site doit se trouver dans le magasin personnel du magasin de certificats de l'ordinateur. |

| COMPOSANT SYSTEM CENTER CONFIGURATION MANAGER | RÔLE DU CERTIFICAT | MODÈLE DE CERTIFICAT MICROSOFT À UTILISER | INFORMATIONS SPÉCIFIQUES DU CERTIFICAT | MODE D'UTILISATION DU CERTIFICAT DANS SYSTEM CENTER CONFIGURATION MANAGER |
|---|---|---|---|---|
| Serveurs exécutant le module de stratégie System Center Configuration Manager avec le service de rôle du Service d'inscription de périphérique réseau. | Authentification du client | **Authentification de station de travail** | **Utilisation avancée de la clé** : la valeur de ce paramètre doit contenir **Authentification du client (1.3.6.1.5.5.7.3.2)**.<br><br>Il n'existe aucune exigence particulière pour l'objet du certificat ou l'autre nom de l'objet. Vous pouvez utiliser le même certificat pour plusieurs serveurs exécutant le service d'inscription de périphérique réseau.<br><br>Les algorithmes de hachage SHA-2 et SHA-3 sont pris en charge.<br><br>Longueurs de clé prises en charge : 1 024 bits et 2 048 bits. | |
| Systèmes de site ayant un point de distribution installé | Authentification du client | **Authentification de station de travail** | **Utilisation avancée de la clé** : la valeur de ce paramètre doit contenir **Authentification du client (1.3.6.1.5.5.7.3.2)**.<br><br>Il n'existe aucune exigence particulière pour l'objet du certificat ou l'autre nom de l'objet. Vous pouvez utiliser le même certificat pour plusieurs points de distribution. Toutefois, nous vous recommandons d'utiliser un certificat différent pour chaque point de distribution.<br><br>La clé privée doit être exportable.<br><br>L'algorithme de hachage SHA-2 est | Ce certificat a deux objectifs :<br><br>• Il authentifie le point de distribution sur un point de gestion HTTPS avant que le point de distribution n'envoie des messages d'état.<br>• Lorsque l'option de point de distribution **Activer la prise en charge PXE pour les clients** est activée, le certificat est envoyé aux ordinateurs. |

| COMPOSANT SYSTEM CENTER CONFIGURATION MANAGER | RÔLE DU CERTIFICAT | MODÈLE DE CERTIFICAT MICROSOFT À UTILISER | INFORMATIONS SPÉCIFIQUES DU CERTIFICAT | MODE D'UTILISATION DU CERTIFICAT DANS SYSTEM CENTER CONFIGURATION MANAGER |
|---|---|---|---|---|
| | | | pris en charge.<br><br>La longueur maximale de la clé est de 2 048 bits. | Si des séquences de tâches du processus de déploiement du système d'exploitation comportent des actions du client, comme la récupération de la stratégie client ou l'envoi d'informations d'inventaire, les ordinateurs clients peuvent se connecter à un point de gestion HTTPS pendant le déploiement du système d'exploitation.<br><br>Ce certificat n'est utilisé que pour la durée de la procédure de déploiement du système d'exploitation et n'est pas installé sur le client. En raison de cette utilisation temporaire, le même certificat peut être utilisé pour chaque déploiement du système d'exploitation si vous ne souhaitez pas utiliser plusieurs certificats de client.<br><br>Le certificat doit être exporté au format Public Key Certificate Standard (PKCS #12). Le mot de passe doit être connu, de sorte qu'il puisse être importé dans les propriétés du point de distribution.<br><br>**Remarque :** la configuration requise pour ce certificat est |

| COMPOSANT SYSTEM CENTER CONFIGURATION MANAGER | RÔLE DU CERTIFICAT | MODÈLE DE CERTIFICAT MICROSOFT À UTILISER | INFORMATIONS SPÉCIFIQUES DU CERTIFICAT | MODE D'UTILISATION DU CERTIFICAT DANS SYSTEM CENTER CONFIGURATION MANAGER |
|---|---|---|---|---|
| | | | | la même que celle du certificat client des images de déploiement de systèmes d'exploitation. Dans la mesure où les exigences sont les mêmes, vous pouvez utiliser le même fichier de certificat. |
| Point du service hors bande | Préparation AMT | **Serveur web** (modifié) | La valeur**Utilisation avancée de la clé** doit contenir **Authentification du serveur (1.3.6.1.5.5.7.3.1)** et l'identificateur d'objet suivant : **2.16.840.1.113741.1.2.3**.<br><br>Le champ Nom de l'objet doit contenir le nom de domaine complet du serveur qui héberge le point de gestion hors bande.<br><br>**Remarque :** un certificat de configuration AMT que vous demandez à partir d'une autorité de certification externe plutôt qu'à partir de votre propre autorité de certification interne ne prend peut-être pas en charge l'identificateur d'objet de configuration AMT 2.16.840.1.113741.1.2.3. Vous pouvez également spécifier la chaîne de texte suivante en tant qu'attribut d'unité d'organisation dans le nom du sujet du certificat : **Intel(R) Client Setup Certificate**. Vous devez utiliser cette chaîne exacte de texte en anglais, en respectant la casse et sans point final et l'ajouter au nom de domaine complet du | Ce certificat se trouve dans le magasin personnel du magasin de certificats de l'ordinateur du serveur de système de site du point de service hors bande.<br><br>Ce certificat de configuration AMT permet de préparer les ordinateurs pour la gestion hors bande.<br><br>Vous devez demander ce certificat auprès d'une autorité de certification fournissant des certificats de configuration AMT. De plus, l'extension BIOS des ordinateurs basés sur AMT doit être configurée pour utiliser l'empreinte numérique de certificat racine (on parle également de « hachage de certificat ») de ce certificat de configuration.<br><br>VeriSign est un exemple type d'autorité de certification externe, fournissant des certificats de configuration AMT, mais vous pouvez également utiliser votre propre autorité de certification interne.<br><br>Installez le certificat sur le serveur |

| COMPOSANT SYSTEM CENTER CONFIGURATION MANAGER | RÔLE DU CERTIFICAT | MODÈLE DE CERTIFICAT MICROSOFT À UTILISER | INFORMATIONS SPÉCIFIQUES DU CERTIFICAT | MODE D'UTILISATION DU CERTIFICAT DANS SYSTEM CENTER CONFIGURATION MANAGER |
|---|---|---|---|---|
| | | | domaine complet du serveur qui héberge le point de service hors bande<br>Longueurs de clé prises en charge : 1 024 et 2 048. Pour AMT 6.0 et versions ultérieures, la longueur de clé de 4 096 bits est également prise en charge. | hébergeant le point de service hors bande qui doit être configuré correctement à l'autorité de certification racine du certificat. (Par défaut, le certificat de l'autorité de certification racine et le certificat de l'autorité de certification intermédiaire de VeriSign sont installés lors de l'installation de Windows.) |
| Serveur de système de site exécutant le connecteur Microsoft Intune | Authentification du client | Non applicable : Intune crée automatiquement ce certificat. | La valeur **Utilisation avancée de la clé** doit contenir **Authentification du client (1.3.6.1.5.5.7.3.2)**.<br><br>Trois extensions personnalisées identifient de manière unique l'abonnement Intune du client.<br><br>La taille de la clé est de 2 048 bits et elle utilise l'algorithme de hachage SHA-1.<br><br>**Remarque :** vous ne pouvez pas modifier ces paramètres. ces informations sont fournies uniquement à titre d'information. | Ce certificat est demandé et installé automatiquement dans la base de données de Configuration Manager quand vous vous abonnez à Microsoft Intune. Quand vous installez le connecteur Microsoft Intune, ce certificat est ensuite installé sur le serveur de système de site qui exécute le connecteur Microsoft Intune. Il est installé dans le magasin de certificats de l'ordinateur.<br><br>Ce certificat est utilisé pour authentifier la hiérarchie Configuration Manager auprès de Microsoft Intune à l'aide du connecteur Microsoft Intune. Toutes les données ainsi transférées utilisent le protocole SSL (Secure Sockets Layer). |

**Serveurs web proxy pour la gestion du client basée sur Internet**

Si le site prend en charge la gestion des clients basés sur Internet et que vous utilisez un serveur Web proxy avec terminaison SSL (pontage) pour les connexions Internet entrantes, le serveur Web proxy exige les certificats répertoriés dans le tableau suivant.

> **NOTE**
> Si vous utilisez un serveur Web proxy sans terminaison SSL (tunnel), aucun autre certificat n'est requis sur le serveur Web proxy.

| COMPOSANT D'INFRASTRUCTURE RÉSEAU | RÔLE DU CERTIFICAT | MODÈLE DE CERTIFICAT MICROSOFT À UTILISER | INFORMATIONS SPÉCIFIQUES DU CERTIFICAT | MODE D'UTILISATION DU CERTIFICAT DANS SYSTEM CENTER CONFIGURATION MANAGER |
|---|---|---|---|---|
| Serveur Web proxy acceptant les connexions de clients sur Internet | Authentification de serveur et authentification de client | 1. **Serveur Web**<br><br>2. **Authentification de station de travail** | Nom de domaine complet Internet dans le champ Nom de l'objet ou Autre nom de l'objet : Si vous utilisez des modèles de certificats Microsoft, l'autre nom de l'objet n'est disponible qu'avec le modèle pour station de travail.<br><br>L'algorithme de hachage SHA-2 est pris en charge. | Ce certificat est utilisé pour authentifier les serveurs suivants auprès de clients Internet et pour crypter toutes les données transférées entre le client et ce serveur en utilisant le protocole SSL :<br><br>• Point de gestion Internet<br>• Point de distribution basé sur Internet<br>• point de mise à jour logicielle Internet<br><br>L'authentification client est utilisée pour ponter les connexions client entre les clients System Center Configuration Manager et les systèmes de site basés sur Internet. |

## Certificats PKI pour les clients

| COMPOSANT SYSTEM CENTER CONFIGURATION MANAGER | RÔLE DU CERTIFICAT | MODÈLE DE CERTIFICAT MICROSOFT À UTILISER | INFORMATIONS SPÉCIFIQUES DU CERTIFICAT | MODE D'UTILISATION DU CERTIFICAT DANS SYSTEM CENTER CONFIGURATION MANAGER |
|---|---|---|---|---|

| COMPOSANT SYSTEM CENTER CONFIGURATION MANAGER | RÔLE DU CERTIFICAT | MODÈLE DE CERTIFICAT MICROSOFT À UTILISER | INFORMATIONS SPÉCIFIQUES DU CERTIFICAT | MODE D'UTILISATION DU CERTIFICAT DANS SYSTEM CENTER CONFIGURATION MANAGER |
|---|---|---|---|---|
| Ordinateurs clients Windows | Authentification du client | **Authentification de station de travail** | **Utilisation avancée de la clé** : la valeur de ce paramètre doit contenir **Authentification du client (1.3.6.1.5.5.7.3.2)**.<br><br>Les ordinateurs clients doivent présenter une valeur unique dans les champs Nom de l'objet ou Autre nom de l'objet.<br><br>**Remarque :** si vous indiquez plusieurs valeurs pour Autre nom de l'objet, seule la première est utilisée.<br><br>L'algorithme de hachage SHA-2 est pris en charge.<br><br>La longueur maximale de la clé est de 2 048 bits. | Par défaut, System Center Configuration Manager recherche des certificats d'ordinateur dans le magasin personnel du magasin de certificats d'ordinateur.<br><br>À l'exception du point de mise à jour logicielle et du point de site web du catalogue des applications, ce certificat authentifie le client auprès de serveurs de système de site qui exécutent IIS et qui sont configurés pour utiliser le protocole HTTPS. |

| COMPOSANT SYSTEM CENTER CONFIGURATION MANAGER | RÔLE DU CERTIFICAT | MODÈLE DE CERTIFICAT MICROSOFT À UTILISER | INFORMATIONS SPÉCIFIQUES DU CERTIFICAT | MODE D'UTILISATION DU CERTIFICAT DANS SYSTEM CENTER CONFIGURATION MANAGER |
|---|---|---|---|---|
| clients d'appareils mobiles | Authentification du client | **Session authentifiée** | **Utilisation avancée de la clé** : la valeur de ce paramètre doit contenir **Authentification du client (1.3.6.1.5.5.7.3.2)**.<br><br>SHA-1<br><br>La longueur maximale de la clé est de 2 048 bits.<br><br>**Remarques** :<br><br>• Ces certificats doivent être au format binaire codé DER X.509.<br>• Le format X.509 codé en Base64 n'est pas pris en charge. | Ce certificat authentifie le client de l'appareil mobile auprès des serveurs de système de site avec lesquels il communique, tels que les points de gestion et les points de distribution. |
| Images de démarrage pour le déploiement de systèmes d'exploitation | Authentification du client | **Authentification de station de travail** | **Utilisation avancée de la clé** : la valeur de ce paramètre doit contenir **Authentification du client (1.3.6.1.5.5.7.3.2)**.<br><br>Aucune configuration spécifique n'est requise pour le champ Nom de l'objet ou Autre nom de l'objet (SAN) du certificat, et vous pouvez utiliser le même certificat pour toutes les images de démarrage.<br><br>La clé privée doit être exportable.<br><br>L'algorithme de hachage SHA-2 est pris en charge.<br><br>La longueur maximale de la clé | Le certificat est utilisé si les séquences des tâches dans la procédure du déploiement du système d'exploitation comprennent des actions du client telles que la récupération de la stratégie du client ou l'envoi des données d'inventaire.<br><br>Ce certificat n'est utilisé que pour la durée de la procédure de déploiement du système d'exploitation et n'est pas installé sur le client. En raison de cette utilisation temporaire, le même certificat peut être utilisé pour chaque déploiement du |

| COMPOSANT SYSTEM CENTER CONFIGURATION MANAGER | RÔLE DU CERTIFICAT | MODÈLE DE CERTIFICAT MICROSOFT À UTILISER | INFORMATIONS SPÉCIFIQUES DU CERTIFICAT | MODE D'UTILISATION DU CERTIFICAT DANS SYSTEM CENTER CONFIGURATION MANAGER |
| --- | --- | --- | --- | --- |
| | | | est de 2 048 bits.<br><br>système d'exploitation si vous ne souhaitez pas utiliser HTTPS. | certificats de client. |
| | | | | Ce certificat doit être exporté au format Public Key Certificate Standard (PKCS #12), et le mot de passe doit être connu, de sorte qu'il puisse être importé dans les images de démarrage de System Center Configuration Manager.<br><br>Ce certificat est temporaire pour la séquence de tâches et n'est pas utilisé pour installer le client. Lorsque vous avez un environnement avec HTTPS uniquement, le client doit avoir un certificat valide pour communiquer avec le site et pour que le déploiement continue. Le client peut générer automatiquement un certificat quand il est joint à Active Directory, ou vous pouvez installer un certificat client à l'aide d'une autre méthode.<br><br>**Remarque :** la configuration requise pour ce certificat est la même que celle du certificat du serveur pour les systèmes de site ayant un point de distribution installé. Dans la mesure où les exigences sont les mêmes, vous pouvez utiliser le même fichier de certificat. |

| COMPOSANT SYSTEM CENTER CONFIGURATION MANAGER | RÔLE DU CERTIFICAT | MODÈLE DE CERTIFICAT MICROSOFT À UTILISER | INFORMATIONS SPÉCIFIQUES DU CERTIFICAT | MODE D'UTILISATION DU CERTIFICAT DANS SYSTEM CENTER CONFIGURATION MANAGER |
|---|---|---|---|---|
| Ordinateurs clients Mac | Authentification du client | Pour l'inscription System Center Configuration Manager : **Session authentifiée**<br><br>Pour une installation de certificat indépendante de System Center Configuration Manager : **Authentification de station de travail** | **Utilisation avancée de la clé** : la valeur de ce paramètre doit contenir **Authentification du client (1.3.6.1.5.5.7.3.2)**.<br><br>Si System Center Configuration Manager crée un certificat utilisateur, la valeur Objet du certificat est renseignée automatiquement en utilisant le nom d'utilisateur de la personne qui inscrit l'ordinateur Mac.<br><br>Dans le cas d'une installation de certificat qui n'utilise pas l'inscription System Center Configuration Manager, mais qui déploie un certificat d'ordinateur indépendamment de System Center Configuration Manager, la valeur Objet du certificat doit être unique. Indiquez par exemple le nom de domaine complet de l'ordinateur.<br><br>Le champ Autre nom de l'objet n'est pas pris en charge.<br><br>L'algorithme de hachage SHA-2 est pris en charge.<br><br>La longueur maximale de la clé est de 2 048 bits. | Ce certificat authentifie l'ordinateur client Mac auprès des serveurs de système de site avec lesquels il communique, tels que les points de gestion et les points de distribution. |

| COMPOSANT SYSTEM CENTER CONFIGURATION MANAGER | RÔLE DU CERTIFICAT | MODÈLE DE CERTIFICAT MICROSOFT À UTILISER | INFORMATIONS SPÉCIFIQUES DU CERTIFICAT | MODE D'UTILISATION DU CERTIFICAT DANS SYSTEM CENTER CONFIGURATION MANAGER |
|---|---|---|---|---|
| Ordinateurs clients Linux et UNIX | Authentification du client | **Authentification de station de travail** | **Utilisation avancée de la clé** : la valeur de ce paramètre doit contenir **Authentification du client (1.3.6.1.5.5.7.3.2)**.<br><br>Le champ Autre nom de l'objet n'est pas pris en charge.<br><br>La clé privée doit être exportable.<br><br>L'algorithme de hachage SHA-2 est pris en charge si le système d'exploitation du client prend en charge SHA-2. Pour plus d'informations, consultez la section À propos des systèmes d'exploitation Linux et UNIX qui ne prennent pas en charge SHA-256 dans la rubrique Planification du déploiement de clients sur des ordinateurs Linux et UNIX dans System Center Configuration Manager.<br><br>Longueurs de clé prises en charge : 2 048 bits.<br><br>**Remarque :** ces certificats doivent être au format binaire encodé DER (Distinguished Encoding Rules) X.509. Le format X.509 codé en Base64 n'est pas pris en charge. | Ce certificat authentifie l'ordinateur client Linux ou UNIX auprès des serveurs de système de site avec lesquels il communique, tels que les points de gestion et les points de distribution. Le certificat doit être exporté au format Public Key Certificate Standard (PKCS#12), et le mot de passe doit être connu, de sorte que vous puissiez l'indiquer au client lors de la spécification du certificat PKI.<br><br>Pour plus d'informations, consultez la section Planification de la sécurité et les certificats pour les serveurs Linux et UNIX dans la rubrique Planification du déploiement de clients sur des ordinateurs Linux et UNIX dans System Center Configuration Manager. |
| Certificats de l'autorité de certification (CA) racine pour les | Chaîne de certificat pour une source approuvée | Non applicable. | Certificat d'autorité de certification racine standard. | Le certificat d'autorité de certification racine doit être fourni |

| COMPOSANT SYSTEM CENTER CONFIGURATION MANAGER | RÔLE DU CERTIFICAT | MODÈLE DE CERTIFICAT MICROSOFT À UTILISER | INFORMATIONS SPÉCIFIQUES DU CERTIFICAT | MODE D'UTILISATION DU CERTIFICAT DANS SYSTEM CENTER CONFIGURATION MANAGER |
|---|---|---|---|---|
| scénarios suivants :<br>• Déploiement du système d'exploitation<br>• Inscription d'appareil mobile<br>• Authentification du serveur RADIUS pour les ordinateurs Intel basés sur AMT<br>• Authentification du certificat du client | | | | lorsque les clients doivent lier les certificats du serveur qu'ils contactent à une source fiable. Cela s'applique aux scénarios suivants :<br>• Lorsque vous déployez un système d'exploitation et pendant l'exécution de séquences de tâches qui connectent l'ordinateur client à un point de gestion configuré pour utiliser le protocole HTTPS.<br>• Quand vous inscrivez un appareil mobile qui doit être géré par System Center Configuration Manager.<br>• Quand vous utilisez l'authentification 802.1X pour les ordinateurs AMT et que vous souhaitez spécifier un fichier pour le certificat racine du serveur RADIUS.<br>De plus, le certificat d'autorité de certification racine des clients doit être fourni si les certificats du client ont été émis par une hiérarchie d'autorité de certification différente de celle ayant émis le certificat du point de gestion. |

| COMPOSANT SYSTEM CENTER CONFIGURATION MANAGER | RÔLE DU CERTIFICAT | MODÈLE DE CERTIFICAT MICROSOFT À UTILISER | INFORMATIONS SPÉCIFIQUES DU CERTIFICAT | MODE D'UTILISATION DU CERTIFICAT DANS SYSTEM CENTER CONFIGURATION MANAGER |
|---|---|---|---|---|
| Ordinateurs Intel basés sur AMT | Authentification du serveur. | **Serveur web** (modifié)<br><br>Vous devez configurer le nom de l'objet pour **Construire à partir de ces informations Active Directory**, puis sélectionnez **Nom commun** pour le **Format du nom de l'objet**.<br><br>Vous devez accorder les autorisations **Lecture** et **Inscription** au groupe de sécurité universel que vous spécifiez dans les propriétés du composant de gestion hors bande. | **Utilisation avancée de la clé** : la valeur de ce paramètre doit contenir **Authentification du serveur (1.3.6.1.5.5.7.3.1)**.<br><br>Le Nom de l'objet doit contenir le nom de domaine complet de l'ordinateur basé sur AMT, qui est fourni automatiquement à partir des services de domaine Active Directory. | Ce certificat réside dans la mémoire RAM non volatile du contrôleur de gestion de l'ordinateur et n'est pas consultable depuis l'interface utilisateur de Windows.<br><br>Chaque ordinateur Intel basé sur AMT demande ce certificat lors de la préparation AMT et des mises à jour ultérieures. Si vous supprimez les informations de préparation AMT de ces ordinateurs, ils révoquent ce certificat.<br><br>Lorsque vous installez ce certificat sur des ordinateurs Intel basés sur AMT, le certificat lié à l'autorité de certification racine est également installé. Les ordinateurs basés sur AMT ne peuvent pas prendre en charge les certificats émis par l'autorité de certification dont la longueur de clé dépasse 2 048 bits.<br><br>Une fois le certificat installé sur les ordinateurs Intel basés sur AMT, ce certificat authentifie les ordinateurs basés sur AMT sur le serveur de système de site du point de service hors bande et sur les ordinateurs exécutant la console de gestion hors bande, et il chiffre toutes les données transférées entre eux |

| COMPOSANT SYSTEM CENTER CONFIGURATION MANAGER | RÔLE DU CERTIFICAT | MODÈLE DE CERTIFICAT MICROSOFT À UTILISER | INFORMATIONS SPÉCIFIQUES DU CERTIFICAT | MODE D'UTILISATION DU CERTIFICAT DANS SYSTEM CENTER CONFIGURATION MANAGER |
| --- | --- | --- | --- | --- |
| Certificat client Intel AMT 802.1X | Authentification du client | **Authentification de station de travail**<br><br>Configurez le nom de l'objet pour **Construire à partir de ces informations Active Directory**, puis sélectionnez **Nom commun** pour le **Format du nom de l'objet**, supprimez le nom DNS et sélectionnez le nom d'utilisateur principal pour l'autre nom de l'objet.<br><br>Vous devez accorder au groupe de sécurité universel que vous spécifiez dans les propriétés du composant de gestion hors bande les autorisations **Lecture** et **Inscription** pour ce modèle de certificat. | **Utilisation avancée de la clé** : la valeur de ce paramètre doit contenir **Authentification du client (1.3.6.1.5.5.7.3.2)**.<br><br>Le champ Nom de l'objet doit contenir le nom de domaine complet de l'ordinateur basé sur AMT et le champ Autre nom de l'objet doit contenir le nom UPN.<br><br>Longueur de clé maximale prise en charge : 2 048 bits. | à l'aide du protocole TLS (Transport Layer Security).<br><br>Ce certificat réside dans la mémoire RAM non volatile du contrôleur de gestion de l'ordinateur et n'est pas consultable depuis l'interface utilisateur de Windows.<br><br>Chaque ordinateur Intel basé sur AMT peut demander ce certificat lors de la préparation AMT, mais il ne révoque pas ce certificat lorsque ses informations de préparation AMT sont supprimées.<br><br>Une fois installé sur les ordinateurs AMT, ce certificat authentifie ceux-ci sur le serveur RADIUS afin que l'accès réseau lui soit accordé. |

| COMPOSANT SYSTEM CENTER CONFIGURATION MANAGER | RÔLE DU CERTIFICAT | MODÈLE DE CERTIFICAT MICROSOFT À UTILISER | INFORMATIONS SPÉCIFIQUES DU CERTIFICAT | MODE D'UTILISATION DU CERTIFICAT DANS SYSTEM CENTER CONFIGURATION MANAGER |
|---|---|---|---|---|
| Appareils mobiles inscrits par Microsoft Intune | Authentification du client | Non applicable : Intune crée automatiquement ce certificat. | La valeur **Utilisation avancée de la clé** doit contenir **Authentification du client (1.3.6.1.5.5.7.3.2)**.<br><br>Trois extensions personnalisées identifient de manière unique l'abonnement Intune du client.<br><br>Les utilisateurs peuvent fournir la valeur Objet du certificat lors de l'inscription. Cependant, Intune n'utilise pas cette valeur pour identifier l'appareil.<br><br>La taille de la clé est de 2 048 bits et elle utilise l'algorithme de hachage SHA-1.<br><br>**Remarque :** vous ne pouvez pas modifier ces paramètres. ces informations sont fournies uniquement à titre d'information. | Ce certificat est demandé et installé automatiquement quand les utilisateurs authentifiés inscrivent leurs appareils mobiles à l'aide de Microsoft Intune. Le certificat obtenu sur l'appareil réside dans le magasin de l'ordinateur et authentifie l'appareil mobile inscrit auprès d'Intune pour qu'il puisse être géré.<br><br>Du fait des extensions personnalisées du certificat, l'authentification se limite à l'abonnement Intune établi pour l'organisation. |

# Vue d'ensemble des certificats CNG

22/06/2018 • 4 minutes to read • Edit Online

Configuration Manager prend en charge les certificats Cryptography : Next Generation (CNG) de manière limitée. Les clients Configuration Manager peuvent utiliser un certificat d'authentification client PKI avec une clé privée dans le fournisseur de stockage de clés (KSP) CNG. La prise en charge du KSP permet aux clients Configuration Manager de prendre en charge une clé privée matérielle, comme TPM KSP pour les certificats d'authentification client PKI.

## Scénarios pris en charge

Vous pouvez utiliser les modèles de certificat Cryptography API : Next Generation (CNG) pour les scénarios suivants :

- Inscription du client et communication avec un point de gestion HTTPS
- Distribution de logiciels et déploiement d'applications avec un point de distribution HTTPS
- Déploiement du système d'exploitation
- Kit SDK de messagerie du client (avec la dernière mise à jour) et proxy ISV
- Configuration de la passerelle de gestion cloud

À compter de la version 1802, utilisez des certificats CNG pour les rôles serveur HTTPS suivants :

- Point de gestion
- Point de distribution
- Point de mise à jour logicielle
- Point de migration d'état

> **NOTE**
> CNG offre une compatibilité descendante avec Crypto API (CAPI). Les certificats CAPI continuent à être pris en charge même lorsque la prise en charge CNG est activée sur le client.

## Scénarios non pris en charge

Les scénarios suivants ne sont actuellement pas pris en charge :

- Les rôles serveur suivants ne sont pas opérationnels quand ils sont installés en mode HTTPS avec un certificat CNG lié au site web dans Internet Information Services (IIS) :
  - Service web du catalogue des applications
  - Site web du catalogue des applications
  - Point d'inscription
  - Point proxy d'inscription
- Le Centre logiciel n'affiche pas les applications et packages disponibles qui sont déployés sur des regroupements d'utilisateurs ou de groupes d'utilisateurs.
- Utilisation de certificats CNG pour créer un point de distribution cloud.
- Si le module de stratégie NDES utilise un certificat CNG pour l'authentification du client, la communication avec le point d'enregistrement de certificat échoue.

- Si vous spécifiez un certificat CNG lors de la création d'un média de séquence de tâches, l'Assistant ne parvient pas à créer un média de démarrage.

## Pour utiliser des certificats CNG

Pour utiliser des certificats CNG, votre autorité de certification (CA) doit fournir des modèles de certificat CNG pour les machines cibles. Bien que les détails du modèle varient selon le scénario, les propriétés suivantes sont requises :

- Onglet **Compatibilité**
  - L'**autorité de certification** doit être Windows Server 2008 ou version ultérieure. (Windows Server 2012 recommandé)
  - Le **destinataire du certificat** doit être Windows Vista/Server 2008 ou version ultérieure. (Windows 8/Windows Server 2012 recommandé)
- Onglet **Chiffrement**
  - La **catégorie de fournisseur** doit être **Fournisseur de stockage de clés**. (obligatoire)

> **NOTE**
> La configuration requise pour votre environnement ou votre organisation peut être différente. Contactez votre expert PKI. Le point important à ne pas négliger est qu'un modèle de certificat doit utiliser un fournisseur de stockage de clés pour tirer parti de CNG.

Pour de meilleurs résultats, nous vous recommandons de créer le nom du sujet à partir des informations Active Directory. Utilisez le nom DNS pour le **format du nom du sujet** et incluez le nom DNS dans le nom de substitution du sujet. Dans le cas contraire, vous devez fournir ces informations au moment de l'inscription de l'appareil dans le profil de certificat.

# Données d'utilisation et de diagnostic pour System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Configuration Manager collecte les données d'utilisation et de diagnostic qui le concernent. Microsoft utilise ensuite ces données pour améliorer le processus d'installation, la qualité et la sécurité des versions ultérieures.

Les données d'utilisation et de diagnostic sont collectées pour chaque hiérarchie Configuration Manager. Elle consistent en requêtes SQL Server qui s'exécutent chaque semaine sur chaque site principal et sur le site d'administration centrale. Quand la hiérarchie utilise un site d'administration centrale, les données provenant des sites principaux sont répliquées sur ce site. Sur le site de niveau supérieur de votre hiérarchie, le point de connexion de service soumet ces informations quand il recherche des mises à jour. Si le point de connexion de service est en mode hors connexion, les informations sont transférées à l'aide de l'outil de connexion de service.

> **NOTE**
> Configuration Manager collecte uniquement les données de la base de données SQL Server du site. Il ne collecte pas de données directement à partir des clients ni des serveurs de site.

Pour plus d'informations, consultez la Déclaration de confidentialité de Microsoft.

## Articles

Pour en savoir plus sur les données d'utilisation et de diagnostic de Configuration Manager, consultez les articles suivants :

- Utilisation des données de diagnostic et d'utilisation
- Niveaux de collecte des données d'utilisation et de diagnostic :
  - Données de diagnostic pour 1802
  - Données de diagnostic pour 1710
  - Données de diagnostic pour 1706
- Mode de collecte des données de diagnostic et d'utilisation
- Mode d'affichage des données de diagnostic et d'utilisation
- Programme d'amélioration de l'expérience utilisateur (CEIP)

  > **NOTE**
  > À compter de Configuration Manager version 1802, la fonctionnalité CEIP ne figure plus dans le produit.

- Forum aux questions sur les données de diagnostic et d'utilisation

## Voir aussi

À propos du point de connexion de service

# Utilisation des données d'utilisation et de diagnostic pour System Center Configuration Manager

22/06/2018 • 3 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les données de diagnostic et d'utilisation que System Center Configuration Manager collecte fournissent à Microsoft un retour d'expérience quasi immédiat sur la manière dont le produit fonctionne, et permettent d'améliorer les mises à jour ultérieures. Nous pouvons également voir des données de configuration qui nous aident à concevoir et tester les configurations qui sont en production. Par exemple :

- Versions de Windows Server utilisées par les serveurs de site
- Modules linguistiques installés
- Différentiel du schéma SQL par rapport aux paramètres par défaut du produit

Ces données aident l'équipe de conception à planifier les prochains tests visant à garantir la meilleure expérience possible pour les configurations les plus courantes. Les mises à jour de Configuration Manager étant publiées à un rythme plus soutenu (pour mieux prendre en charge les technologies qui évoluent rapidement, telles que Windows 10 et Microsoft Intune), ces données sont cruciales pour une adaptation rapide.

Il est également important de savoir à quoi les données de diagnostic et d'utilisation ne sont pas utilisées. Microsoft n'utilise pas ces données pour ce qui suit :

- Audits de licence (par exemple, comparer l'utilisation des clients avec les contrats de licence)
- Audit de produits non pris en charge
- Publicité basée sur des données disponibles, telles que l'utilisation de fonctionnalités ou la géolocalisation (fuseau horaire)

## Exemples de la manière dont les données de diagnostic et d'utilisation contribuent à améliorer le produit

Microsoft utilise les données disponibles pour améliorer le produit. Voici quelques exemples :

- **Prise en charge révisée pour les systèmes d'exploitation serveur plus anciens :**

  La prise en charge initiale offerte par System Center Configuration Manager (Current Branch) limitait la période de prise en charge de Windows Server 2008 R2. Après examen des données d'utilisation de clients qui avaient effectué une mise à niveau vers la version Current Branch de Configuration Manager, nous avons jugé utile de modifier et d'étendre cette période pour prendre en charge les clients qui continuaient d'utiliser ce système d'exploitation serveur pour héberger des serveurs de site et des rôles de système de site.

- **Vérifications de configuration requise améliorées :**

  Sur la base des données d'utilisation, nous avons amélioré les vérifications des conditions préalables à l'installation d'une mise à jour pour supprimer des règles obsolètes, tenir compte de cas supplémentaires et, dans certains cas, résoudre automatiquement certains problèmes.

# Niveaux de collecte des données de diagnostic et d'utilisation pour la version 1802 de System Center Configuration Manager

22/06/2018 • 27 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Configuration Manager version 1802 collecte trois niveaux de données d'utilisation et de diagnostic : **De base**, **Étendu** et **Complet**. Par défaut, cette fonctionnalité est définie sur le niveau Étendu. Les sections suivantes fournissent des détails supplémentaires sur les données collectées à chaque niveau.

Les modifications par rapport aux versions précédentes sont indiquées par ***[Nouveau]***, ***[Mis à jour]***, ***[Supprimé]*** ou ***[Déplacé]***.

> **IMPORTANT**
> Configuration Manager ne collecte pas les codes des sites, les noms des sites, les adresses IP, les noms d'utilisateur ou d'ordinateur, les adresses physiques ou les adresses e-mail aux niveaux De base et Étendu. Toute collecte de ces informations au niveau Complet n'est pas intentionnelle. Elles peuvent être incluses dans des informations de diagnostic avancées comme des fichiers journaux ou des instantanés de mémoire. Microsoft n'utilise pas ces informations pour vous identifier ou vous contacter, ni à des fins publicitaires.

## Modification du niveau

Les administrateurs qui ont une étendue d'administration basée sur des rôles incluant les autorisations **Modifier** sur la classe d'objets **Site** peuvent changer le niveau des données collectées dans les paramètres des données de diagnostic et d'utilisation de la console Configuration Manager.

Vous pouvez changer le niveau de collecte des données à partir de la console en accédant à **Administration** > **Vue d'ensemble** > **Configuration du site** > **Sites**. Ouvrez **Paramètres de hiérarchie**, puis sélectionnez le niveau de données que vous voulez utiliser.

## Niveau 1 - De base

Le niveau De base comprend les données relatives à votre hiérarchie, qui sont nécessaires pour aider à améliorer votre expérience d'installation ou de mise à niveau, ainsi que des données pour aider à identifier les mises à jour Configuration Manager qui s'appliquent à votre hiérarchie.

Pour Configuration Manager version 1802, ce niveau inclut les données suivantes :

- Statistiques sur les connexions de la console Configuration Manager : version du système d'exploitation, langue, référence (SKU) et architecture, mémoire système, nombre de processeurs logiques, ID du site de connexion, versions .NET installées et modules linguistiques de la console
- Nombres de types d'application et de déploiement de base : nombre total d'applications, nombre total d'applications avec plusieurs types de déploiement, nombre total d'applications avec des dépendances, nombre total d'applications remplacées, nombre de technologies de déploiement en cours d'utilisation
- Données de la hiérarchie des sites Configuration Manager de base : liste des sites, type, version, état, nombre de clients et fuseau horaire

- Configuration de base de données simple : processeurs, configuration du cluster et configuration des vues distribuées
- Statistiques de découverte de base : nombre de découvertes, tailles de groupe minimale/maximale/moyenne) et moment où le site est entièrement exécuté avec les services Active Directory Azure
- Informations Endpoint Protection de base sur les versions du client de logiciel anti-programme malveillant
- Nombres d'images de déploiements de système d'exploitation de base
- Informations de serveur de système de site de base : rôles de système de site utilisés, état SSL et Internet, système d'exploitation, processeurs, ordinateur physique ou machine virtuelle, et utilisation de la haute disponibilité du serveur de site
- Schéma de base de données Configuration Manager (hachage de toutes les définitions d'objet)
- Niveau de télémétrie configuré, mode en ligne ou hors connexion, et configuration de la mise à jour rapide
- Nombre de paramètres régionaux et de langues du client
- Nombre de versions du client Configuration Manager, de versions du système d'exploitation et de versions d'Office
- Nombre de systèmes d'exploitation des appareils gérés et stratégies définies par le connecteur Exchange
- Nombre d'appareils Windows 10 par branche et build
- ***[Déplacé]*** Nombre de clients Windows 10 qui utilisent Windows Update pour Entreprise
- Métriques de performances de base de données : informations sur le traitement de la réplication, procédures stockées SQL Server les plus utilisées par processeur et utilisation des disques
- Types de point de distribution et de point de gestion, et informations de configuration de base : protégés, préparés, PXE, multidiffusion, état SSL, points de distribution d'extraction/entre homologues, compatibles avec la gestion locale des appareils mobiles (MDM) et compatibles SSL
- Liste hachée d'extensions des Assistants et pages de propriétés de console Administrateur
- Informations d'installation :
  - Build, type d'installation, modules linguistiques, fonctionnalités que vous avez activées
  - Utilisation en préversion, type de support de configuration, type de branche
  - Date d'expiration de Software Assurance
  - État et erreurs du déploiement du package de mise à jour, progression du téléchargement, et erreurs liées aux prérequis
  - Utilisation de l'anneau rapide de mise à jour
  - Version du script après mise à niveau
- Version SQL, niveau de Service Pack, édition, ID de classement et jeu de caractères
- Statistiques de télémétrie : à l'exécution, runtime, erreurs
- Information indiquant si la découverte du réseau est activée ou désactivée
- ***[Déplacé]*** Nombre de clients joints à Azure Active Directory
- ***[Nouveau]*** Nombre de déploiements par phases créés par type

- ***[Nouveau]*** Nombre de clients d'interopérabilité étendue
- ***[Nouveau]*** Liste haché des propriétés de l'inventaire matériel de plus de 255 caractères

## Niveau 2 – Étendu

Le niveau Étendu est configuré par défaut après l'installation. Ce niveau comprend les données collectées au niveau De base, ainsi que les données spécifiques aux fonctionnalités (fréquence et durée d'utilisation), les paramètres du client Configuration Manager (nom du composant, état et paramètres, comme les intervalles d'interrogation) et les informations de base sur les mises à jour logicielles.

Ce niveau est recommandé, car il fournit à Microsoft les données minimales nécessaires pour apporter des améliorations utiles dans les futures versions des produits et services. Ce niveau ne collecte pas les noms des objets (sites, utilisateurs, ordinateur ou objets), les informations sur les objets relatifs à la sécurité ni les vulnérabilités, comme le nombre de systèmes qui nécessitent des mises à jour logicielles.

Pour Configuration Manager version 1802, ce niveau inclut les données suivantes :

**Gestion des applications**

- Exigences pour les applications : nombre de conditions prédéfinies référencé par la technologie de déploiement
- Remplacement des applications, profondeur de chaîne maximale
- Statistiques d'approbation de l'application et fréquence d'utilisation
- Statistiques sur les tailles de contenu d'application
- Informations de déploiement d'application : utilisation de l'installation par rapport à la désinstallation, approbation exigée, interaction utilisateur activée/désactivée, dépendance, remplacement et nombre d'utilisations de la fonctionnalité de comportement à l'installation
- Statistiques de taille et de complexité des stratégies d'applications
- Statistiques de demande d'application disponibles
- Informations de configuration de base pour les packages et les programmes : options de déploiement et indicateurs de programme
- Informations de base d'utilisation/de ciblage pour les types de déploiement : ciblé utilisateur ou appareil, nécessaire ou disponible, et applications universelles
- Nombre d'environnements App-V et propriétés de déploiement
- Nombre d'applicabilités de l'application par système d'exploitation
- Nombre d'applications référencées par une séquence de tâches
- Nombre de personnalisations distinctes pour le catalogue d'applications
- Nombre d'applications Office 365 créées à l'aide du tableau de bord
- Nombre de packages par type
- Nombre de déploiements de package/programme
- Nombre de licences d'application Windows 10 concédées
- Nombre de types de déploiement Windows Installer par paramètres du contenu de désinstallation
- Nombre d'applications de Microsoft Store pour Entreprises et statistiques de synchronisation : résumé des types d'applications, état des applications sous licence et nombre d'applications sous licence en ligne et hors

connexion

- Type et durée de fenêtre de maintenance
- Nombre minimal/maximal/moyen de déploiements d'applications par utilisateur/appareil par période
- Codes d'erreur d'installation d'application les plus courants par technologie de déploiement
- Options de configuration MSI et nombres
- Statistiques sur l'interaction de l'utilisateur final avec notification des déploiements de logiciels requis
- Utilisation et mode de création d'Universal Data Access (UDA)
- ***[Nouveau]*** Statistiques agrégées d'affinité entre appareil et utilisateur
- ***[Nouveau]*** Nombre maximal et moyen d'utilisateurs principaux par appareil

**Client**

- Version du client AMT (Active Management Technology)
- Âge du BIOS en années
- Nombre d'appareils avec démarrage sécurisé
- Nombre d'appareils par état TPM
- Mise à niveau automatique du client : configuration du déploiement, notamment le test du client et l'utilisation de l'exclusion (client d'interopérabilité étendue)
- Configuration de la taille du cache du client
- Erreurs de téléchargement de déploiement des clients
- Statistiques d'intégrité du client et récapitulatif des problèmes principaux
- État des actions de notification du client : nombre d'exécutions de chaque action, nombre maximal de clients ciblés et taux de réussite moyen
- Nombre d'installations de client à partir de chaque type d'emplacement source
- Nombre d'échecs d'installation de client
- Nombre d'appareils virtualisés par Hyper-V ou Azure
- Nombre d'actions du Centre logiciel
- Nombre d'appareils compatibles UEFI
- Méthodes de déploiement utilisées pour le client et nombre de clients par méthode de déploiement
- Liste/nombre d'agents clients activés
- Âge du système d'exploitation en mois
- Nombre de classes d'inventaire matériel, règles d'inventaire logiciel et règles de regroupement de fichiers
- Statistiques pour l'attestation d'intégrité des appareils : codes d'erreur les plus courants, nombre de serveurs locaux et nombre d'appareils dans différents états
- ***[Nouveau]*** Nombre d'appareils par navigateur par défaut

**Services cloud**

- Statistiques de découverte Azure Active Directory

- Statistiques de configuration et d'utilisation de la passerelle de gestion cloud : nombre de régions et d'environnements, et statistiques d'authentification/autorisation
- Nombre d'applications et services Azure Active Directory connectés à Configuration Manager
- Nombre de regroupements qui sont synchronisés avec Operations Management Suite
- Nombre de connecteurs Upgrade Analytics
- Activation ou non du connecteur cloud Operations Management Suite

**Cogestion**

- Statistiques agrégées d'utilisation de la cogestion : nombre de clients inscrits, clients recevant la stratégie, états de la charge de travail, tailles des regroupements de pilotes/d'exclusions et erreurs d'inscription
- Nombre de clients par méthode d'inscription à la cogestion
- Statistiques d'erreurs pour l'inscription à la cogestion
- Planification de l'inscription et statistiques d'historique
- Nombre de clients éligibles à la cogestion
- Locataire Microsoft Intune associé

**Regroupements**

- Utilisation des ID de regroupement (ne pas manquer d'ID)
- Statistiques d'évaluation des regroupements : durée des requêtes, nombre de regroupements affectés et non affectés, nombres par type, substitution d'ID et utilisation des règles
- Regroupements sans déploiement

**Paramètres de conformité**

- Informations de la ligne de base de configuration de base : décompte, nombre de déploiements et nombre de références
- Statistiques d'erreurs de stratégie de conformité
- Nombre d'éléments de configuration par type
- Nombre de déploiements qui référencent des paramètres prédéfinis, notamment le paramètre de correction
- Nombre de règles et de déploiements créés pour des paramètres personnalisés, notamment le paramètre de correction
- Nombre de modèles SCEP (Simple Certificate Enrollment Protocol), VPN, Wi-Fi, de certificat (.pfx) et de stratégie de conformité déployés
- Nombre de déploiements de certificat SCEP, VPN, Wi-Fi, certificat (.pfx) et stratégie de conformité par plateforme
- Stratégie Windows Hello Entreprise (créée, déployée)

**Content**

- ***[Mis à jour]*** Statistiques des groupes de limites : nombre de rapides, nombre de lents, nombre par groupe et relations de secours
- Informations sur les groupes de limites : nombre de limites et de systèmes de site qui sont attribués à chaque groupe de limites
- Relations de groupes de limites et configuration de secours

- Statistiques de téléchargement du contenu client
- Nombre de limites par type
- Nombre de clients de cache d'homologue, statistiques d'utilisation et statistiques de téléchargements partiels
- Informations sur la configuration du gestionnaire de distribution : threads, délai de nouvelle tentative, nombre de nouvelles tentatives et paramètres de point de distribution d'extraction
- Informations sur la configuration des points de distribution : utilisation de BranchCache et surveillance des points de distribution
- Informations sur les groupes de points de distribution : nombre de packages et de points de distribution qui sont affectés à chaque groupe de points de distribution

**Endpoint Protection**

- Stratégies Windows Defender - Protection avancée contre les menaces (ATP) : nombre de stratégies et indication de déploiement des stratégies
- Nombre d'alertes configurées pour la fonctionnalité Endpoint Protection
- Nombre de regroupements sélectionnés pour être affichés dans le tableau de bord Endpoint Protection
- Nombre de stratégies, de déploiements et de clients ciblés Windows Defender Exploit Guard
- Erreurs de déploiement Endpoint Protection : nombre de codes d'erreur de déploiement de stratégie Endpoint Protection
- Utilisation des stratégies du Pare-feu Windows et de logiciel anti-programme malveillant Endpoint Protection (nombre de stratégies uniques affectées au groupe)

  Ces données ne comprennent pas d'informations sur les paramètres inclus dans la stratégie.

**Migration**

- Nombre d'objets migrés (utilisation de l'Assistant Migration)

**Gestion des appareils mobiles (MDM)**

- Nombre d'actions d'appareil mobile émises : commandes de verrouillage, de réinitialisation, de mise hors service et de synchronisation immédiate
- Nombre de stratégies d'appareil mobile
- Nombre d'appareils mobiles gérés par Configuration Manager et Microsoft Intune, et méthode d'inscription (en bloc ou basée sur l'utilisateur)
- Nombre d'utilisateurs qui ont plusieurs appareils mobiles inscrits
- Statistiques et calendrier d'interrogation des appareils mobiles pour la durée d'inscription des appareils mobiles

**Dépannage de Microsoft Intune**

- Nombre et taille des messages d'actions d'appareil (réinitialiser, mettre hors service, verrouiller), de télémétrie et de données qui sont répliqués vers Microsoft Intune
- Nombre et taille des messages d'état, de statut, d'inventaire, RDR, DDR, UDX, d'état de locataire, POL, LOG, de certificat, CRP, de resynchronisation, CFD, RDO, BEX, ISM et de conformité qui sont téléchargés à partir de Microsoft Intune
- Statistiques de synchronisation utilisateur complète et différentielle pour Microsoft Intune

**Gestion locale des appareils mobiles**

- Nombre de profils et de packages d'inscription en bloc Windows 10
- Statistiques de réussite/échec de déploiement pour les déploiements d'applications de gestion MDM locale

**Déploiement de système d'exploitation**

- Nombre d'images de démarrage, de pilotes, de packages de pilotes, de points de distribution en multidiffusion, de points de distribution compatibles PXE et de séquences de tâches
- Nombre d'images de démarrage par version cliente de Configuration Manager
- Nombre d'images de démarrage par version de Windows PE
- Nombre de stratégies de mise à niveau d'édition
- Nombre d'identificateurs de matériel exclus de PXE
- Nombre de déploiement du système d'exploitation par version de système d'exploitation
- Nombre de mises à niveau du système d'exploitation au fil du temps
- Nombre de déploiements de séquences de tâches utilisant l'option de prétéléchargement du contenu
- Nombre d'utilisations des étapes de séquence de tâches
- Version de Windows ADK installée

**Mises à jour du site**

- Versions des correctifs logiciels de Configuration Manager installés

**mises à jour logicielles**

- Différentiels de disponibilité et d'échéance qui sont utilisés dans les règles de déploiement automatique
- Nombre moyen et maximal d'attributions par mise à jour
- Calendriers d'analyse et d'évaluation des mises à jour client
- Classifications qui sont synchronisées par le point de mise à jour logicielle
- Statistiques d'application de correctifs logiciels au cluster
- Configuration des mises à jour rapides de Windows 10
- Configurations qui sont utilisées pour les plans de maintenance actifs de Windows 10
- Nombre de mises à jour Office 365 déployées
- Nombre de pilotes Microsoft Surface synchronisés
- Nombre de groupes et d'attributions de mises à jour
- Nombre de packages de mises à jour et nombre maximal/minimal/moyen de points de distribution qui sont ciblés par les packages
- Nombre de mises à jour créées et déployées avec System Center Update Publisher
- Nombre de stratégies Windows Update for Business créées et déployées
- ***[Nouveau]*** Statistiques agrégées des configurations de Windows Update pour Entreprise
- Nombre de règles de déploiement automatique qui sont liées à la synchronisation
- Nombre de règles de déploiement automatique qui créent de nouvelles mises à jour ou ajoutent des mises à jour à un groupe existant

- Nombre de règles de déploiement automatique avec plusieurs déploiements
- Nombre de groupes de mises à jour et nombre minimal/maximal/moyen de mises à jour par groupe
- Nombre de mises à jour et pourcentage de mises à jour qui sont déployées, expirées, remplacées, téléchargées et qui contiennent des CLUF
- Statistiques d'équilibrage de charge du point de mise à jour logicielle
- Planification de la synchronisation du point de mise à jour logicielle
- Nombre total/moyen de regroupements comportant des déploiements de mises à jour logicielles et nombre maximal/moyen de mises à jour déployées
- Codes d'erreur d'analyse des mises à jour et nombre d'ordinateurs
- Versions de contenu du tableau de bord Windows 10

**Données de performances/SQL**

- Configuration et durée de la synthèse du site
- Nombre des plus grandes tables de base de données
- Statistiques opérationnelles de découverte (nombre d'objets trouvés)
- Types de découverte activés et planifiés (complète, incrémentielle)
- Informations sur les réplicas SQL AlwaysOn, utilisation et état d'intégrité
- Problèmes de performances du suivi des modifications SQL, période de rétention et état de nettoyage automatique
- Période de rétention du suivi des modifications SQL
- Statistiques de performances des messages d'état et de statut, notamment les types de messages les plus courants et les plus coûteux

**Divers**

- Configuration du point de service de l'entrepôt de données, notamment la planification et la durée moyenne de la synchronisation
- Nombre de scripts et statistiques d'exécution
- Nombre de sites avec Wake On LAN (WOL)
- Statistiques de performances et d'utilisation des rapports
- ***[Nouveau]*** Statistiques d'utilisation du déploiement par phases

# Niveau 3 – Complet

Le niveau Complet inclut toutes les données des niveaux De base et Étendu. Il inclut également des informations supplémentaires sur Endpoint Protection, les pourcentages de compatibilité des mises à jour et les informations de mise à jour logicielle. Ce niveau peut également inclure des informations de diagnostic avancées telles que des fichiers système et des instantanés de la mémoire, qui peuvent inclure des informations personnelles qui existaient dans la mémoire ou les fichiers journaux au moment de la capture.

Pour Configuration Manager version 1802, ce niveau inclut les données suivantes :

- Informations sur le calendrier d'évaluation de règle de déploiement automatique

- Récapitulatif d'intégrité ATP
- Statistiques d'évaluation et d'actualisation des regroupements
- Statistiques de stratégie de conformité pour les erreurs et la conformité
- Paramètres de conformité : détails de configuration des modèles SCEP, VPN, Wi-Fi et de stratégie de conformité
- Pack de configuration DCM pour l'utilisation de System Center Configuration Manager
- Détails des erreurs d'installation du déploiement des clients
- Récapitulatif de l'intégrité Endpoint Protection : nombre de clients protégés, présentant un risque, inconnus et non pris en charge
- Configuration de la stratégie Endpoint Protection
- Liste des processus configurés avec le comportement à l'installation des applications
- Nombre minimal/maximal/moyen d'heures depuis la dernière analyse des mises à jour logicielles
- Nombre minimal/maximal/moyen de clients inactifs dans les regroupements de déploiements de mise à jour logicielle
- Nombre minimal/maximal/moyen de mises à jour logicielles par package
- ***[Mis à jour]*** Statistiques de déploiement de code de produit MSI
- Compatibilité globale des déploiements de mise à jour logicielle
- Nombre de groupes avec des mises à jour logicielles expirées
- Nombres et codes d'erreur de déploiement de mise à jour logicielle
- Informations de déploiement de mise à jour logicielle : pourcentage de déploiements ciblés avec le client ou l'heure UTC, obligatoire/facultatif/en mode silencieux, et suppression du redémarrage
- Produits des mises à jour logicielles synchronisés par point de mise à jour logicielle
- Pourcentages de réussite d'analyse des mises à jour logicielles
- 50 premières unités centrales dans l'environnement
- Type de stratégies d'accès conditionnel EAS (Exchange Active Sync) (bloquer ou mettre en quarantaine) pour les appareils gérés par Microsoft Intune
- Détails des applications de Microsoft Store pour Entreprises : liste de non-agrégation des applications synchronisées, notamment l'ID de l'application, l'état en ligne ou hors connexion, et le nombre total de licences achetées

# Niveaux de collecte des données de diagnostic et d'utilisation pour la version 1710 de System Center Configuration Manager

22/06/2018 • 26 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

System Center Configuration Manager version 1710 collecte trois niveaux de données d'utilisation et de diagnostic : **De base**, **Étendu** et **Complet**. Par défaut, cette fonctionnalité est définie sur le niveau Étendu. Les sections suivantes fournissent des détails supplémentaires sur les données collectées par chaque niveau.

Les modifications par rapport aux versions précédentes sont indiquées par ***[Nouveau]***, ***[Mis à jour]***, ***[Supprimé]*** ou ***[Déplacé]***.

> **IMPORTANT**
> Configuration Manager ne collecte pas les codes des sites, les noms des sites, les adresses IP, les noms d'utilisateur ou d'ordinateur, les adresses physiques ni les adresses e-mail aux niveaux De base et Étendu. Toute collecte de ces informations au niveau Complet n'est pas intentionnelle : elles peuvent être incluses dans des informations de diagnostic avancées comme des fichiers journaux ou des instantanés de la mémoire. Microsoft n'utilisera pas ces informations pour vous identifier ou vous contacter, ni à des fins publicitaires.

## Modification du niveau

Les administrateurs qui ont une étendue d'administration basée sur des rôles incluant les autorisations **Modifier** sur la classe d'objets **Site** peuvent changer le niveau des données collectées dans les paramètres des données de diagnostic et d'utilisation de la console Configuration Manager.

Vous pouvez changer le niveau de collecte des données à partir de la console en accédant à **Administration** > **Vue d'ensemble** > **Configuration du site** > **Sites**. Ouvrez **Paramètres de hiérarchie**, puis sélectionnez le niveau de données que vous voulez utiliser.

## Niveau 1 - De base

Le niveau De base comprend les données relatives à votre hiérarchie, qui sont nécessaires pour aider à améliorer votre expérience d'installation ou de mise à niveau, ainsi que des données pour aider à identifier les mises à jour Configuration Manager qui s'appliquent à votre hiérarchie.

Pour System Center Configuration Manager version 1710, ce niveau inclut les éléments suivants :

- Console d'administration :
  - Statistiques sur les connexions de la console (version, langue, référence (SKU) et architecture du système d'exploitation, mémoire système, nombre de processeurs logiques, ID du site de connexion, versions .NET installées et modules linguistiques de la console)
- Nombres de types d'application et de déploiement de base (nombre total d'applications, nombre total d'applications avec plusieurs types de déploiement, nombre total d'applications avec des dépendances, nombre total d'applications remplacées, nombre de technologies de déploiement utilisées)
- Données de la hiérarchie des sites Configuration Manager de base (liste des sites, type, version, état, nombre

de clients et fuseau horaire)

- Configuration de base de données simple (processeurs, configuration du cluster et configuration des vues distribuées)
- Statistiques élémentaires de découverte (nombre de découvertes et tailles de groupe minimum/maximum/moyenne), notamment quand le site est entièrement exécuté avec les services Active Directory Azure.
- Informations Endpoint Protection de base (versions du client de logiciel anti-programme malveillant)
- Nombre de déploiements de systèmes d'exploitation de base (images)
- Informations de serveur de système de site de base (rôles de système de site utilisés, état SSL et Internet, système d'exploitation, processeurs, ordinateur physique ou machine virtuelle, et utilisation de la haute disponibilité de serveur de site)
- Schéma de base de données Configuration Manager (hachage de toutes les définitions d'objet)
- Niveau de télémétrie configuré, mode (en ligne ou hors connexion) et configuration de la mise à jour rapide
- Nombre de paramètres régionaux et de langues du client
- ***[Mise à jour]*** Nombre de versions du client Configuration Manager, de versions du système d'exploitation et de versions d'Office
- Nombre de systèmes d'exploitation des appareils gérés et stratégies définies par le connecteur Exchange
- Nombre d'appareils Windows 10 par branche et build
- Métriques de performances de base de données (informations sur le traitement de la réplication, procédures stockées SQL Server les plus utilisées par processeur et utilisation des disques)
- Types de point de distribution et de point de gestion, et informations de configuration de base (protégés, préparés, PXE, de multidiffusion, d'état SSL, points de distribution pairs/d'extraction, compatibles MDM, compatibles SSL, etc.)
- Liste hachée d'extensions des Assistants et pages de propriétés de console Administrateur
- Informations d'installation :
  - Build, type d'installation, modules linguistiques, fonctionnalités que vous avez activées
  - Utilisation en préversion, type de support de configuration, type de branche
  - Date d'expiration de Software Assurance
  - État et erreurs du déploiement du package de mise à jour, progression du téléchargement, et erreurs liées aux prérequis
  - Utilisation de l'anneau rapide de mise à jour
  - Version du script après mise à niveau
- Version SQL, niveau de Service Pack, édition, ID de classement et jeu de caractères
- Statistiques de télémétrie (à l'exécution, runtime, erreurs)
- Utilisation de la découverte du réseau (activée ou désactivée)

## Niveau 2 – Étendu

Le niveau Étendu est configuré par défaut après l'installation. Ce niveau comprend les données collectées au

niveau De base, ainsi que les données spécifiques aux fonctionnalités (fréquence et durée d'utilisation), les paramètres du client Configuration Manager (nom du composant, état et paramètres, comme les intervalles d'interrogation) et les informations de base sur les mises à jour logicielles.

Ce niveau est recommandé, car il fournit à Microsoft les données minimales nécessaires pour apporter des améliorations utiles dans les futures versions des produits et services. Ce niveau ne collecte pas les noms des objets (sites, utilisateurs, ordinateur ou objets), les informations sur les objets relatifs à la sécurité ni les vulnérabilités, comme le nombre de systèmes qui nécessitent des mises à jour logicielles.

Pour System Center Configuration Manager version 1710, ce niveau inclut les éléments suivants :

- **Gestion des applications :**
    - Exigences pour les applications (le nombre de conditions prédéfinies est référencé par la technologie de déploiement)
    - Remplacement des applications, profondeur de chaîne maximale
    - Statistiques d'approbation de l'application et fréquence d'utilisation
    - Statistiques sur les tailles de contenu d'application
    - Informations de déploiement d'application (utilisation de l'installation par rapport à la désinstallation, approbation requise, interaction utilisateur activée/désactivée, dépendance, remplacement et nombre d'utilisations de la fonctionnalité de comportement à l'installation)
    - Statistiques de taille et de complexité des stratégies d'applications
    - Statistiques de demande d'application disponibles
    - Informations de configuration de base pour les packages et les programmes (options de déploiement et indicateurs de programme)
    - Informations de base d'utilisation/de ciblage pour les types de déploiement utilisés au sein de l'organisation (ciblé utilisateur ou appareil, nécessaire ou disponible, et applications universelles)
    - Statistiques des groupes de limites (nombre de rapides, nombre de lents, nombre par groupe)
    - Nombre d'environnements App-V et propriétés de déploiement
    - Nombre d'applicabilités de l'application par système d'exploitation
    - Nombre d'applications référencées par une séquence de tâches
    - Nombre de personnalisations distinctes pour le catalogue d'applications
    - Nombre d'applications Office 365 créées à l'aide du tableau de bord
    - Nombre de packages par type
    - Nombre de déploiements de package/programme
    - Nombre de licences d'application Windows 10 concédées
    - Nombre de types de déploiement Windows Installer par paramètres du contenu de désinstallation
    - Nombre d'applications du Microsoft Store pour Entreprises et statistiques de synchronisation (notamment un résumé des types d'applications, l'état des applications sous licence ainsi que le nombre d'applications sous licence en ligne et hors connexion)
    - Type et durée de fenêtre de maintenance
    - Nombre minimal/maximal/moyen de déploiements d'applications par utilisateur/appareil par période

- Codes d'erreur d'installation d'application les plus courants par technologie de déploiement
- Options de configuration MSI et nombres
- Statistiques sur l'interaction de l'utilisateur final avec notification des déploiements de logiciels requis
- Utilisation et mode de création d'Universal Data Access (UDA)

- **Client :**
  - Version du client AMT (Active Management Technology)
  - Âge du BIOS en années
  - Nombre d'appareils avec démarrage sécurisé
  - Nombre d'appareils par état TPM
  - Mise à niveau automatique du client : configuration du déploiement, notamment le test du client et l'utilisation de l'exclusion (client d'interopérabilité étendue)
  - Configuration de la taille du cache du client
  - Erreurs de téléchargement de déploiement des clients
  - Statistiques d'intégrité du client et récapitulatif des problèmes principaux
  - État des actions de notification du client (nombre d'exécutions de chaque action, nombre maximal de clients ciblés et taux de réussite moyen)
  - Nombre d'installations de client à partir de chaque type d'emplacement source
  - Nombre d'échecs d'installation de client
  - Nombre d'appareils virtualisés par Hyper-V ou Azure
  - Nombre d'actions du Centre logiciel
  - Nombre d'appareils compatibles UEFI
  - Méthodes de déploiement utilisées pour le client et nombre de clients par méthode de déploiement
  - Liste/nombre d'agents clients activés
  - Ancienneté du système d'exploitation en mois
  - Nombre de classes d'inventaire matériel, règles d'inventaire logiciel et règles de regroupement de fichiers
  - Statistiques pour l'attestation de l'intégrité des appareils, notamment les codes d'erreur les plus courants, le nombre de serveurs locaux et le nombre d'appareils dans différents états.
- **Services cloud :**
  - Statistiques de découverte Azure Active Directory
  - Statistiques de configuration et d'utilisation de la passerelle de gestion cloud, notamment le nombre de régions et d'environnements, et statistiques d'authentification/autorisation
  - Nombre d'applications et services Azure Active Directory connectés à Configuration Manager
  - Nombre de clients joints aux services Azure Active Directory
  - Nombre de regroupements qui sont synchronisés avec Operations Management Suite

- Nombre de connecteurs Upgrade Analytics
- Activation ou non du connecteur cloud Operations Management Suite

- ***[Nouveau]*** Cogestion
  - ***[Nouveau]*** Statistiques d'utilisation agrégées de la cogestion, comprenant le nombre de clients inscrits, les clients recevant la stratégie, les états de la charge de travail, les tailles des regroupements de pilotes/à exclure, les erreurs d'inscription
  - ***[Nouveau]*** Nombre de clients par méthode d'inscription à la cogestion
  - ***[Nouveau]*** Statistiques d'erreurs pour l'inscription à la cogestion
  - ***[Nouveau]*** Planification de l'inscription et statistiques historiques
  - ***[Nouveau]*** Nombre de clients éligibles à la cogestion
  - ***[Nouveau]*** Locataire Intune associé
- **Regroupements :**
  - Utilisation des ID de regroupement (ne pas manquer d'ID)
  - Statistiques d'évaluation des regroupements (durée des requêtes, nombre de regroupements affectés et non affectés, nombres par type, substitution d'ID et utilisation des règles)
  - Regroupements sans déploiement
- **Paramètres de compatibilité :**
  - Informations de la ligne de base de configuration de base (nombre, nombre de déploiements et nombre de références)
  - Statistiques d'erreurs de stratégie de conformité
  - Nombre d'éléments de configuration par type
  - Nombre de déploiements qui référencent des paramètres prédéfinis (avec capture du paramètre de correction)
  - Nombre de règles et de déploiements créés pour les paramètres personnalisés (avec capture du paramètre de correction)
  - Nombre de modèles SCEP (Simple Certificate Enrollment Protocol), VPN, Wi-Fi, de certificat (.pfx) et de stratégie de conformité déployés
  - Nombre de déploiements de certificat SCEP, VPN, Wi-Fi, certificat (.pfx) et stratégie de conformité par plateforme
  - Stratégie Passport for Work (créée, déployée)
- **Contenu :**
  - Informations sur les groupes de limites (nombre de limites et de systèmes de site qui sont attribués à chaque groupe de limites)
  - Relations de groupes de limites et configuration de secours
  - Statistiques de téléchargement du contenu client
  - Nombre de limites par type
  - Nombre de clients de cache d'homologue, statistiques d'utilisation et statistiques de téléchargements partiels
  - Informations sur la configuration du gestionnaire de distribution (threads, délai de nouvelle tentative,

nombre de nouvelles tentatives et paramètres de point de distribution d'extraction)

- Informations sur la configuration des points de distribution (utilisation de BranchCache et surveillance des points de distribution)
- Informations sur les groupes de points de distribution (nombre de packages et de points de distribution qui sont affectés à chaque groupe de points de distribution)

- **Endpoint Protection :**
  - Nombre de stratégies ATP (Advanced Threat Protection) (nombre de stratégies et si elles sont ou non déployées)
  - Nombre d'alertes configurées pour la fonctionnalité Endpoint Protection
  - Nombre de regroupements sélectionnés pour être affichés dans le tableau de bord Endpoint Protection
  - ***[Nouveau]*** Nombre de stratégies, de déploiements et de clients ciblés Windows Defender Exploit Guard
  - Erreurs de déploiement Endpoint Protection (nombre de codes d'erreur de déploiement de stratégie Endpoint Protection)
  - Utilisation des stratégies du Pare-feu Windows et de logiciel anti-programme malveillant Endpoint Protection (nombre de stratégies uniques affectées au groupe)

    Ceci ne comprend pas d'informations sur les paramètres inclus dans la stratégie.
- **Migration :**
  - Nombre d'objets migrés (utilisation de l'Assistant Migration)
- **Gestion des appareils mobiles (MDM) :**
  - Nombre d'actions d'appareil mobile émises : commandes de verrouillage, de réinitialisation, de mise hors service et Synchroniser maintenant
  - Nombre de stratégies d'appareil mobile
  - Nombre d'appareils mobiles gérés par Configuration Manager et Microsoft Intune, et méthode d'inscription (en bloc ou basée sur l'utilisateur)
  - Nombre d'utilisateurs qui ont plusieurs appareils mobiles inscrits
  - Statistiques et calendrier d'interrogation des appareils mobiles pour la durée d'inscription des appareils mobiles
- **Dépannage de Microsoft Intune :**
  - Nombre et taille des messages d'actions d'appareil (réinitialiser, mettre hors service, verrouiller), de télémétrie et de données qui sont répliqués vers Microsoft Intune
  - Nombre et taille des messages d'état, de statut, d'inventaire, RDR, DDR, UDX, d'état de locataire, POL, LOG, de certificat, CRP, de resynchronisation, CFD, RDO, BEX, ISM et de conformité qui sont téléchargés à partir de Microsoft Intune
  - Statistiques de synchronisation utilisateur complète et différentielle pour Microsoft Intune
- **Gestion des appareils mobiles (MDM) locale :**
  - Nombre de profils et de packages d'inscription en bloc Windows 10

- Statistiques de réussite/échec de déploiement pour les déploiements d'applications de gestion MDM locale

- **Déploiement du système d'exploitation :**
  - Nombre d'images de démarrage, de pilotes, de packages de pilotes, de points de distribution en multidiffusion, de points de distribution compatibles PXE et de séquences de tâches
  - Nombre d'images de démarrage par version cliente de Configuration Manager
  - Nombre d'images de démarrage par version de Windows PE
  - Nombre de stratégies de mise à niveau d'édition
  - Nombre d'identificateurs de matériel exclus de PXE
  - ***[Nouveau]*** Nombre de déploiement du système d'exploitation par version de système d'exploitation
  - ***[Nouveau]*** Nombre de mises à niveau du système d'exploitation au fil du temps
  - Nombre de déploiements de séquences de tâches utilisant l'option de prétéléchargement du contenu
  - Nombre d'utilisations des étapes de séquence de tâches
  - Version de Windows ADK installée
- **Mises à jour du site :**
  - Versions des correctifs logiciels de Configuration Manager installés
- **Mises à jour logicielles :**
  - Différentiels de disponibilité et d'échéance qui sont utilisés dans les règles de déploiement automatique
  - Nombre moyen et maximal d'attributions par mise à jour
  - Calendriers d'analyse et d'évaluation des mises à jour client
  - Classifications qui sont synchronisées par le point de mise à jour logicielle
  - Statistiques d'application de correctifs logiciels au cluster
  - Configuration des mises à jour rapides de Windows 10
  - Configurations qui sont utilisées pour les plans de maintenance actifs de Windows 10
  - Nombre de mises à jour Office 365 déployées
  - Nombre de pilotes Microsoft Surface synchronisés
  - Nombre de groupes et d'attributions de mises à jour
  - Nombre de packages de mises à jour et nombre maximal/minimal/moyen de points de distribution qui sont ciblés par les packages
  - Nombre de mises à jour créées et déployées avec System Center Update Publisher
  - Nombre de clients Windows 10 qui utilisent Windows Update for Business
  - Nombre de stratégies Windows Update for Business créées et déployées
  - Nombre de règles de déploiement automatique qui sont liées à la synchronisation
  - Nombre de règles de déploiement automatique qui créent de nouvelles mises à jour ou ajoutent des mises à jour à un groupe existant

- Nombre de règles de déploiement automatique avec plusieurs déploiements
- Nombre de groupes de mises à jour et nombre minimal/maximal/moyen de mises à jour par groupe
- Nombre de mises à jour et pourcentage de mises à jour qui sont déployées, expirées, remplacées, téléchargées et qui contiennent des CLUF
- Statistiques d'équilibrage de charge du point de mise à jour logicielle
- Planification de la synchronisation du point de mise à jour logicielle
- Nombre total/moyen de regroupements comportant des déploiements de mises à jour logicielles et nombre maximal/moyen de mises à jour déployées
- Codes d'erreur d'analyse des mises à jour et nombre d'ordinateurs
- Versions de contenu du tableau de bord Windows 10

- **Données de performances/SQL :**
  - Configuration et durée de la synthèse du site
  - Nombre des plus grandes tables de base de données
  - Statistiques opérationnelles de découverte (nombre d'objets trouvés)
  - Types de découverte, activés et planifiés (complète, incrémentielle)
  - Informations sur les réplicas SQL AlwaysOn, utilisation et état d'intégrité
  - Problèmes de performances du suivi des modifications SQL, période de rétention et état de nettoyage automatique
  - Période de rétention du suivi des modifications SQL
  - Statistiques de performances des messages d'état et de statut, notamment les types de messages les plus courants et les plus coûteux

- **Divers**
  - Configuration du Point de service de l'entrepôt de données, notamment la planification de la synchronisation et le délai moyen
  - Nombre de scripts et statistiques d'exécution
  - Nombre de sites avec Wake On Lan (WOL)
  - Statistiques de performances et d'utilisation des rapports

## Niveau 3 – Complet

Le niveau Complet inclut toutes les données des niveaux De base et Étendu. Il inclut également des informations supplémentaires sur Endpoint Protection, les pourcentages de compatibilité des mises à jour et les informations de mise à jour logicielle. Ce niveau peut également inclure des informations de diagnostic avancées telles que des fichiers système et des instantanés de la mémoire, qui peuvent inclure des informations personnelles qui existaient dans la mémoire ou les fichiers journaux au moment de la capture.

Pour System Center Configuration Manager version 1710, ce niveau inclut les éléments suivants :

- Informations sur le calendrier d'évaluation de règle de déploiement automatique
- Récapitulatif d'intégrité ATP

- Statistiques d'évaluation et d'actualisation des regroupements
- Statistiques de stratégie de conformité pour les erreurs et la conformité
- Paramètres de conformité : détails de configuration des modèles SCEP, VPN, Wi-Fi et stratégie de conformité, nombre de groupes avec des mises à jour logicielles expirées
- Pack de configuration DCM pour l'utilisation de System Center Configuration Manager
- Détails des erreurs d'installation du déploiement des clients
- Récapitulatif de l'intégrité Endpoint Protection (y compris le nombre de clients protégés, présentant un risque, inconnus et non pris en charge)
- Configuration de la stratégie Endpoint Protection
- Liste des processus configurés avec le comportement à l'installation des applications
- Nombre minimal/maximal/moyen d'heures depuis la dernière analyse des mises à jour logicielles
- Nombre minimal/maximal/moyen de clients inactifs dans les regroupements de déploiements de mise à jour logicielle
- Nombre minimal/maximal/moyen de mises à jour logicielles par package
- Code de produit MSI (applications courantes que les clients déploient)
- Compatibilité globale des déploiements de mise à jour logicielle
- Nombres et codes d'erreur de déploiement de mise à jour logicielle
- Informations de déploiement de mise à jour logicielle (pourcentage de déploiements ciblés avec le client ou l'heure UTC, obligatoire/facultatif/en mode silencieux, et suppression du redémarrage)
- Produits des mises à jour logicielles synchronisés par le point de mise à jour logicielle
- Pourcentages de réussite d'analyse des mises à jour logicielles
- 50 premières unités centrales dans l'environnement
- Type de stratégies d'accès conditionnel EAS (bloquer ou mettre en quarantaine) pour les appareils gérés par Intune
- Détails des applications du Microsoft Store pour Entreprises (liste de non-agrégation des applications synchronisées, notamment l'ID de l'application, l'état (en ligne ou hors connexion) et le nombre total de licences achetées)

# Niveaux de la collecte de données des données de diagnostic et d'utilisation pour la version 1706 de System Center Configuration Manager

22/06/2018 • 25 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

System Center Configuration Manager version 1706 collecte trois niveaux de données d'utilisation et de diagnostic : **De base**, **Étendu** et **Complet**. Par défaut, cette fonctionnalité est définie sur le niveau Étendu. Les sections suivantes fournissent des détails supplémentaires sur les données collectées par chaque niveau.

Les modifications par rapport aux versions précédentes sont indiquées par ***[Nouveau]***, ***[Mis à jour]***, ***[Supprimé]*** ou ***[Déplacé]***.

> **IMPORTANT**
> Configuration Manager ne collecte pas les codes des sites, les noms des sites, les adresses IP, les noms d'utilisateur ou d'ordinateur, les adresses physiques ni les adresses e-mail aux niveaux De base et Étendu. Toute collecte de ces informations au niveau Complet n'est pas intentionnelle : elles peuvent être incluses dans des informations de diagnostic avancées comme des fichiers journaux ou des instantanés de la mémoire. Microsoft n'utilisera pas ces informations pour vous identifier ou vous contacter, ni à des fins publicitaires.

## Modification du niveau

Les administrateurs qui ont une étendue d'administration basée sur des rôles incluant les autorisations **Modifier** sur la classe d'objets **Site** peuvent changer le niveau des données collectées dans les paramètres des données de diagnostic et d'utilisation de la console Configuration Manager.

Vous pouvez changer le niveau de collecte des données à partir de la console en accédant à **Administration** > **Vue d'ensemble** > **Configuration du site** > **Sites**. Ouvrez **Paramètres de hiérarchie**, puis sélectionnez le niveau de données que vous voulez utiliser.

## Niveau 1 - De base

Le niveau De base comprend les données relatives à votre hiérarchie, qui sont nécessaires pour aider à améliorer votre expérience d'installation ou de mise à niveau, ainsi que des données pour aider à identifier les mises à jour Configuration Manager qui s'appliquent à votre hiérarchie.

Pour System Center Configuration Manager version 1706, ce niveau inclut les éléments suivants :

- Console d'administration :
  - Statistiques sur les connexions de la console (version, langue, référence (SKU) et architecture du système d'exploitation, mémoire système, nombre de processeurs logiques, ID du site de connexion, versions .NET installées et modules linguistiques de la console)
- Nombres de types d'application et de déploiement de base (nombre total d'applications, nombre total d'applications avec plusieurs types de déploiement, nombre total d'applications avec des dépendances, nombre total d'applications remplacées, nombre de technologies de déploiement utilisées)
- Données de la hiérarchie des sites Configuration Manager de base (liste des sites, type, version, état, nombre

de clients et fuseau horaire)

- Configuration de base de données simple (processeurs, configuration du cluster et configuration des vues distribuées)
- Statistiques élémentaires de découverte (nombre de découvertes et tailles de groupe minimum/maximum/moyenne), notamment quand le site est entièrement exécuté avec les services Active Directory Azure.
- Informations Endpoint Protection de base (versions du client de logiciel anti-programme malveillant)
- Nombre de déploiements de systèmes d'exploitation de base (images)
- ***[Mis à jour]*** Informations de serveur de système de site de base (rôles de système de site utilisés, état SSL et Internet, système d'exploitation, processeurs, ordinateur physique ou machine virtuelle, et utilisation de la haute disponibilité de serveur de site)
- Schéma de base de données Configuration Manager (hachage de toutes les définitions d'objet)
- Niveau de télémétrie configuré, mode (en ligne ou hors connexion) et configuration de la mise à jour rapide
- Nombre de paramètres régionaux et de langues du client
- Nombre de versions du client Configuration Manager et de versions du système d'exploitation
- Nombre de systèmes d'exploitation des appareils gérés et stratégies définies par le connecteur Exchange
- Nombre d'appareils Windows 10 par branche et build
- Métriques de performances de base de données (informations sur le traitement de la réplication, procédures stockées SQL Server les plus utilisées par processeur et utilisation des disques)
- Types de point de distribution et de point de gestion, et informations de configuration de base (protégés, préparés, PXE, de multidiffusion, d'état SSL, points de distribution pairs/d'extraction, compatibles MDM, compatibles SSL, etc.)
- ***[Nouveau]*** Liste hachée d'extensions des Assistants et pages de propriétés de console Administrateur
- Informations d'installation :
  - Build, type d'installation, modules linguistiques, fonctionnalités que vous avez activées
  - Utilisation en préversion, type de support de configuration, type de branche
  - Date d'expiration de Software Assurance
  - État et erreurs du déploiement du package de mise à jour, progression du téléchargement, et erreurs liées aux prérequis
  - Utilisation de l'anneau rapide de mise à jour
  - Version du script après mise à niveau
- Version SQL, niveau de Service Pack, édition, ID de classement et jeu de caractères
- Statistiques de télémétrie (à l'exécution, runtime, erreurs)
- Utilisation de la découverte du réseau (activée ou désactivée)

## Niveau 2 – Étendu

Le niveau Étendu est configuré par défaut après l'installation. Ce niveau comprend les données collectées au niveau De base, ainsi que les données spécifiques aux fonctionnalités (fréquence et durée d'utilisation), les

paramètres du client Configuration Manager (nom du composant, état et paramètres, comme les intervalles d'interrogation) et les informations de base sur les mises à jour logicielles.

Ce niveau est recommandé, car il fournit à Microsoft les données minimales nécessaires pour apporter des améliorations utiles dans les futures versions des produits et services. Ce niveau ne collecte pas les noms des objets (sites, utilisateurs, ordinateur ou objets), les informations sur les objets relatifs à la sécurité ni les vulnérabilités, comme le nombre de systèmes qui nécessitent des mises à jour logicielles.

Pour System Center Configuration Manager version 1706, ce niveau inclut les éléments suivants :

- **Gestion des applications :**
  - Exigences pour les applications (le nombre de conditions prédéfinies est référencé par la technologie de déploiement)
  - Remplacement des applications, profondeur de chaîne maximale
  - Statistiques d'approbation de l'application et fréquence d'utilisation
  - ***[Nouveau]*** Statistiques sur les tailles de contenu d'application
  - Informations de déploiement d'application (utilisation de l'installation par rapport à la désinstallation, approbation requise, interaction utilisateur activée/désactivée, dépendance, remplacement et nombre d'utilisations de la fonctionnalité de comportement à l'installation)
  - Statistiques de taille et de complexité des stratégies d'applications
  - Statistiques de demande d'application disponibles
  - Informations de configuration de base pour les packages et les programmes (options de déploiement et indicateurs de programme)
  - Informations de base d'utilisation/de ciblage pour les types de déploiement utilisés au sein de l'organisation (ciblé utilisateur ou appareil, nécessaire ou disponible, et applications universelles)
  - Statistiques des groupes de limites (nombre de rapides, nombre de lents, nombre par groupe)
  - Nombre d'environnements App-V et propriétés de déploiement
  - Nombre d'applicabilités de l'application par système d'exploitation
  - Nombre d'applications référencées par une séquence de tâches
  - ***[Nouveau]*** Nombre de personnalisations distinctes pour le catalogue d'applications
  - ***[Nouveau]*** Nombre d'applications Office 365 créées à l'aide du tableau de bord
  - Nombre de packages par type
  - Nombre de déploiements de package/programme
  - Nombre de licences d'application Windows 10 concédées
  - ***[Nouveau]*** Nombre de types de déploiement Windows Installer par paramètres du contenu de désinstallation
  - Nombre d'applications Windows Store pour Entreprises et statistiques de synchronisation (notamment un résumé des types d'applications, l'état des applications sous licence ainsi que le nombre d'applications sous licence en ligne et hors connexion)
  - Type et durée de fenêtre de maintenance
  - Nombre minimal/maximal/moyen de déploiements d'applications par utilisateur/appareil par période

- Codes d'erreur d'installation d'application les plus courants par technologie de déploiement
- Options de configuration MSI et nombres
- Statistiques sur l'interaction de l'utilisateur final avec notification des déploiements de logiciels requis
- Utilisation et mode de création d'Universal Data Access (UDA)

- **Client :**
  - Version du client AMT (Active Management Technology)
  - Âge du BIOS en années
  - ***[Nouveau]*** Nombre d'appareils avec démarrage sécurisé
  - ***[Nouveau]*** Nombre d'appareils par état TPM
  - Mise à niveau automatique du client : configuration du déploiement, notamment le test du client et l'utilisation de l'exclusion (client d'interopérabilité étendue)
  - Configuration de la taille du cache du client
  - Erreurs de téléchargement de déploiement des clients
  - Statistiques d'intégrité du client et récapitulatif des problèmes principaux
  - État des actions de notification du client (nombre d'exécutions de chaque action, nombre maximal de clients ciblés et taux de réussite moyen)
  - Nombre d'installations de client à partir de chaque type d'emplacement source
  - Nombre d'échecs d'installation de client
  - Nombre d'appareils virtualisés par Hyper-V ou Azure
  - Nombre d'actions du Centre logiciel
  - Nombre d'appareils compatibles UEFI
  - Méthodes de déploiement utilisées pour le client et nombre de clients par méthode de déploiement
  - Liste/nombre d'agents clients activés
  - Ancienneté du système d'exploitation en mois
  - Nombre de classes d'inventaire matériel, règles d'inventaire logiciel et règles de regroupement de fichiers
  - Statistiques pour l'attestation de l'intégrité des appareils, notamment les codes d'erreur les plus courants, le nombre de serveurs locaux et le nombre d'appareils dans différents états.
- **Services cloud :**
  - ***[Nouveau]*** Statistiques de découverte Azure Active Directory
  - ***[Mis à jour]*** Statistiques de configuration et d'utilisation de la passerelle de gestion cloud, notamment le nombre de régions et d'environnements, et statistiques d'authentification/autorisation
  - ***[Nouveau]*** Nombre d'applications et services Azure Active Directory connectés à Configuration Manager
  - Nombre de clients joints aux services Azure Active Directory
  - Nombre de regroupements qui sont synchronisés avec Operations Management Suite

- Nombre de connecteurs Upgrade Analytics
- Activation ou non du connecteur cloud Operations Management Suite

- **Regroupements :**
  - Utilisation des ID de regroupement (ne pas manquer d'ID)
  - Statistiques d'évaluation des regroupements (durée des requêtes, nombre de regroupements affectés et non affectés, nombres par type, substitution d'ID et utilisation des règles)
  - Regroupements sans déploiement
- **Paramètres de compatibilité :**
  - Informations de la ligne de base de configuration de base (nombre, nombre de déploiements et nombre de références)
  - ***[Nouveau]*** Statistiques d'erreurs de stratégie de conformité
  - Nombre d'éléments de configuration par type
  - Nombre de déploiements qui référencent des paramètres prédéfinis (avec capture du paramètre de correction)
  - Nombre de règles et de déploiements créés pour les paramètres personnalisés (avec capture du paramètre de correction)
  - Nombre de modèles SCEP (Simple Certificate Enrollment Protocol), VPN, Wi-Fi, de certificat (.pfx) et de stratégie de conformité déployés
  - Nombre de déploiements de certificat SCEP, VPN, Wi-Fi, certificat (.pfx) et stratégie de conformité par plateforme
  - Stratégie Passport for Work (créée, déployée)
- **Contenu :**
  - Informations sur les groupes de limites (nombre de limites et de systèmes de site qui sont attribués à chaque groupe de limites)
  - Relations de groupes de limites et configuration de secours
  - Statistiques de téléchargement du contenu client
  - Nombre de limites par type
  - ***[Mis à jour]*** Nombre de clients de cache d'homologue, statistiques d'utilisation et statistiques de téléchargements partiels
  - Informations sur la configuration du gestionnaire de distribution (threads, délai de nouvelle tentative, nombre de nouvelles tentatives et paramètres de point de distribution d'extraction)
  - Informations sur la configuration des points de distribution (utilisation de BranchCache et surveillance des points de distribution)
  - Informations sur les groupes de points de distribution (nombre de packages et de points de distribution qui sont affectés à chaque groupe de points de distribution)
- **Endpoint Protection :**
  - Nombre de stratégies ATP (Advanced Threat Protection) (nombre de stratégies et si elles sont ou non déployées)

- Nombre d'alertes configurées pour la fonctionnalité Endpoint Protection
- Nombre de regroupements sélectionnés pour être affichés dans le tableau de bord Endpoint Protection
- Erreurs de déploiement Endpoint Protection (nombre de codes d'erreur de déploiement de stratégie Endpoint Protection)
- Utilisation des stratégies du Pare-feu Windows et de logiciel anti-programme malveillant Endpoint Protection (nombre de stratégies uniques affectées au groupe)

  Ceci ne comprend pas d'informations sur les paramètres inclus dans la stratégie.

- **Migration :**
  - Nombre d'objets migrés (utilisation de l'Assistant Migration)
- **Gestion des appareils mobiles (MDM) :**
  - Nombre d'actions d'appareil mobile émises : commandes de verrouillage, de réinitialisation, de mise hors service et Synchroniser maintenant
  - Nombre de stratégies d'appareil mobile
  - Nombre d'appareils mobiles gérés par Configuration Manager et Microsoft Intune, et méthode d'inscription (en bloc ou basée sur l'utilisateur)
  - Nombre d'utilisateurs qui ont plusieurs appareils mobiles inscrits
  - Statistiques et calendrier d'interrogation des appareils mobiles pour la durée d'inscription des appareils mobiles
- **Dépannage de Microsoft Intune :**
  - Nombre et taille des messages d'actions d'appareil (réinitialiser, mettre hors service, verrouiller), de télémétrie et de données qui sont répliqués vers Microsoft Intune
  - Nombre et taille des messages d'état, de statut, d'inventaire, RDR, DDR, UDX, d'état de locataire, POL, LOG, de certificat, CRP, de resynchronisation, CFD, RDO, BEX, ISM et de conformité qui sont téléchargés à partir de Microsoft Intune
  - Statistiques de synchronisation utilisateur complète et différentielle pour Microsoft Intune
- **Gestion des appareils mobiles (MDM) locale :**
  - Nombre de profils et de packages d'inscription en bloc Windows 10
  - Statistiques de réussite/échec de déploiement pour les déploiements d'applications de gestion MDM locale
- **Déploiement du système d'exploitation :**
  - Nombre d'images de démarrage, de pilotes, de packages de pilotes, de points de distribution en multidiffusion, de points de distribution compatibles PXE et de séquences de tâches
  - ***[Nouveau]*** Nombre d'images de démarrage par version cliente de Configuration Manager
  - ***[Nouveau]*** Nombre d'images de démarrage par version de Windows PE
  - Nombre de stratégies de mise à niveau d'édition
  - ***[Nouveau]*** Nombre d'identificateurs de matériel exclus de PXE

- ***[Nouveau]*** Nombre de déploiements de séquences de tâches utilisant l'option de prétéléchargement du contenu
- Nombre d'utilisations des étapes de séquence de tâches
- ***[Nouveau]*** Version de Windows ADK installée

- **Mises à jour du site :**
  - Versions des correctifs logiciels de Configuration Manager installés
- **Mises à jour logicielles :**
  - Différentiels de disponibilité et d'échéance qui sont utilisés dans les règles de déploiement automatique
  - Nombre moyen et maximal d'attributions par mise à jour
  - Calendriers d'analyse et d'évaluation des mises à jour client
  - Classifications qui sont synchronisées par le point de mise à jour logicielle
  - Statistiques d'application de correctifs logiciels au cluster
  - Configuration des mises à jour rapides de Windows 10
  - Configurations qui sont utilisées pour les plans de maintenance actifs de Windows 10
  - Nombre de mises à jour Office 365 déployées
  - ***[Nouveau]*** Nombre de pilotes Microsoft Surface synchronisés
  - Nombre de groupes et d'attributions de mises à jour
  - Nombre de packages de mises à jour et nombre maximal/minimal/moyen de points de distribution qui sont ciblés par les packages
  - Nombre de mises à jour créées et déployées avec System Center Update Publisher
  - Nombre de clients Windows 10 qui utilisent Windows Update for Business
  - ***[Nouveau]*** Nombre de stratégies Windows Update for Business créées et déployées
  - Nombre de règles de déploiement automatique qui sont liées à la synchronisation
  - Nombre de règles de déploiement automatique qui créent de nouvelles mises à jour ou ajoutent des mises à jour à un groupe existant
  - Nombre de règles de déploiement automatique avec plusieurs déploiements
  - Nombre de groupes de mises à jour et nombre minimal/maximal/moyen de mises à jour par groupe
  - Nombre de mises à jour et pourcentage de mises à jour qui sont déployées, expirées, remplacées, téléchargées et qui contiennent des CLUF
  - Statistiques d'équilibrage de charge du point de mise à jour logicielle
  - Planification de la synchronisation du point de mise à jour logicielle
  - Nombre total/moyen de regroupements comportant des déploiements de mises à jour logicielles et nombre maximal/moyen de mises à jour déployées
  - Codes d'erreur d'analyse des mises à jour et nombre d'ordinateurs
  - Versions de contenu du tableau de bord Windows 10

- **Données de performances/SQL :**
  - ***[Nouveau]*** Configuration et durée de la synthèse du site
  - Nombre des plus grandes tables de base de données
  - Statistiques opérationnelles de découverte (nombre d'objets trouvés)
  - Types de découverte, activés et planifiés (complète, incrémentielle)
  - Informations sur les réplicas SQL AlwaysOn, utilisation et état d'intégrité
  - Problèmes de performances du suivi des modifications SQL, période de rétention et état de nettoyage automatique
  - Période de rétention du suivi des modifications SQL
  - Statistiques de performances des messages d'état et de statut, notamment les types de messages les plus courants et les plus coûteux
- **Divers**
  - Configuration du Point de service de l'entrepôt de données, notamment la planification de la synchronisation et le délai moyen
  - ***[Nouveau]*** Nombre de scripts et statistiques d'exécution
  - Nombre de sites avec Wake On Lan (WOL)
  - Statistiques de performances et d'utilisation des rapports

## Niveau 3 – Complet

Le niveau Complet inclut toutes les données des niveaux De base et Étendu. Il inclut également des informations supplémentaires sur Endpoint Protection, les pourcentages de compatibilité des mises à jour et les informations de mise à jour logicielle. Ce niveau peut également inclure des informations de diagnostic avancées, comme des fichiers système et des instantanés de la mémoire, qui peuvent inclure des informations personnelles qui existaient dans la mémoire ou les fichiers journaux au moment de la capture.

Pour System Center Configuration Manager version 1706, ce niveau inclut les éléments suivants :

- Informations sur le calendrier d'évaluation de règle de déploiement automatique
- Récapitulatif d'intégrité ATP
- Statistiques d'évaluation et d'actualisation des regroupements
- ***[Nouveau]*** Statistiques de stratégie de conformité pour les erreurs et la conformité
- Paramètres de conformité : détails de configuration des modèles SCEP, VPN, Wi-Fi et stratégie de conformité, nombre de groupes avec des mises à jour logicielles expirées
- Pack de configuration DCM pour l'utilisation de System Center Configuration Manager
- Détails des erreurs d'installation du déploiement des clients
- Récapitulatif de l'intégrité Endpoint Protection (y compris le nombre de clients protégés, présentant un risque, inconnus et non pris en charge)
- Configuration de la stratégie Endpoint Protection
- Liste des processus configurés avec le comportement à l'installation des applications

- Nombre minimal/maximal/moyen d'heures depuis la dernière analyse des mises à jour logicielles
- Nombre minimal/maximal/moyen de clients inactifs dans les regroupements de déploiements de mise à jour logicielle
- Nombre minimal/maximal/moyen de mises à jour logicielles par package
- Code de produit MSI (applications courantes que les clients déploient)
- Compatibilité globale des déploiements de mise à jour logicielle
- Nombres et codes d'erreur de déploiement de mise à jour logicielle
- Informations de déploiement de mise à jour logicielle (pourcentage de déploiements ciblés avec le client ou l'heure UTC, obligatoire/facultatif/en mode silencieux, et suppression du redémarrage)
- Produits des mises à jour logicielles synchronisés par le point de mise à jour logicielle
- Pourcentages de réussite d'analyse des mises à jour logicielles
- 50 premières unités centrales dans l'environnement
- Type de stratégies d'accès conditionnel EAS (bloquer ou mettre en quarantaine) pour les appareils gérés par Intune
- Détails des applications du Windows Store pour Entreprises (liste de non-agrégation des applications synchronisées, notamment l'ID de l'application, l'état (en ligne ou hors connexion) et le nombre total de licences achetées)

# Comment les données d'utilisation et de diagnostic sont collectées pour System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Pour collecter les données de diagnostic et d'utilisation pour System Center Configuration Manager, chaque site principal exécute des requêtes SQL Server à une fréquence hebdomadaire. Dans une hiérarchie multisite, les données sont répliquées vers le site d'administration centrale.

Sur le site de niveau supérieur d'une hiérarchie, le rôle système de site de point de connexion de service soumet ces informations quand il recherche des mises à jour. Le mode du point de connexion de service détermine comment les données sont transférées :

- **En mode en ligne :** les données d'utilisation et de diagnostic sont envoyées automatiquement une fois par semaine du point de connexion de service au service cloud.
- **En mode hors connexion :** les données d'utilisation et de diagnostic sont transférées manuellement à l'aide de l'outil de connexion de service. Pour plus d'informations, voir Utiliser l'outil de connexion de service pour System Center Configuration Manager.

Pour plus d'informations, voir À propos du point de connexion de service dans System Center Configuration Manager.

# Comment afficher les données d'utilisation et de diagnostic pour System Center Configuration Manager

22/06/2018 • 4 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez afficher les données d'utilisation et de diagnostic de votre hiérarchie System Center Configuration Manager pour vérifier qu'elle ne contient aucune information sensible ni identifiable. Les données de télémétrie sont résumées et stockées dans la table **TEL_TelemetryResults** de la base de données du site et mises en forme de manière à être utilisables et efficaces en programmation. Bien que les options suivantes vous offrent une vue des données exactes envoyées à Microsoft, celles-ci ne sont pas destinées à être utilisées à d'autres fins, comme l'analyse des données.

Utilisez la commande SQL suivante pour voir le contenu de cette table et afficher les données exactes qui sont envoyées. (Vous pouvez également exporter ces données dans un fichier texte.) :

- **SELECT * FROM TEL_TelemetryResults**

> **NOTE**
> Avant d'installer la version 1602, la table qui stocke les données de télémétrie est **TelemetryResults**.

Quand le point de connexion de service est en mode hors connexion, vous pouvez utiliser l'outil de connexion de service pour exporter les données d'utilisation et de diagnostic actives dans un fichier de valeurs séparées par des virgules (CSV). Exécutez l'outil de connexion de service sur le point de connexion de service en utilisant le paramètre **-Export**.

## Hachages unidirectionnels

Certaines données se composent de chaînes de caractères alphanumériques aléatoires. Configuration Manager utilise l'algorithme SHA-256, qui utilise le hachage à sens unique, pour garantir que nous ne collectons pas de données potentiellement sensibles. L'algorithme laisse les données dans un état où elles peuvent encore être utilisées à des fins de comparaison et de corrélation. Par exemple, au lieu de collecter les noms des tables dans la base de données de site, un hachage unidirectionnel est capturé pour chaque nom de table. Ceci garantit que les noms de tables personnalisés que vous avez créés ou que des modules complémentaires d'un produit ont créés ne sont pas visibles. Nous pouvons ensuite effectuer le même hachage à sens unique des noms des tables SQL fournis par défaut dans le produit et comparer les résultats de deux requêtes pour déterminer l'écart de votre schéma de base de données par rapport aux paramètres par défaut du produit. Cet écart est ensuite utilisé pour améliorer les mises à jour qui nécessitent des modifications du schéma SQL.

Lorsque vous affichez les données brutes, une valeur hachée apparaît dans chaque ligne de données. Il s'agit de l'ID de hiérarchie. Cette valeur hachée est utilisée pour garantir que les données sont corrélées avec la même hiérarchie, sans identification du client ou de la source.

**Pour voir comment fonctionne le hachage unidirectionnel**

1. Obtenez l'ID de votre hiérarchie en exécutant l'instruction SQL suivante dans SQL Management Studio sur la base de données Configuration Manager : **select [dbo].[fnGetHierarchyID]()**

2. Utilisez le script Windows PowerShell suivant pour réaliser le hachage en sens unique du GUID obtenu de

la base de données. Vous pouvez alors le comparer à l'ID de hiérarchie dans les données brutes pour voir comment nous masquons ces données.

```
Param( [Parameter(Mandatory=$True)] [string]$value )
  $guid = [System.Guid]::NewGuid()
  if( [System.Guid]::TryParse($value,[ref] $guid) -eq $true ) {
  #many of the values we hash are Guids
  $bytesToHash = $guid.ToByteArray()
} else {
  #otherwise hash as string (unicode)
  $ue = New-Object System.Text.UnicodeEncoding
  $bytesToHash = $ue.GetBytes($value)
}
  # Load Hash Provider (https://en.wikipedia.org/wiki/SHA-2)
$hashAlgorithm = [System.Security.Cryptography.SHA256Cng]::Create()
# Hash the input
$hashedBytes = $hashAlgorithm.ComputeHash($bytesToHash)
# Base64 encode the result for transport
$result = [Convert]::ToBase64String($hashedBytes)
return $result
```

# Programme d'amélioration des services (CEIP) pour System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

> **NOTE**
> À compter de Configuration Manager version 1802, la fonctionnalité CEIP ne figure plus dans le produit.

Lors de l'installation de la console de Configuration Manager, vous pouvez choisir de participer au **Programme d'amélioration de l'expérience utilisateur** (CEIP). Ce programme est désactivé par défaut. Il reste activé s'il l'était auparavant.

- Le programme CEIP est distinct des Données d'utilisation et de diagnostic pour System Center Configuration Manager.
- Le programme CEIP fonctionne console par console. Il collecte des données comme le nombre de fois que chaque élément est sélectionné dans l'interface utilisateur.
- Lisez la déclaration de confidentialité.

Modifiez les paramètres du programme CEIP pour chaque installation de console. Pour cela, accédez à l'onglet Backstage de la console (onglet supérieur gauche avec la flèche déroulante) et sélectionnez **Programme d'amélioration de l'expérience utilisateur**.

# Sécurité et confidentialité pour System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cet article inclut des ressources concernant la sécurité et la confidentialité pour System Center Configuration Manager.

Avant de poursuivre, assurez-vous de connaître les principes de base de System Center Configuration Manager. Si vous avez déjà installé System Center Configuration Manager, examinez les décisions de conception de votre mise en œuvre. Le calendrier et le contenu de déploiement de Configuration Manager pourront vous être utiles.

Consultez les articles suivants pour en savoir plus sur les fonctionnalités liées à la sécurité dans le produit :

- Sécurité et confidentialité du déploiement de systèmes d'exploitation dans System Center Configuration Manager
- Sécurité et confidentialité pour la gestion des applications dans System Center Configuration Manager
- Sécurité et confidentialité pour les mises à jour logicielles dans System Center Configuration Manager
- Sécurité et confidentialité des paramètres de compatibilité dans System Center Configuration Manager
- Endpoint Protection dans System Center Configuration Manager
- Sécurité et confidentialité pour les regroupements dans System Center Configuration Manager
- Sécurité et confidentialité pour les requêtes dans System Center Configuration Manager
- Sécurité et confidentialité pour la gestion de l'alimentation dans System Center Configuration Manager
- Sécurité et confidentialité pour le contrôle à distance dans System Center Configuration Manager
- Sécurité et confidentialité pour l'inventaire matériel dans System Center Configuration Manager
- Sécurité et confidentialité pour l'inventaire logiciel dans System Center Configuration Manager
- Sécurité et confidentialité pour Asset Intelligence dans System Center Configuration Manager
- Sécurité et confidentialité pour les rapports dans System Center Configuration Manager

**Articles relatifs à la sécurité et à la confidentialité :**

- Planifier la sécurité dans System Center Configuration Manager
- Configurer la sécurité dans System Center Configuration Manager
- Bonnes pratiques de sécurité et informations de confidentialité de System Center Configuration Manager
- Informations techniques de référence sur les contrôles de chiffrement pour System Center Configuration Manager
- Ports utilisés dans System Center Configuration Manager
- Comptes utilisés dans System Center Configuration Manager

# Planifier la sécurité dans System Center Configuration Manager

22/06/2018 • 45 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

## Planifier des certificats (auto-signés et PKI)

Configuration Manager utilise une combinaison de certificats auto-signés et de certificats pour infrastructure à clé publique (PKI).

Comme bonne pratique de sécurité, utilisez des certificats PKI dès que possible. Pour en savoir plus sur la configuration requise pour les certificats PKI, consultez Configuration requise des certificats PKI pour System Center Configuration Manager. Si Configuration Manager demande des certificats PKI, notamment pendant l'inscription d'appareils mobiles et la configuration Intel Active Management Technology (AMT), vous devez utiliser les services de domaine Active Directory et une autorité de certification d'entreprise. Tous les autres certificats PKI doivent être déployés et gérés indépendamment de Configuration Manager.

Les certificats PKI sont également nécessaires quand des ordinateurs clients se connectent à des systèmes de site basés sur Internet. Nous vous recommandons d'utiliser des certificats PKI quand des clients se connectent à des systèmes de site exécutant les services IIS. Pour en savoir plus sur les communications client, consultez Guide pratique pour configurer les ports de communication des clients dans System Center Configuration Manager.

Quand vous utilisez une infrastructure à clés publiques, vous pouvez également utiliser IPsec pour renforcer la sécurité de la communication serveur à serveur entre les systèmes de site d'un site, entre les sites, et pour tout autre transfert de données entre ordinateurs. L'implémentation d'IPsec est indépendante de Configuration Manager.

Configuration Manager peut générer automatiquement des certificats auto-signés en l'absence de certificats PKI disponibles. Dans Configuration Manager, certains certificats sont toujours auto-signés. Dans la plupart des cas, Configuration Manager gère automatiquement les certificats auto-signés, et vous n'avez rien à faire de plus. Une exception possible est le certificat de signature du serveur de site. Le certificat de signature du serveur de site est toujours auto-signé et il garantit que les stratégies client que les clients téléchargent à partir du point de gestion ont été envoyées à partir du serveur de site et n'ont pas été falsifiées.

**Planifier le certificat de signature du serveur de site (auto-signé)**

Les clients peuvent obtenir en toute sécurité une copie du certificat de signature du serveur de site à partir des services de domaine Active Directory et à partir de l'installation Push du client. Si les clients ne peuvent pas obtenir une copie du certificat de signature du serveur de site d'une de ces façons, une bonne pratique pour la sécurité consiste à installer une copie du certificat de signature du serveur de site quand vous installez le client. Cela est particulièrement important si la première communication du client avec le site s'effectue via Internet, car le point de gestion étant connecté à un réseau non approuvé, il est vulnérable aux attaques. Si vous ne prenez pas cette mesure supplémentaire, les clients téléchargent automatiquement une copie du certificat de signature du serveur de site à partir du point de gestion.

Les scénarios suivants se présentent quand les clients ne peuvent pas obtenir une copie du certificat du serveur de site en toute sécurité :

- Vous n'installez pas le client de manière poussée et l'une des conditions suivantes est vraie :
    - Le schéma Active Directory n'est pas étendu pour Configuration Manager.

- Le site du client n'est pas publié dans les services de domaine Active Directory.
- Le client est issu d'une forêt non approuvée ou d'un groupe de travail.

- Vous installez le client lorsqu'il se trouve sur Internet.

Pour installer des clients ainsi qu'une copie du certificat de signature du serveur de site

1. Recherchez le certificat de signature du serveur de site sur le serveur de site principal du client. Le certificat est stocké dans le magasin de certificats **SMS** et possède le nom d'objet **Serveur de site** et le nom convivial **Certificat de signature du serveur de site**.
2. Exportez le certificat sans la clé privée, stockez le fichier dans un emplacement sécurisé et accédez-y uniquement à partir d'un canal sécurisé, par exemple, en utilisant la signature Server Message Block (SMB) ou IPsec.
3. Installez le client en spécifiant la propriété de Client.msi, **SMSSIGNCERT=**<*chemin_complet_et_nom_de_fichier*>, avec CCMSetup.exe.

**Planifier la révocation de certificats PKI**

Si vous utilisez des certificats PKI avec Configuration Manager, déterminez si les clients et serveurs doivent utiliser une liste de révocation des certificats (CRL) et, le cas échéant, de quelle manière, pour vérifier le certificat sur l'ordinateur connecté. Le fichier CRL est un fichier créé et signé par une autorité de certification (AC) qui contient une liste des certificats que cette autorité a émis, puis annulés. L'administrateur d'une autorité de certification peut annuler des certificats, par exemple, si un certificat émis est altéré ou suspecté de l'être.

> **IMPORTANT**
> L'emplacement de la liste de révocation des certificats est ajouté à un certificat au moment de son émission par une autorité de certification. Vous devez donc planifier la liste de révocation des certificats avant de déployer les certificats PKI utilisés par Configuration Manager.

Par défaut, IIS vérifie toujours la liste de révocation des certificats pour les certificats clients. Ce paramètre de configuration n'est pas modifiable dans Configuration Manager. Par défaut, les clients Configuration Manager vérifient toujours la liste de révocation des certificats pour les systèmes de site. Vous pouvez désactiver ce paramètre en spécifiant une propriété de site et une propriété CCMSetup. Quand vous gérez des ordinateurs Intel AMT hors bande, vous pouvez également activer la vérification de la liste de révocation des certificats pour le point de service hors bande et pour les ordinateurs qui exécutent la console de gestion hors bande.

Les ordinateurs qui utilisent la vérification de la révocation des certificats, mais qui ne parviennent pas à localiser la liste de révocation des certificats considèrent que tous les certificats de la chaîne de certification sont révoqués puisque leur absence de la liste ne peut pas être vérifiée. Dans ce scénario, toutes les connexions nécessitant des certificats et utilisant une liste de révocation des certificats échouent.

Le fait de vérifier la liste de révocation des certificats chaque fois qu'un certificat est utilisé offre un niveau de sécurité supérieur par rapport à l'utilisation d'un certificat qui a été révoqué, mais ajoute un délai de connexion et de traitement sur le client. Vous êtes plus susceptible de demander cette vérification de sécurité supplémentaire lorsque les clients sont sur Internet ou sur un réseau non approuvé.

Avec l'aide des administrateurs de votre infrastructure PKI, déterminez si les clients Configuration Manager doivent ou non vérifier la liste de révocation des certificats. Envisagez de laisser cette option activée dans Configuration Manager si les deux conditions suivantes sont réunies :

- Votre infrastructure PKI prend en charge une liste de révocation des certificats, et cette liste est publiée à un emplacement accessible par tous les clients Configuration Manager. N'oubliez pas que cela peut inclure des clients sur Internet si vous utilisez la gestion des clients basés sur Internet et les clients situés dans des forêts non approuvées.

- La nécessité de vérifier la liste de révocation des certificats pour chaque connexion à un système de site qui est configuré pour utiliser un certificat PKI est prioritaire sur celle d'avoir des connexions plus rapides et un traitement efficace sur le client, et au risque d'échec de connexion des clients sur les serveurs si la liste de révocation des certificats est introuvable.

**Planifier les certificats racine approuvés PKI et la liste des émetteurs de certificats**

Si vos systèmes de site IIS utilisent des certificats clients PKI pour l'authentification du client sur HTTP ou pour le chiffrement et l'authentification du client sur HTTPS, vous pouvez être amené à importer des certificats d'autorités de certification racine comme propriété de site. Voici les deux scénarios :

- Vous déployez des systèmes d'exploitation à l'aide de Configuration Manager, et les points de gestion acceptent uniquement les connexions de clients HTTPS.
- Vous utilisez des certificats clients PKI qui ne se lient pas à un certificat d'autorité de certification racine qui est approuvé par des points de gestion.

> **NOTE**
> Lorsque vous émettez des certificats PKI clients à partir de la même hiérarchie de certification racine que celle qui émet les certificats de serveurs que vous utilisez pour les points de gestion, il n'est pas nécessaire de spécifier ce certificat d'autorité de certification racine. Toutefois, si vous utilisez plusieurs hiérarchies d'autorité de certification et si vous n'êtes pas certain qu'elles s'approuvent mutuellement, importez l'autorité de certification racine pour la hiérarchie d'autorité de certification des clients.

Si vous devez importer des certificats d'autorité de certification racine pour Configuration Manager, exportez-les de l'autorité de certification émettrice ou de l'ordinateur client. Si vous exportez le certificat à partir de l'autorité de certification émettrice, qui est également l'autorité de certification racine, assurez-vous que la clé privée n'est pas exportée. Stockez le fichier du certificat exporté dans un emplacement sécurisé pour empêcher toute falsification. Vous devez pouvoir accéder au fichier au moment de la configuration du site. Si vous accédez au fichier sur le réseau, assurez-vous que la communication est protégée contre la falsification à l'aide de la signature SMB ou IPsec.

Si un certificat d'autorité de certification racine que vous importez est renouvelé, vous devez l'importer.

Ces certificats d'autorité de certification racine importés et le certificat d'autorité de certification racine de chaque point de gestion créent la liste des émetteurs de certificats que les ordinateurs Configuration Manager utilisent de la manière suivante :

- Quand un client se connecte à un point de gestion, le point de gestion vérifie que le certificat client est lié à un certificat racine approuvé dans la liste des émetteurs de certificats du site. Dans le cas contraire, le certificat est rejeté et la connexion PKI échoue.
- Quand des clients sélectionnent un certificat PKI et ont une liste des émetteurs de certificats, ils sélectionnent un certificat lié à un certificat racine approuvé dans la liste des émetteurs de certificats. En cas d'absence de correspondance, le client ne sélectionne pas de certificat PKI. Pour en savoir plus sur le processus des certificats clients, consultez la section Planifier la sélection des certificats clients PKI, dans cet article.

Indépendamment de la configuration du site, vous pouvez également être amené à importer un certificat d'autorité de certification racine quand vous inscrivez des appareils mobiles ou des ordinateurs Mac, et configurez des ordinateurs Intel AMT pour des réseaux sans fil.

**Planifier la sélection des certificats clients PKI**

Si vos systèmes de site IIS utilisent des certificats clients PKI pour l'authentification des clients sur HTTP ou pour le chiffrement et l'authentification des clients sur HTTPS, planifiez la manière dont les clients Windows vont sélectionner le certificat à utiliser pour Configuration Manager.

> **NOTE**
> Certains appareils ne prennent pas en charge de méthode de sélection du certificat. À la place, ils sélectionnent automatiquement le premier certificat qui répond aux exigences de certificat. C'est le cas, par exemple, des clients sur les ordinateurs Mac et les appareils mobiles.

Dans de nombreux cas, la configuration par défaut et le comportement seront suffisants. Le client Configuration Manager sur les ordinateurs Windows filtre plusieurs certificats en appliquant les critères suivants, dans cet ordre :

1. La liste des émetteurs de certificats : le certificat est lié à une autorité de certification racine qui est approuvée par le point de gestion.
2. Le certificat se trouve dans le magasin de certificats par défaut de **Personnel**.
3. Le certificat est valide, non révoqué, et n'a pas expiré. La vérification de la validité vérifie que la clé privée est accessible et que le certificat n'est pas créé avec un modèle de certificat version 3, qui n'est pas compatible avec Configuration Manager.
4. Le certificat dispose d'une fonctionnalité d'authentification client ou il est émis vers le nom d'ordinateur.
5. Le certificat possède la plus longue période de validité.

Les clients peuvent être configurés pour utiliser la liste des émetteurs de certificats selon les mécanismes suivants :

- La liste est publiée comme informations de site Configuration Manager vers les services de domaine Active Directory.
- Les clients sont installés à l'aide de la poussée du client.
- Les clients la téléchargent à partir du point de gestion après qu'ils sont correctement affectés à leur site.
- Elle est spécifiée pendant l'installation du client comme propriété client.msi CCMSetup de CCMCERTISSUERS.

Les clients qui n'ont pas la liste des émetteurs de certificats lors de leur installation initiale et qui ne sont pas encore affectés au site ignorent cette étape. Si les clients ont la liste des émetteurs de certificats, mais n'ont pas de certificat PKI lié à un certificat racine approuvé dans la liste des émetteurs de certificats, la sélection du certificat échoue et les clients ne poursuivent pas avec les autres critères de sélection de certificat.

Dans la plupart des cas, le client Configuration Manager identifie correctement un certificat PKI unique et approprié. Dans le cas contraire, plutôt que de sélectionner le certificat à partir de la fonctionnalité d'authentification client, vous pouvez configurer deux autres méthodes de sélection :

- Une correspondance partielle des chaînes pour les valeurs Nom d'objet du certificat du client. Cette correspondance ne tient pas compte de la casse et convient parfaitement si vous utilisez le nom de domaine complet (FQDN) d'un ordinateur dans le champ Objet et souhaitez que la sélection du certificat soit basée sur le suffixe de domaine, par exemple **contoso.com**. Vous pouvez néanmoins utiliser cette méthode de sélection pour identifier une chaîne de caractères séquentiels dans le Nom d'objet du certificat qui différencie le certificat des autres dans le magasin de certificats du client.

> **NOTE**
>
> Vous ne pouvez pas utiliser la correspondance partielle des chaînes avec l'Autre nom de l'objet comme paramètre de site. Bien que vous puissiez spécifier une correspondance partielle des chaînes pour l'Autre nom de l'objet à l'aide de CCMSetup, il sera écrasé par les propriétés du site dans les scénarios suivants :
>
> - Les clients récupèrent les informations de site qui sont publiées dans les services de domaine Active Directory.
>
>   - Les clients sont installés à l'aide de la poussée du client.
>
>   Utilisez une correspondance partielle des chaînes dans l'autre nom de l'objet uniquement quand vous installez manuellement des clients qui ne récupèrent pas les informations de site à partir des services de domaine Active Directory. Par exemple, ces conditions s'appliquent aux clients qui utilisent Internet uniquement.

- Une correspondance pour les valeurs d'attribut Nom d'objet ou Autre nom de l'objet du certificat du client. Cette correspondance tient compte de la casse et convient parfaitement si vous utilisez un nom unique X500 ou des identificateurs d'objet équivalents (OID) conformément à la norme RFC 3280 et souhaitez que la sélection du certificat soit fondée sur les valeurs d'attribut. Vous pouvez spécifier uniquement les attributs et leurs valeurs s'ils doivent identifier de manière unique ou valider le certificat et le différencier des autres certificats du magasin de certificats.

Le tableau suivant indique les valeurs d'attribut que Configuration Manager prend en charge pour les critères de sélection de certificat.

| ATTRIBUT D'OID | ATTRIBUT DE NOM UNIQUE | DÉFINITION DE L'ATTRIBUT |
|---|---|---|
| 0.9.2342.19200300.100.1.25 | DC | Composant de domaine |
| 1.2.840.113549.1.9.1 | E ou E-mail | Adresse de messagerie |
| 2.5.4.3 | CN | Nom commun |
| 2.5.4.4 | SN | Nom d'objet |
| 2.5.4.5 | SERIALNUMBER | Numéro de série |
| 2.5.4.6 | C | Code du pays |
| 2.5.4.7 | L | Localité |
| 2.5.4.8 | S ou ST | Nom de département/province |
| 2.5.4.9 | STREET | Adresse |
| 2.5.4.10 | O | Nom de l'organisation |
| 2.5.4.11 | OU | Unité d'organisation |
| 2.5.4.12 | T ou Title | Titre |
| 2.5.4.42 | G ou GN ou GivenName | Prénom |

| ATTRIBUT D'OID | ATTRIBUT DE NOM UNIQUE | DÉFINITION DE L'ATTRIBUT |
|---|---|---|
| 2.5.4.43 | I ou Initials | Initiales |
| 2.5.29.17 | (aucune valeur) | Autre nom de l'objet |

Si plusieurs certificats appropriés sont détectés après l'application des critères de sélection, vous pouvez remplacer la configuration par défaut pour sélectionner le certificat ayant la plus longue période de validité et spécifier, au contraire, qu'aucun certificat n'est sélectionné. Dans ce scénario, le client ne peut pas communiquer avec des systèmes de site IIS à l'aide d'un certificat PKI. Le client transmet un message d'erreur au point d'état de secours qui lui est attribué pour vous prévenir de l'échec de sélection du certificat et vous permettre de modifier ou d'affiner vos critères de sélection de certificat. Le comportement du client dépend ensuite de l'emplacement de la connexion qui a échoué, à savoir sur HTTPS ou HTTP :

- Si la connexion qui a échoué était sur HTTPS, le client tente de se connecter sur HTTP et d'utiliser le certificat de client auto-signé.
- Si la connexion qui a échoué était sur HTTP, le client tente de se reconnecter sur HTTP à l'aide du certificat de client auto-signé.

Pour identifier facilement un certificat de client unique PKI, vous pouvez également spécifier un magasin personnalisé autre que le magasin par défaut **Personnel** dans **Ordinateur**. Toutefois, vous devez créer ce magasin indépendamment de Configuration Manager, mais aussi être en mesure de déployer des certificats dans ce magasin personnalisé et de les renouveler avant l'expiration de la période de validité.

Pour plus d'informations sur la configuration des paramètres des certificats clients, consultez la section Configurer les paramètres des certificats clients PKI dans l'article Configurer la sécurité dans System Center Configuration Manager.

**Planifier une stratégie de transition pour les certificats PKI et la gestion des clients basée sur Internet**

Grâce aux options de configuration flexibles de Configuration Manager, vous pouvez effectuer progressivement la transition des clients et du site pour utiliser des certificats PKI et sécuriser ainsi davantage les points de terminaison des clients. Les certificats PKI vous permettent de gérer les clients Internet, tout en renforçant la sécurité.

Les options et choix de configuration sont multiples dans Configuration Manager. Cela explique pourquoi il n'y a pas une méthode unique recommandée pour effectuer la transition d'un site afin que tous les clients utilisent des connexions HTTPS. Toutefois, vous pouvez suivre ces étapes comme guide :

1. Installez le site Configuration Manager et configurez-le de sorte que les systèmes de site acceptent les connexions client via HTTP et HTTPS.
2. Dans les propriétés du site, sous l'onglet **Communication de l'ordinateur client**, définissez **Paramètres du système de site** sur **HTTP ou HTTPS** et sélectionnez **Utiliser le certificat client PKI (fonctionnalité d'authentification du client) lorsqu'il est disponible**. Pour plus d'informations, consultez la section Configurer les paramètres des certificats clients PKI dans l'article Configurer la sécurité dans System Center Configuration Manager.
3. Pilotez un déploiement PKI pour les certificats clients. Pour obtenir un exemple de déploiement, consultez la section *Déploiement du certificat client sur les ordinateurs Windows* dans l'article Exemple de déploiement pas à pas des certificats PKI pour System Center Configuration Manager : autorité de certification Windows Server 2008.
4. Installez des clients à l'aide de la méthode d'installation poussée du client. Pour plus d'informations, consultez la section Installer des clients Configuration Manager à l'aide de l'installation Push du client dans l'article Guide pratique pour déployer des clients sur des ordinateurs Windows dans System Center

Configuration Manager.

5. Surveillez le déploiement et l'état des clients à l'aide des rapports et des informations affichés dans la console Configuration Manager.

6. Déterminez combien de clients utilisent un certificat client PKI en affichant la colonne **Certificat client** dans l'espace de travail **Ressources et conformité**, nœud **Appareils**.

   Vous pouvez également déployer l'outil d'évaluation HTTPS Readiness (**cmHttpsReadiness.exe**) de Configuration Manager sur les ordinateurs et utiliser les rapports pour afficher le nombre d'ordinateurs susceptibles d'utiliser un certificat client PKI avec Configuration Manager.

   > **NOTE**
   > Quand le client Configuration Manager est installé, l'outil **cmHttpsReadiness.exe** est installé dans le dossier *%windir%***\CCM**. Lorsque vous exécutez cet outil sur des clients, vous pouvez spécifier les options suivantes :
   >
   > - /Store:<nom>
   >   - /Issuers:<liste>
   >   - /Criteria:<critères>
   >   - /SelectFirstCert
   >
   > Ces options mappent aux propriétés Client.msi **CCMCERTSTORE**, **CCMCERTISSUERS**, **CCMCERTSEL**et **CCMFIRSTCERT** , respectivement. Pour en savoir plus sur ces options, consultez À propos des propriétés d'installation du client dans System Center Configuration Manager.

7. Quand vous êtes certain que suffisamment de clients utilisent leur certificat client PKI pour l'authentification sur HTTP, suivez ces étapes :

   a. Déployez un certificat de serveur Web PKI sur un serveur de membre qui exécutera un point de gestion supplémentaire pour le site et configurez ce certificat dans IIS. Pour plus d'informations, consultez la section *Déploiement du certificat de serveur web pour les systèmes de site qui exécutent IIS* dans l'article Exemple de déploiement pas à pas des certificats PKI pour System Center Configuration Manager : autorité de certification Windows Server 2008.

   b. Installez le rôle de point de gestion sur ce serveur et configurez l'option **Connexions clients** dans les propriétés du point de gestion pour **HTTPS**.

8. Contrôlez et vérifiez que les clients qui possèdent un certificat PKI utilisent le nouveau point de gestion à l'aide du protocole HTTPS. Pour vérifier cela, vous pouvez utiliser le processus d'enregistrement du journal d'IIS ou les compteurs de performance.

9. Reconfigurez d'autres rôles de système de site pour utiliser les connexions de clients HTTPS. Si vous souhaitez gérer des clients sur Internet, assurez-vous que les systèmes de site disposent d'un nom de domaine complet Internet et configurez des points de distribution et des points de gestion individuels pour accepter les connexions de clients à partir d'Internet.

   > **IMPORTANT**
   > Avant de définir des rôles de système de site pour accepter les connexions à partir d'Internet, consultez les informations de planification et les conditions préalables pour la gestion de clients basée sur Internet. Pour plus d'informations, consultez Communications entre points de terminaison dans System Center Configuration Manager.

10. Déployez le certificat PKI pour les clients et les systèmes de site qui exécutent IIS, et définissez les rôles de système de site pour les connexions de client HTTPS et les connexions Internet, au besoin.

11. Pour une sécurité maximale : quand vous êtes certain que tous les clients utilisent un certificat client PKI

pour l'authentification et le chiffrement, modifiez les propriétés de site pour utiliser HTTPS uniquement.

En suivant ce plan pour introduire progressivement des certificats PKI, d'abord pour l'authentification uniquement sur HTTP et ensuite pour l'authentification et le chiffrement sur HTTPS, vous réduisez le risque que les clients ne soient plus gérés. En outre, vous bénéficierez de la sécurité maximale prise en charge par Configuration Manager.

## Planifier la clé racine approuvée

La clé racine approuvée dans Configuration Manager est utilisée par les clients Configuration Manager pour vérifier que les systèmes de site appartiennent à leur hiérarchie. Chaque serveur de site génère une clé d'échange de site pour communiquer avec d'autres sites. La clé d'échange du site de niveau supérieur dans la hiérarchie est appelée clé racine approuvée.

La clé racine approuvée dans Configuration Manager a un rôle similaire à un certificat racine dans une infrastructure à clé publique en ce sens que tout ce qui est signé par la clé privée de la clé racine approuvée est également approuvé dans le reste de la hiérarchie. Par exemple, en signant le certificat du point de gestion avec la paire clé privée/clé racine approuvée, et en effectuant une copie de la paire clé publique/clé racine approuvée qui leur est accessible, les clients peuvent distinguer les points de gestion qui se trouvent dans leur hiérarchie des points de gestion qui ne sont pas dans leur hiérarchie. Les clients utilisent l'infrastructure Windows Management Instrumentation (WMI) pour stocker une copie de la clé racine approuvée dans l'espace de noms **root\ccm\locationservices**.

Les clients peuvent récupérer automatiquement la copie publique de la clé racine approuvée selon deux mécanismes :

- Le schéma Active Directory est étendu pour Configuration Manager, le site est publié dans les services de domaine Active Directory, et les clients peuvent récupérer ces informations de site à partir d'un serveur de catalogue global.
- Les clients sont installés à l'aide de la poussée du client.

Si les clients ne peuvent pas récupérer la clé racine approuvée selon l'un de ces mécanismes, ils font confiance à la clé racine approuvée qui est fournie par le premier point de gestion avec lequel ils communiquent. Dans ce scénario, un client peut être redirigé vers le point de gestion d'un pirate informatique où il recevrait la stratégie à partir du point de gestion non autorisé. Cela ne peut être que l'œuvre d'un pirate chevronné et ne peut se produire qu'au cours d'une période limitée, avant que le client ne récupère la clé racine approuvée à partir d'un point de gestion valide. Toutefois, pour réduire le risque d'un acte de piraterie consistant à réacheminer les clients vers un point de gestion factice, préconfigurez les clients avec la clé racine approuvée.

Pour préconfigurer et vérifier la clé racine approuvée pour un client Configuration Manager, procédez comme suit :

- Préconfigurez un client avec la clé racine approuvée en utilisant un fichier.
- Préconfigurez un client avec la clé racine approuvée sans utiliser de fichier.
- Vérifiez la clé racine approuvée sur un client.

> **NOTE**
> Vous n'avez pas besoin de préconfigurer un client avec la clé racine approuvée si le client peut l'obtenir à partir des services de domaine Active Directory ou s'il est installé à l'aide de l'installation Push du client. C'est également le cas si le client utilise la communication HTTPS pour les points de gestion, car l'approbation est établie par les certificats PKI.

Vous pouvez supprimer la clé racine approuvée d'un client en utilisant la propriété Client.msi,

**RESETKEYINFORMATION = TRUE**, avec CCMSetup.exe. Pour remplacer la clé racine approuvée, réinstallez le client avec la nouvelle clé racine approuvée, par exemple en utilisant l'installation push du client ou en spécifiant la propriété Client.msi **SMSPublicRootKey** à l'aide de CCMSetup.exe.

**Pour mettre en service anticipé un client avec la clé racine approuvée à l'aide d'un fichier**

1. Dans un éditeur de texte, ouvrez le fichier <*répertoire_Configuration_Manager*>**\bin\mobileclient.tcf**.
2. Recherchez l'entrée **SMSPublicRootKey=**, copiez la clé à partir de cette ligne et fermez le fichier sans effectuer de modification.
3. Créez un fichier texte, puis collez dans ce nouveau fichier les informations de clé que vous avez copiées à partir du fichier mobileclient.tcf.
4. Enregistrez le fichier à un emplacement accessible à tous les ordinateurs. Cet emplacement doit être sécurisé pour empêcher toute falsification.
5. Installez le client à l'aide d'une méthode d'installation qui accepte les propriétés de Client.msi. Spécifiez ensuite la propriété de Client.msi, **SMSROOTKEYPATH=**<*chemin_complet_et_nom_de_fichier*>.

> **IMPORTANT**
> Quand vous spécifiez la clé racine approuvée pour renforcer la sécurité lors de l'installation du client, vous devez également spécifier le code de site en utilisant la propriété de Client.msi **SMSSITECODE=<code_site>**.

**Pour mettre en service anticipé un client avec la clé racine approuvée sans utiliser de fichier**

1. Dans un éditeur de texte, ouvrez le fichier <*répertoire_Configuration_Manager*>**\bin\mobileclient.tcf**.
2. Recherchez l'entrée SMSPublicRootKey=, notez la clé à partir de cette ligne ou copiez-la dans le Presse-papiers, puis fermez le fichier sans effectuer de modification.
3. Installez le client à l'aide d'une méthode d'installation qui accepte les propriétés de Client.msi. Spécifiez ensuite la propriété de Client.msi, **SMSPublicRootKey=**<*clé*>, où <*clé*> est la chaîne que vous avez copiée du fichier mobileclient.tcf.

> **IMPORTANT**
> Quand vous spécifiez la clé racine approuvée pour renforcer la sécurité lors de l'installation du client, vous devez également spécifier le code de site en utilisant la propriété de Client.msi **SMSSITECODE=<code_site>**.

**Pour vérifier la clé racine approuvée sur un client**

1. Dans le menu **Démarrer**, cliquez sur **Exécuter**, puis entrez **Wbemtest**.
2. Dans la boîte de dialogue **Testeur WMI**, choisissez **Connecter**.
3. Dans la boîte de dialogue **Connecter**, dans la zone **Espace de noms**, entrez **root\ccm\locationservices**, puis choisissez **Connecter**.
4. Dans la boîte de dialogue **Testeur WMI**, dans la section **IWbemServices**, choisissez **Énumérer les classes**.
5. Dans la boîte de dialogue **Informations de la superclasse**, choisissez **Récursive**, puis choisissez **OK**.
6. Dans la fenêtre **Résultats d'interrogation** , accédez à la fin de la liste, puis double-cliquez sur **TrustedRootKey ()**.
7. Dans la boîte de dialogue **Éditeur d'objets pour TrustedRootKey**, choisissez **Instances**.
8. Dans la nouvelle fenêtre **Résultat de la requête**, qui affiche les instances de **TrustedRootKey**, double-

cliquez sur **TrustedRootKey=@**.

9. Dans la boîte de dialogue **Éditeur d'objets pour TrustedRootKey=@** , dans la section **Propriétés** , accédez à **TrustedRootKey CIM_STRING**. La chaîne dans la colonne droite correspond à la clé racine approuvée. Vérifiez qu'elle correspond à la valeur **SMSPublicRootKey** dans le fichier *<répertoire_Configuration_Manager>***\bin\mobileclient.tcf**.

## Planifier la signature et le chiffrement

Lorsque vous utilisez des certificats PKI pour toutes les communications client, vous n'avez pas à planifier la signature et le chiffrement pour contribuer à sécuriser les communications de données client. Toutefois, si vous installez des systèmes de site qui exécutent IIS pour autoriser les connexions client HTTP, vous devez décider comment sécuriser la communication client pour le site.

Pour contribuer à protéger les données que les clients envoient aux points de gestion, vous pouvez exiger que les données soient signées. En outre, vous pouvez exiger que toutes les données signées provenant de clients qui utilisent le protocole HTTP soient signées à l'aide de l'algorithme SHA-256. Bien qu'il s'agisse d'un paramètre plus sécurisé, n'activez cette option que si tous les clients prennent en charge SHA-256. De nombreux systèmes d'exploitation offrent une prise en charge native de SHA-256, mais les systèmes d'exploitation plus anciens peuvent nécessiter une mise à jour ou un correctif logiciel. Par exemple, les ordinateurs qui exécutent Windows Server 2003 SP2 doivent installer un correctif qui est référencé dans l'article 938397 de la Base de connaissances Microsoft.

Bien que la signature contribue à protéger les données de la falsification, le chiffrement permet de protéger les données contre la divulgation d'informations. Vous pouvez activer le chiffrement 3DES pour les données d'inventaire et les messages d'état que les clients envoient aux points de gestion dans le site. Il n'est pas nécessaire d'installer des mises à jour sur des clients pour prendre en charge cette option, mais tenez compte de l'utilisation supplémentaire du processeur qui sera requise sur les clients et le point de gestion pour effectuer le chiffrement et le déchiffrement.

Pour en savoir plus sur la configuration des paramètres de signature et de chiffrement, consultez la section Configurer la signature et le chiffrement dans l'article Configurer la sécurité dans System Center Configuration Manager.

## Planifier l'administration basée sur des rôles

Pour plus d'informations, consultez Principes de base de l'administration basée sur des rôles pour System Center Configuration Manager.

**Voir aussi**

Informations techniques de référence sur les contrôles de chiffrement pour System Center Configuration Manager.

# Bonnes pratiques de sécurité et informations de confidentialité de System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez les informations suivantes pour rechercher de bonnes pratiques de sécurité et des informations de confidentialité pour System Center Configuration Manager.

## Contenu relatif à la sécurité et à la confidentialité :

- Sécurité et confidentialité pour l'administration de site dans System Center Configuration Manager
- Sécurité et confidentialité pour les rapports dans System Center Configuration Manager
- Sécurité et confidentialité pour la migration vers System Center Configuration Manager
- Sécurité et confidentialité pour les clients dans System Center Configuration Manager
- Sécurité et confidentialité pour la gestion du contenu dans System Center Configuration Manager
- Sécurité et confidentialité pour la gestion des applications dans System Center Configuration Manager
- Sécurité et confidentialité pour les mises à jour logicielles dans System Center Configuration Manager
- Sécurité et confidentialité du déploiement de systèmes d'exploitation dans System Center Configuration Manager
- Sécurité et confidentialité pour les regroupements dans System Center Configuration Manager
- Sécurité et confidentialité pour les requêtes dans System Center Configuration Manager
- Sécurité et confidentialité pour l'inventaire matériel dans System Center Configuration Manager
- Sécurité et confidentialité pour l'inventaire logiciel dans System Center Configuration Manager
- Sécurité et confidentialité pour Asset Intelligence dans System Center Configuration Manager
- Sécurité et confidentialité pour la gestion de l'alimentation dans System Center Configuration Manager
- Sécurité et confidentialité pour le contrôle à distance dans System Center Configuration Manager
- Sécurité et confidentialité pour l'inventaire logiciel dans System Center Configuration Manager
- Sécurité et confidentialité des paramètres de compatibilité dans System Center Configuration Manager
- Consultez la section *Considérations relatives à la sécurité et à la confidentialité pour les profils de connexion à distance* dans Profils de connexion à distance dans System Center Configuration Manager
- Sécurité et confidentialité pour les profils de certificat dans System Center Configuration Manager
- Sécurité et confidentialité des profils Wi-Fi et VPN dans System Center Configuration Manager

# Déclaration de confidentialité de System Center Configuration Manager – Bibliothèque d'applets de commande de Configuration Manager

22/06/2018 • 3 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cette déclaration de confidentialité couvre les fonctionnalités de la bibliothèque d'applets de commande de System Center Configuration Manager.

## Données d'utilisation

**Descriptif de cette fonctionnalité**

La bibliothèque d'applets de commande de System Center Configuration Manager vous permet de gérer une hiérarchie Configuration Manager à l'aide d'applets de commande et de scripts Windows PowerShell. La bibliothèque d'applets de commande collecte des informations sur l'utilisation des applets de commande dans la bibliothèque pour identifier des tendances et des modèles d'utilisation. La bibliothèque d'applets de commande collecte également les types et le nombre d'erreurs que vous recevez quand vous utilisez les applets de commande.

**Informations collectées, traitées ou transmises**

Les données d'utilisation collectées comprennent le démarrage, l'arrêt et l'interruption des applets de commande, l'exécution d'applets de commande dépréciées et des métriques d'activité pour les opérations du fournisseur SMS qui sont liées aux applets de commande. Ces informations ne permettent pas de vous identifier personnellement. Les informations collectées sur les erreurs comprennent les erreurs que les applets de commande renvoient ainsi que les détails des erreurs d'exception. Certains rapports détaillés sur les erreurs peuvent inclure par inadvertance des identificateurs individuels, comme le numéro de série d'un appareil connecté à votre ordinateur. La bibliothèque d'applets de commande filtre et rend anonymes les informations dans les rapports d'erreur pour supprimer les identificateurs individuels avant leur transmission à Microsoft.

**Utilisation des informations**

Microsoft utilise ces informations pour améliorer la qualité, la sécurité et l'intégrité des produits et services qu'elles propose.

**Choix/contrôle**

Cette fonctionnalité de données d'utilisation est activée par défaut. La bibliothèque d'applets de commande de System Center Configuration Manager a deux clés de Registre qui contrôlent cette fonctionnalité.

Pour la désactiver complètement, définissez la valeur de ces deux clés de Registre. Ils correspondent à chacun des fournisseurs de suivi d'événements pour Windows (ETW) :

- HKLM\Software\Microsoft\ConfigMgr10\PowerShell\Microsoft.ConfigurationManagement.PowerShell.Provider:CeipLevel=0 (désactive la fonctionnalité Données d'utilisation pour le fournisseur du lecteur)
- HKLM\Software\Microsoft\ConfigMgr10\PowerShell\Microsoft.ConfigurationManagement.PowerShell.Cmdlets:CeipLevel=0 (désactive la fonctionnalité Données d'utilisation pour les applets de commande)

  Les changements des paramètres de données d'utilisation sont spécifiques à l'ordinateur sur lequel ils sont apportés.

## Étapes suivantes

Documentation de la bibliothèque d’applets de commande de System Center Configuration Manager.

# Informations supplémentaires sur la confidentialité pour System Center Configuration Manager

22/06/2018 • 18 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

## Mises à jour et maintenance

System Center Configuration Manager introduit un nouveau modèle de mise à jour qui vous aide à maintenir à jour votre déploiement actuel de Configuration Manager avec les dernières mises à jour et fonctionnalités. Une fois installée, cette fonctionnalité ajoute un nouveau rôle de système de site qui est appelé point de connexion de service sur un serveur de site choisi par un administrateur. Pour en savoir plus sur les informations collectées et sur leur utilisation, consultez la section Données d'utilisation dans cet article.

## Données d'utilisation

System Center Configuration Manager collecte les données d'utilisation et de diagnostic sur lui-même. Microsoft utilise ensuite ces données pour améliorer le processus d'installation, la qualité et la sécurité des versions ultérieures. Des données d'utilisation et de diagnostic sont collectées pour chaque hiérarchie System Center Configuration Manager. Elle consistent en requêtes SQL Server qui s'exécutent chaque semaine sur chaque site principal et sur le site d'administration centrale. Quand la hiérarchie utilise un site d'administration centrale, les données provenant des sites principaux sont répliquées sur ce site. Sur le site de niveau supérieur de votre hiérarchie, le point de connexion de service soumet ces informations quand il recherche des mises à jour. Si le point de connexion de service est en mode hors connexion, les informations sont transférées à l'aide de l'outil de connexion de service.

Configuration Manager collecte uniquement les données de la base de données SQL Server des sites. Il ne collecte pas de données directement à partir des clients ni des serveurs de site.

Les administrateurs peuvent modifier le niveau des données collectées en accédant à la section **Données d'utilisation** de la console Configuration Manager.

Pour plus d'informations, consultez les articles « En savoir plus » sur les niveaux et les paramètres des données d'utilisation mentionnés dans l'article Données d'utilisation et de diagnostic pour System Center Configuration Manager.

## Programme d'amélioration de l'expérience utilisateur

> **NOTE**
> À compter de Configuration Manager version 1802, la fonctionnalité CEIP ne figure plus dans le produit.

Le programme d'amélioration de l'expérience utilisateur (CEIP) collecte des informations de base à partir de la console Configuration Manager sur votre configuration matérielle, et sur votre utilisation de nos logiciels et services afin d'identifier des tendances et des modèles d'utilisation. Le programme CEIP collecte également le type et le nombre d'erreurs rencontrées, les performances logicielles et matérielles, et la rapidité des services. Nous ne collectons pas votre nom, votre adresse ni d'autres informations de contact. Aucune donnée CEIP n'est collectée à partir des ordinateurs des clients.

Les informations recueillies sont utilisées pour améliorer la qualité, la fiabilité et les performances des produits et services Microsoft.

Pour plus d'informations sur les informations collectées, traitées et transmises par le programme d'amélioration de l'expérience utilisateur (CEIP), consultez la Déclaration de confidentialité pour le programme d'amélioration de l'expérience utilisateur de Microsoft.

## Connecteur Operations Management Suite

Le connecteur Microsoft Operations Management Suite synchronise les données, comme les regroupements, de System Center Configuration Manager vers Microsoft Operations Management Suite. L'ID et la clé secrète de l'abonnement Microsoft Azure sont stockés dans la base de données Configuration Manager quand un administrateur configure la fonctionnalité. La clé secrète du client Azure Active Directory et la clé partagée de l'espace de travail Microsoft Operations Management Suite sont stockées dans la base de données locale de System Center Configuration Manager. Toutes les communications entre System Center Configuration Manager et Microsoft Operations Management Suite utilisent HTTPS. Aucune information supplémentaire sur les regroupements n'est fournie à Microsoft en dehors de données de télémétrie aléatoires. Pour plus d'informations sur les informations collectées par Microsoft Operations Management Suite, consultez Sécurité des données Log Analytics.

## Asset Intelligence

Asset Intelligence permet aux administrateurs informatiques de définir, de suivre et de gérer de façon proactive la conformité à des normes de configuration. La mesure et les rapports concernant le déploiement et l'utilisation des applications physiques et virtuelles permettent aux entreprises de prendre de meilleures décisions au sujet des licences de logiciel et de tenir à jour la conformité aux accords de licence. Une fois les données d'utilisation des clients Configuration Manager collectées, les administrateurs peuvent utiliser différentes fonctionnalités pour afficher les données, notamment les regroupements, les requêtes et les rapports.

Lors de chaque synchronisation, un catalogue des logiciels connus est téléchargé à partir de Microsoft. Les administrateurs informatiques peuvent choisir d'envoyer à Microsoft des informations sur les titres de logiciels sans catégorie découverts au sein de leur organisation pour y effectuer des recherches et les ajouter au catalogue. Avant le chargement de ces informations, une boîte de dialogue montre les données qui vont être chargées. Les données téléchargées ne peuvent pas être rappelées. Asset Intelligence n'envoie pas d'informations sur les utilisateurs, les ordinateurs ou l'utilisation des licences à Microsoft.

Une fois qu'un titre de logiciel est chargé, les chercheurs de Microsoft l'identifient, le classent, puis le mettent à la disposition de tous les autres clients qui utilisent cette fonctionnalité et d'autres utilisateurs du catalogue. Tout titre de logiciel chargé devient public. L'application et sa classification font alors partie du catalogue et peuvent ensuite être téléchargées par d'autres utilisateurs du catalogue. Avant de configurer le regroupement de données Asset Intelligence et de décider de soumettre des informations à Microsoft, pensez aux besoins de votre organisation en matière de confidentialité.

Asset Intelligence n'est pas activé dans System Center Configuration Manager par défaut. Le téléchargement de titres sans catégorie ne se produit jamais automatiquement et le système n'est pas conçu pour que cette tâche soit automatisée. Vous devez sélectionner et approuver manuellement le téléchargement de chaque nom de logiciel.

## Endpoint Protection

Microsoft Cloud Protection Service s'appelait auparavant Microsoft Active Protection Service ou MAPS. Les produits applicables sont Microsoft Cloud Protection Service et la fonctionnalité Endpoint Protection de System Center Configuration Manager (pour la gestion de System Center Endpoint Protection et de Windows Defender pour Windows 10). Cette fonctionnalité n'est pas implémentée pour System Center Endpoint Protection pour Linux ni System Center Endpoint Protection pour Mac.

La communauté anti-programme malveillant de Microsoft Cloud Protection Service est une communauté en ligne internationale bénévole qui rassemble les utilisateurs de System Center Endpoint Protection. Quand vous vous joignez à Microsoft Cloud Protection Service, System Center Endpoint Protection envoie automatiquement des informations à Microsoft. Microsoft utilise les informations pour déterminer les logiciels où rechercher d'éventuelles menaces et pour améliorer l'efficacité de System Center Endpoint Protection. Cette communauté contribue à limiter la portée des infections des nouveaux logiciels malveillants. Si un rapport Microsoft Cloud Protection Service inclut des détails sur des logiciels malveillants ou potentiellement non désirés que le client Endpoint Protection peut supprimer, Microsoft Cloud Protection Service télécharge la signature la plus récente pour y procéder. Microsoft Cloud Protection Service peut également rechercher de « faux positifs » (un élément initialement identifié comme logiciel malveillant mais qui ne l'est pas) et les corriger.

Les rapports Microsoft Cloud Protection Service contiennent des informations sur les fichiers des logiciels malveillants potentiels, comme les noms de fichiers, le hachage de chiffrement, le fournisseur, la taille et les horodatages. Par ailleurs, Microsoft Cloud Protection Service peut collecter des URL complètes pour indiquer l'origine du fichier. Ces URL contiennent parfois des informations personnelles, comme des termes de recherche ou des données entrées dans des formulaires. Les rapports peuvent également inclure les actions que vous avez effectuées quand Endpoint Protection vous a informé sur des logiciels indésirables. Les rapports Microsoft Cloud Protection Service incluent ces informations pour aider Microsoft à évaluer l'efficacité avec laquelle Endpoint Protection peut détecter et supprimer des programmes malveillants et potentiellement indésirables et pour tenter d'identifier les nouveaux logiciels malveillants.

Vous pouvez adhérer à Microsoft Cloud Protection Service si vous avez un abonnement de base ou avancé. Les rapports des abonnés de base contiennent les informations décrites ci-dessus. Les rapports des abonnés avancés sont plus complets et peuvent contenir des informations complémentaires sur les logiciels détectés par Endpoint Protection, notamment l'emplacement, le nom des fichiers, le mode de fonctionnement du logiciel et l'incidence sur votre ordinateur. Ces rapports, ainsi que ceux des autres utilisateurs d'Endpoint Protection qui participent à Microsoft Cloud Protection Service, aident les chercheurs de Microsoft à découvrir les nouvelles menaces plus rapidement. Les définitions des programmes malveillants sont ensuite créées pour les programmes qui répondent aux critères d'analyse et les définitions actualisées sont rendues disponibles à tous les utilisateurs via Microsoft Update.

Pour vous aider à détecter et résoudre certains types d'infections de logiciels malveillants, le produit envoie régulièrement à Microsoft Cloud Protection Service des informations sur l'état de sécurité de votre ordinateur. Ces informations comprennent des informations sur les paramètres de sécurité et les fichiers journaux de votre ordinateur qui décrivent les pilotes et autres logiciels qui se chargent pendant que votre ordinateur démarre. Un numéro qui identifie de façon unique votre PC est également envoyé. De plus, Microsoft Cloud Protection Service peut collecter les adresses IP auxquelles les fichiers de programmes malveillants potentiels se connectent.

Les rapports Microsoft Cloud Protection Service sont utilisés pour améliorer les logiciels et services Microsoft. Ils peuvent également servir à des fins de statistique, de test ou d'analyse, et pour générer des définitions. Seuls les employés, les prestataires, les sous-traitants, les partenaires et les fournisseurs de Microsoft qui ont besoin d'utiliser les rapports dans le cadre de leurs activités professionnelles y ont accès.

Microsoft Cloud Protection Service ne collecte pas intentionnellement des informations personnelles. Dans la mesure où Microsoft Cloud Protection Service collecte des informations personnelles, Microsoft ne les utilise pas pour vous identifier ou vous contacter.

Vous pouvez trouver des informations supplémentaires sur les données collectées dans la documentation du produit, dans Endpoint Protection dans System Center Configuration Manager.

## Hiérarchie de site : vue géographique avec cartes Bing

Hiérarchie de site : la vue géographique vous permet d'utiliser des cartes fournies par Microsoft Bing Maps pour afficher la topologie des serveurs physiques de Configuration Manager. Pour activer cette fonctionnalité, les informations d'emplacement que vous fournissez sont envoyées depuis votre serveur au service web Bing Maps.

Microsoft utilise les informations pour exploiter et améliorer les cartes Microsoft Bing et autres sites et services Microsoft. Pour plus d'informations, consultez la Déclaration de confidentialité de Microsoft. Vous pouvez choisir de ne pas utiliser la vue géographique pour la hiérarchie du site. La vue Diagramme de la hiérarchie vous permet d'afficher la hiérarchie ; elle n'utilise pas le service Bing Maps.

## Abonnement Microsoft Intune

Les clients qui ont souscrit un abonnement à Microsoft Intune peuvent utiliser Configuration Manager pour gérer leurs appareils mobiles connectés via Microsoft Intune. La déclaration de confidentialité des Services en ligne de Microsoft s'applique à Microsoft Online Services, qui inclut Microsoft Intune. Si les clients possèdent également un abonnement à Microsoft Intune, la déclaration de confidentialité Microsoft Online Services doit être lue conjointement avec la présente déclaration de confidentialité.

Toutes les communications avec Microsoft Intune utilisent le protocole HTTPS. Pour configurer l'abonnement à Microsoft Intune et télécharger la Demande de signature de certificat (DSC) qui est nécessaire à la configuration de la prise en charge d'iOS, un administrateur doit se connecter à Microsoft Intune en utilisant son compte et son mot de passe professionnels. Ces informations d'identification ne sont pas stockées dans Configuration Manager. Toutes les autres communications avec Microsoft Intune sont authentifiées à l'aide de certificats PKI qui sont générés automatiquement par Microsoft Intune.

Pour gérer les appareils connectés à Microsoft Intune, certaines informations sont envoyées à et reçues de Microsoft Intune. Ces informations incluent le nom principal de l'utilisateur (UPN) de tous les utilisateurs qui sont affectés au service et les informations d'inventaire d'appareils pour les appareils qui sont gérés par Microsoft Intune. Des métadonnées, comme le nom, l'éditeur et la version de l'application, pour le contenu qui est affecté aux points de distribution Manage.Microsoft.com sont envoyées à Microsoft Intune. Le contenu binaire réel affecté à un point de distribution Manage.Microsoft.com est chiffré avant son chargement vers Microsoft Intune.

Cette fonction n'est pas configurée par défaut. Les administrateurs contrôlent le contenu qui est transféré vers le point de distribution Manage.Microsoft.com et les utilisateurs qui sont affectés au service. La fonctionnalité peut être supprimée à tout moment.

# Configurer la sécurité dans System Center Configuration Manager

22/06/2018 • 10 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez les informations de cet article pour configurer les options de sécurité pour System Center Configuration Manager.

## Configurer les paramètres de certificat client PKI

Si vous souhaitez utiliser des certificats PKI (infrastructure à clés publiques) pour les connexions client aux systèmes de site utilisant les services IIS (Internet Information Services), la procédure suivante vous permet de configurer les paramètres pour ces certificats.

**Pour configurer des paramètres de certificat client PKI**

1. Dans la console Configuration Manager, choisissez **Administration**.
2. Dans l'espace de travail **Administration**, développez **Configuration du site**, choisissez **Sites**, puis le site principal à configurer.
3. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**, puis l'onglet **Communication de l'ordinateur client**.

   Cet onglet est disponible uniquement sur un site principal. Si vous ne voyez pas l'onglet **Communication de l'ordinateur client** , vérifiez que vous n'êtes pas connecté à un site d'administration centrale ni à un site secondaire.
4. Choisissez **HTTPS uniquement** quand vous voulez que les clients attribués au site utilisent toujours un certificat client PKI pour se connecter aux systèmes de site qui utilisent IIS. Sinon, choisissez **HTTPS ou HTTP** quand vous n'avez pas besoin que les clients utilisent des certificats PKI.
5. Si vous avez choisi **HTTPS ou HTTP**, choisissez **Utiliser le certificat client PKI (fonctionnalité d'authentification client) si possible** quand vous voulez utiliser un certificat client PKI pour des connexions HTTP. Le client utilise ce certificat au lieu d'un certificat auto-signé pour s'authentifier auprès des systèmes de site. Cette option est automatiquement sélectionnée si vous choisissez **HTTPS uniquement**.

   Lorsque des clients sont détectés sur Internet ou qu'ils sont configurés pour la gestion des clients Internet uniquement, ils utilisent toujours un certificat client PKI.
6. Choisissez **Modifier** pour configurer votre méthode de sélection de client quand plusieurs certificats clients PKI valides sont disponibles sur un client, puis choisissez **OK**.

   Pour plus d'informations sur la méthode de sélection des certificats clients, consultez Planification de la sélection des certificats clients PKI.
7. Activez ou désactivez la case à cocher pour permettre aux clients de vérifier la liste de révocation de certificats.

   Pour plus d'informations sur la vérification de la liste de révocation de certificats pour les clients, consultez Planification de la révocation de certificats PKI.
8. Si vous devez spécifier des certificats d'autorité de certification racine approuvés pour les clients,

choisissez **Définir**, importez les fichiers de certificat d'autorité de certification racine, puis choisissez **OK**.

Pour plus d'informations sur ce paramètre, consultez Planification des certificats racines approuvés PKI et de la liste des émetteurs de certificats.

9. Choisissez **OK** pour fermer la boîte de dialogue des propriétés du site.

Répétez cette procédure pour tous les sites principaux de la hiérarchie.

## Configurer la signature et le chiffrement

Configurez les paramètres de signature et de chiffrement les plus sécurisés pour les systèmes de site pris en charge par tous les clients du site. Ces paramètres sont particulièrement importants lorsque vous permettez aux clients de communiquer avec les systèmes de site à l'aide de certificats auto-signés via HTTP.

**Pour configurer la signature et le chiffrement pour un site**

1. Dans la console Configuration Manager, choisissez **Administration**.
2. Dans l'espace de travail **Administration**, développez **Configuration du site**, choisissez **Sites**, puis le site principal à configurer.
3. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**, puis l'onglet **Signature et chiffrement**.

   Cet onglet est disponible uniquement sur un site principal. Si vous ne voyez pas l'onglet **Signature et chiffrement** , vérifiez que vous n'êtes pas connecté à un site d'administration centrale ni à un site secondaire.
4. Configurez les options de signature et de chiffrement de votre choix, puis choisissez **OK**.

   > **WARNING**
   > Ne choisissez pas l'option **Demander SHA-256** sans vérifier d'abord que tous les clients susceptibles d'être attribués au site peuvent prendre en charge l'algorithme de hachage ou qu'ils disposent d'un certificat d'authentification client PKI valide. Vous devrez peut-être installer des mises à jour ou des correctifs logiciels sur les clients pour prendre en charge SHA-256. Par exemple, les ordinateurs qui exécutent Windows Server 2003 SP2 doivent installer un correctif qui est référencé dans l'article 938397 de la Base de connaissances Microsoft.
   >
   > Si vous choisissez cette option pour des clients qui ne prennent pas en charge SHA-256 et qui utilisent des certificats auto-signés, Configuration Manager rejette ces clients. Dans ce scénario, le composant SMS_MP_CONTROL_MANAGER enregistre l'ID de message 5443.
5. Choisissez **OK** pour fermer la boîte de dialogue **Propriétés** du site.

Répétez cette procédure pour tous les sites principaux de la hiérarchie.

## Configurer l'administration basée sur des rôles

L'administration basée sur des rôles combine des rôles de sécurité, des étendues de sécurité et des regroupements attribués pour définir l'étendue administrative de chaque utilisateur administratif. L'étendue administrative inclut les objets qu'un utilisateur administratif peut afficher dans la console Configuration Manager et les tâches associées à ces objets que cet utilisateur est autorisé à exécuter. Les configurations d'administration basée sur des rôles s'appliquent à chaque site dans une hiérarchie.

Les liens suivants renvoient vers les sections correspondantes de l'article Configurer l'administration basée sur des rôles pour System Center Configuration Manager :

- Créer des rôles de sécurité personnalisés

- Configurer des rôles de sécurité
- Configurer des étendues de sécurité pour un objet
- Configurer des regroupements pour gérer la sécurité
- Créer un utilisateur administratif
- Modifier l'étendue administrative d'un utilisateur administratif

> **IMPORTANT**
> Votre propre étendue administrative définit les objets et les paramètres que vous pouvez attribuer lorsque vous configurez une administration basée sur des rôles pour un autre utilisateur administratif. Pour plus d'informations sur la planification de l'administration basée sur des rôles, consultez Principes de base de l'administration basée sur des rôles pour System Center Configuration Manager.

## Gérer les comptes utilisés par Configuration Manager

Configuration Manager prend en charge les comptes Windows pour de nombreuses tâches et utilisations différentes.

Utilisez la procédure suivante pour afficher les comptes qui sont configurés pour différentes tâches et pour gérer le mot de passe utilisé par Configuration Manager pour chaque compte.

**Pour gérer les comptes utilisés par Configuration Manager**

1. Dans la console Configuration Manager, choisissez **Administration**.
2. Dans l'espace de travail **Administration**, développez **Sécurité**, puis choisissez **Comptes** pour afficher les comptes qui sont configurés pour Configuration Manager.
3. Pour modifier le mot de passe d'un compte qui est configuré pour Configuration Manager, choisissez le compte.
4. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
5. Choisissez **Définir** pour ouvrir la boîte de dialogue **Compte d'utilisateur Windows**, puis spécifiez le nouveau mot de passe que Configuration Manager doit utiliser pour ce compte.

   > **NOTE**
   > Le mot de passe que vous spécifiez doit correspondre au mot de passe spécifié pour le compte dans Utilisateurs et ordinateurs Active Directory.

6. Choisissez **OK** pour terminer la procédure.

# Évaluer System Center Configuration Manager en créant votre propre environnement lab

22/06/2018 • 4 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Découvrez comment créer un environnement lab pour évaluer System Center Configuration Manager pour une utilisation dans votre organisation.

System Center Configuration Manager est un outil complexe et puissant qui permet de gérer vos utilisateurs, logiciels et appareils. Il est judicieux de procéder à une évaluation approfondie de System Center Configuration Manager avant de procéder à un déploiement complet de façon à combiner vos connaissances conceptuelles à des exercices pratiques.

Ce guide s'adresse principalement aux administrateurs qui évaluent l'utilisation de Configuration Manager dans des environnements d'entreprise :

- Administrateurs à la recherche d'une solution de gestion complète de PC, serveurs et appareils mobiles
- Administrateurs dans les secteurs de haute sécurité qui exigent la sécurité liée à la gestion locale des appareils et la souplesse liée à la gestion des appareils dans le cloud
- Administrateurs qui souhaitent gérer la montée en puissance de leur architecture de serveurs locale

## Ce que fait ce lab

L'objectif principal sous-tendant la création de cet environnement lab est de vous fournir les connaissances générales qui vous permettront de commencer à utiliser Configuration Manager et d'améliorer votre connaissance de cet outil. Vous allez examiner pas à pas un assembly expédié de la version actuelle de Configuration Manager en utilisant deux serveurs :

- L'un hébergeant Active Directory, le contrôleur de domaine et le serveur DNS
- Un autre hébergeant Configuration Manager et tous les composants SQL Server associés

Les ordinateurs clients sont installés sur Hyper-V. Le lab proprement dit peut aussi être exécuté en tant que système entièrement virtualisé sur un seul serveur.

## Ce que ne fait pas ce lab

Ce lab ne vous guidera pas dans tous les scénarios de Configuration Manager possibles. Il n'est pas conçu pour être migré immédiatement dans un environnement actif.

Une fois ce lab généré, vous disposerez d'un environnement de travail opérationnel. Toutefois, cet environnement ne sera pas optimisé pour des facteurs tels que les performances du système, la gestion de l'espace sur disque dur et le stockage SQL Server.

## Lecture recommandée avant d'élaborer le lab

La documentation de System Center Configuration Manager propose un contenu très riche. Nous vous recommandons de lire les rubriques suivantes de cette bibliothèque avant de commencer le lab :

- Découvrez les concepts de base concernant la console Configuration Manager, les portails d'utilisateurs

finaux, ainsi que des exemples de scénarios dans Présentation de System Center Configuration Manager.

- Découvrez les principales fonctionnalités de gestion de Configuration Manager dans Fonctions et fonctionnalités de System Center Configuration Manager.
- Approfondissez vos connaissances avec Principes de base de System Center Configuration Manager.
- Découvrez l'importance des rôles de sécurité dans Principes de base de l'administration basée sur des rôles pour System Center Configuration Manager.
- Découvrez la gestion de contenu dans Concepts de la gestion de contenu.
- Apprenez à traiter correctement les opérations quotidiennes tout au long de votre déploiement dans Comprendre comment les clients recherchent des services et des ressources de site pour System Center Configuration Manager.

# Configurer votre laboratoire de System Center Configuration Manager

17/07/2018 • 27 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

En suivant les recommandations de cette rubrique, vous pourrez mettre en place un laboratoire pour évaluer Configuration Manager en simulant des activités réelles.

## Composants principaux

La configuration de votre environnement pour System Center Configuration Manager requiert certains composants principaux pour prendre en charge l'installation de Configuration Manager.

- **L'environnement lab utilise Windows Server 2012 R2**, sur lequel nous allons installer System Center Configuration Manager.

  Vous pouvez télécharger une version d'évaluation de Windows Server 2012 R2 à partir du Centre d'évaluation TechNet.

  Envisagez de modifier ou de désactiver la configuration de sécurité renforcée d'Internet Explorer pour accéder plus facilement à certains téléchargements référencés tout au long de ces exercices. Consultez Internet Explorer : Configuration de sécurité renforcée .

- **L'environnement lab utilise SQL Server 2012 SP2** pour la base de données de site.

  Vous pouvez télécharger une version d'évaluation de SQL Server 2012 à partir du Centre de téléchargement Microsoft.

  SQL Server a des versions prises en charge de SQL Server qui doivent être satisfaites pour pouvoir être utilisées avec System Center Configuration Manager.

  - Configuration Manager requiert une version 64 bits de SQL Server pour héberger la base de données de site.
  - **SQL_Latin1_General_CP1_CI_AS** en tant que classe **Classement SQL** .
  - **L'authentification Windows**, au lieu de l'authentification SQL, est obligatoire.
  - Une **instance SQL Server** dédiée est requise.
  - Ne limitez pas la **mémoire adressable système** pour SQL Server.
  - Configurez le **compte de service SQL Server** de sorte qu'il s'exécute avec un compte d'utilisateur de domaine doté de droits restreints.
  - Vous devez installer **SQL Server Reporting Services**.
  - **communications intersites** utilisent SQL Server Service Broker sur le port par défaut TCP 4022.
  - Les **communications intrasites** entre le moteur de base de données SQL Server et divers rôles de systèmes de site Configuration Manager utilisent par défaut le port TCP 1433.

- **Le contrôleur de domaine utilise Windows Server 2008 R2** avec Active Directory Domain Services. Le contrôleur de domaine fonctionne également en tant qu'hôte pour les serveurs DNS et DHCP à utiliser avec

un nom de domaine complet.

Pour plus d'informations, consultez cette vue d'ensemble des services de domaine Active Directory.

- **Hyper-V est utilisé avec quelques machines virtuelles** pour vérifier que les opérations de gestion entreprises dans ces exercices fonctionnent comme prévu. Un minimum de trois machines virtuelles est recommandé quand Windows 7 (ou version ultérieure) est installé.

  Pour plus d'informations, consultez cette vue d'ensemble d'Hyper-V.

- **Les droits d'administrateur** sont obligatoires pour tous ces composants.
  - Configuration Manager nécessite un administrateur avec des autorisations locales dans l'environnement Windows Server
  - Active Directory nécessite un administrateur avec des autorisations de modification du schéma
  - Les machines virtuelles nécessitent des autorisations locales sur les machines elles-mêmes

Bien qu'elles ne soient pas requises pour ce laboratoire, vous pouvez consulter les configurations prises en charge pour System Center Configuration Manager pour plus d'informations sur la configuration requise pour implémenter System Center Configuration Manager. Reportez-vous à la documentation pour les versions logicielles autres que celles référencées ici.

Une fois que vous avez installé tous ces composants, des étapes supplémentaires sont à suivre pour configurer votre environnement Windows pour Configuration Manager :

## Préparer le contenu d'Active Directory pour le laboratoire

Pour ce laboratoire, vous allez créer un groupe de sécurité, puis lui ajouter un utilisateur de domaine.

- Groupe de sécurité : **Evaluation**
  - Étendue du groupe : **Universal**
  - Type de groupe : **Security**
- Utilisateur du domaine : **ConfigUser**

  Dans des circonstances normales, vous n'accorderiez pas un accès universel à tous les utilisateurs au sein de votre environnement. Vous le faites ici avec cet utilisateur afin de rationaliser la mise en ligne de votre laboratoire.

Les étapes suivantes requises pour permettre aux clients Configuration Manager d'interroger les services de domaine Active Directory pour localiser les ressources de site sont répertoriées dans les procédures suivantes.

## Créer le conteneur System Management

Configuration Manager ne crée pas automatiquement le conteneur System Management requis dans les services de domaine Active Directory quand le schéma est étendu. Par conséquent, vous allez le créer pour votre laboratoire. Dans cette étape, vous devez installer l'Éditeur ADSI.

Veillez à être connecté sous un compte possédant l'autorisation **Créer tous les objets enfants** sur le conteneur **System** dans les services de domaine Active Directory.

**Pour créer le conteneur System Management :**

1. Exécutez l' **Éditeur ADSI**et connectez-vous au domaine dans lequel réside le serveur de site.
2. Développez **Domaine<nom_domaine_complet_ordinateur>**, développez **<nom_unique>**, cliquez avec le bouton droit sur **CN=System**, cliquez sur **Nouveau**, puis cliquez sur **Objet**.

3. Dans la boîte de dialogue **Créer un objet** , sélectionnez **Conteneur**et cliquez sur **Suivant**.
4. Dans le champ **Valeur** , tapez **System Management**, puis cliquez sur **Suivant**.
5. Cliquez sur **Terminer** pour terminer la procédure.

## Définir les autorisations de sécurité pour le conteneur System Management

Accordez au compte d'ordinateur du serveur de site les autorisations nécessaires à la publication des informations de site sur le conteneur. Vous devez utiliser l'Éditeur ADSI pour cette tâche également.

> **IMPORTANT**
> Vérifiez que vous êtes connecté au domaine du serveur de site avant de commencer la procédure suivante.

**Pour définir les autorisations de sécurité pour le conteneur System Management :**

1. Dans le volet de la console, développez successivement le **domaine du serveur de site**, **DC=<nom_unique_serveur>**, puis **CN=System**. Cliquez avec le bouton droit sur **CN=System Management**, puis cliquez sur **Propriétés**.
2. Dans boîte de dialogue **CN=Propriétés de System Management** , cliquez sur l'onglet **Sécurité** , puis cliquez sur **Ajouter** pour ajouter le compte d'ordinateur du serveur de site. Accordez au compte les autorisations **Contrôle intégral** .
3. Cliquez sur **Avancé**, sélectionnez le compte d'ordinateur du serveur de site, puis cliquez sur **Modifier**.
4. Dans la liste **Appliquer à** , sélectionnez **Cet objet et tous ceux descendants**.
5. Cliquez sur **OK** pour fermer la console **Éditeur ADSI** et terminer la procédure.

   Pour obtenir des informations supplémentaires sur cette procédure, consultez Étendre le schéma Active Directory pour System Center Configuration Manager

## Étendre le schéma Active Directory avec extadsch.exe

Vous allez étendre le schéma Active Directory pour ce laboratoire, car cela permet d'utiliser toutes les fonctions et fonctionnalités Configuration Manager avec une surcharge administrative minimale. L'extension du schéma Active Directory est une configuration à l'échelle de la forêt, qui ne peut être réalisée qu'une seule fois par forêt. L'extension du schéma modifie définitivement l'ensemble des classes et des attributs dans la configuration Active Directory de base. Cette action est irréversible. L'extension du schéma permet à Configuration Manager d'accéder aux composants qui lui permettront de fonctionner plus efficacement dans votre environnement de laboratoire.

> **IMPORTANT**
> Vérifiez que vous êtes connecté au contrôleur de domaine principal du schéma via un compte qui appartient au groupe de sécurité **Administrateurs du schéma** . Toute tentative d'utilisation d'autres informations d'identification échouera.

**Pour étendre le schéma Active Directory avec extadsch.exe :**

1. Créez une sauvegarde de l'état système du contrôleur de domaine principal du schéma. Pour plus d'informations sur la sauvegarde d'un contrôleur de domaine principal, consultez Sauvegarde de Windows Server.
2. Accédez à **\SMSSETUP\BIN\X64** sur le support d'installation.
3. Exécutez **extadsch.exe**.

4. Pour vérifier que l'extension du schéma a réussi, passez en revue le fichier **extadsch.log** situé dans le dossier racine du lecteur système.

   Pour obtenir des informations supplémentaires sur cette procédure, consultez Étendre le schéma Active Directory pour System Center Configuration Manager.

## Autres tâches requises

Vous devez également effectuer les tâches suivantes avant l'installation.

**Créer un dossier pour stocker tous les téléchargements**

Plusieurs téléchargements sont nécessaires pour obtenir les composants du support d'installation tout au long de cet exercice. Avant de commencer les procédures d'installation, déterminez un emplacement qui ne nécessite pas le déplacement de ces fichiers tant que vous souhaitez utiliser votre laboratoire. Il est recommandé d'utiliser un dossier unique avec des sous-dossiers distincts pour stocker ces téléchargements.

**Installer .NET et activer Windows Communication Foundation**

Vous devez installer deux infrastructures .NET : .NET 3.5.1 puis .NET 4.5.2+. Vous devez également activer Windows Communication Foundation (WCF). WCF est conçu pour offrir une approche gérable de l'informatique distribuée, une grande interopérabilité et une prise en charge directe de l'orientation service. Il simplifie le développement d'applications connectées via un modèle de programmation orienté service. Consultez Qu'est-ce que Windows Communication Foundation ? pour obtenir des informations supplémentaires sur WCF.

**Pour installer .NET et activer Windows Communication Foundation :**

1. Ouvrez **Server Manager**, puis accédez à **Gérer**. Cliquez sur **Ajouter des rôles et fonctionnalités** pour ouvrir l' **Ajouter des rôles et fonctionnalités Wizard**.
2. Passez en revue les informations fournies dans le panneau **Avant de commencer** , puis cliquez sur **Suivant**.
3. Sélectionnez **Installation basée sur un rôle ou une fonctionnalité**, puis cliquez sur **Suivant**.
4. Sélectionnez votre serveur à partir du **Pool de serveurs**, puis cliquez sur **Suivant**.
5. Examinez le panneau **Rôles de serveurs** , puis cliquez sur **Suivant**.
6. Ajoutez les **Fonctionnalités** suivantes en les sélectionnant dans la liste :
   - **Fonctionnalités de .NET Framework 3.5**
     - **.NET Framework 3.5 (inclut .NET 2.0 et 3.0)**
   - **Fonctionnalités de .NET Framework 4.5**
     - **.NET Framework 4.5**
     - **ASP.NET 4.5**
     - **Services WCF**
       - **Activation HTTP**
       - **Partage de port TCP**
7. Examinez l'écran **Rôle Serveur Web (IIS)** et **Services de rôle** , puis cliquez sur **Suivant**.
8. Examinez l'écran **Confirmation** , puis cliquez sur **Suivant**.
9. Cliquez sur **Installer** et vérifiez que l'installation s'est déroulée correctement dans le volet **Notifications** du **Gestionnaire de serveur**.

10. Une fois l'installation de base de .NET terminée, accédez au Centre de téléchargement Microsoft pour obtenir le programme d'installation web de .NET Framework 4.5.2. Cliquez sur le bouton **Télécharger** , puis sur **Exécuter** pour lancer le programme d'installation. Il détecte et installe automatiquement les composants nécessaires dans la langue sélectionnée.

Pour plus d'informations, consultez les articles suivants qui expliquent pourquoi ces composants .NET Framework sont nécessaires :

- Versions et dépendances du .NET Framework
- Procédure pas à pas de vérification de la compatibilité des applications avec .NET Framework 4 RTM
- Comment : mettre à niveau une application web ASP.NET vers ASP.NET 4
- Forum Aux Questions sur la politique de support - Microsoft .NET Framework
- Les coulisses du CLR – L'approche « In-Process Side-by-Side »

**Activer BITS, IIS et RDC**

Le service de transfert intelligent en arrière-plan (BITS) est utilisé pour les applications qui ont besoin de transférer de façon asynchrone des fichiers entre un client et un serveur. En contrôlant le flux des transferts au premier plan et en arrière-plan, le service BITS préserve la réactivité des autres applications réseau. Il reprend également automatiquement les transferts de fichiers en cas d'interruption d'une session de transfert.

Vous devez installer le service BITS pour ce laboratoire, car ce serveur de site fera également office de point de gestion.

Internet Information Services (IIS) est un serveur web flexible et évolutif, qui peut servir à héberger ce que vous voulez sur le web. Il est utilisé par Configuration Manager pour plusieurs rôles de système de site. Pour plus d'informations sur IIS, consultez Sites web pour les serveurs de système de site dans System Center Configuration Manager.

Lacompression différentielle à distance (RDC) est un ensemble d'API que les applications peuvent utiliser pour déterminer si des modifications ont été apportées à un ensemble de fichiers. La fonctionnalité RDC permet à l'application de répliquer uniquement les parties modifiées d'un fichier, limitant ainsi au maximum le trafic réseau.

**Pour activer les rôles de serveur de site BITS, IIS et RDC :**

1. Sur votre serveur de site, ouvrez **Server Manager**. Accédez à **Gérer**. Cliquez sur **Ajouter des rôles et fonctionnalités** pour ouvrir l' **Assistant Ajout de rôles et de fonctionnalités**.
2. Passez en revue les informations fournies dans le panneau **Avant de commencer** , puis cliquez sur **Suivant**.
3. Sélectionnez **Installation basée sur un rôle ou une fonctionnalité**, puis cliquez sur **Suivant**.
4. Sélectionnez votre serveur à partir du **Pool de serveurs**, puis cliquez sur **Suivant**.
5. Ajoutez les **Rôles de serveur** suivants en les sélectionnant dans la liste :
    - **Serveur web (IIS)**
        - **Fonctionnalités HTTP communes**
            - **Document par défaut**
            - **Exploration des répertoires**
            - **Erreurs HTTP**
            - **Contenu statique**

        - Redirection HTTP
    - Intégrité et diagnostics
        - Journalisation HTTP
        - Outils de journalisation
        - Observateur de demandes
        - Suivi
- Performancess
    - Compression de contenu statique
    - Compression de contenu dynamique
- Security
    - Filtrage des demandes
    - Authentification de base
    - Authentification par mappage de certificat client
    - Restrictions IP et de domaine
    - Autorisation URL
    - Autorisation Windows
- Développement d'applications
    - Extensibilité .NET 3.5
    - Extensibilité .NET 4.5
    - ASP
    - ASP.NET 3.5
    - ASP.NET 4.5
    - Extensions ISAPI
    - Filtres ISAPI
    - Fichiers Include côté serveur
- Serveur FTP
    - Service FTP
- Outils de gestion
    - Console de gestion IIS
    - IIS 6 Management Compatibility
        - Compatibilité avec la métabase de données IIS 6
        - Console de gestion IIS 6
        - Outils de script IIS 6
        - Compatibilité WMI d'IIS 6

    - **Scripts et outils de gestion d'IIS 6**
    - **Service d'administration**

6. Ajoutez les **Fonctionnalités** suivantes en les sélectionnant dans la liste :

    - **service de transfert intelligent en arrière-plan (BITS)**
        - **Extension de serveur IIS**
    - **Outils d'administration de serveur distant**
        - **Outils d'administration de fonctionnalités**
        - **Outils d'extensions du serveur BITS**

7. Cliquez sur **Installer** et vérifiez que l'installation s'est déroulée correctement dans le volet **Notifications** du **Gestionnaire de serveur**.

Par défaut, le service IIS bloque l'accès via la communication HTTP ou HTTPS à plusieurs types d'extensions et d'emplacements de fichier. Pour permettre la distribution de ces fichiers sur les systèmes clients, vous devez configurer le filtrage des demandes pour IIS sur votre point de distribution. Pour plus d'informations, consultez Filtrage des demandes IIS pour les points de distribution.

**Pour configurer le filtrage IIS sur les points de distribution :**

1. Ouvrez **IIS Manager** et sélectionnez le nom de votre serveur dans la barre latérale. Vous accédez à l'écran **Accueil** .
2. Vérifiez que l'option **Affichage des fonctionnalités** est sélectionnée au bas de l'écran **Accueil** . Accédez à **IIS** et ouvrez **Filtrage des demandes**.
3. Dans le volet **Actions** , cliquez sur **Autoriser une extension de nom de fichier...**
4. Tapez **.msi** dans la boîte de dialogue et cliquez sur **OK**.

# Installation de Configuration Manager

Vous allez déterminer quand utiliser un site principal pour gérer directement les clients. Cela permettra à votre environnement lab de prendre en charge la gestion de la mise à l'échelle du système de site des appareils potentiels.
Au cours de ce processus, vous allez également installer la console Configuration Manager qui permettra de gérer vos appareils d'évaluation.

Avant de commencer l'installation, lancez l'outil de vérification des prérequis sur le serveur utilisant Windows Server 2012 pour confirmer que tous les paramètres ont été correctement activés.

**Pour télécharger et installer Configuration Manager :**

1. Accédez à la page System Center Évaluations pour télécharger la dernière version d'évaluation de System Center Configuration Manager.
2. Décompressez le média de téléchargement dans votre emplacement prédéfini.
3. Suivez la procédure d'installation indiquée dans la rubrique Installer un site à l'aide de l'Assistant Installation de System Center Configuration Manager. Dans cette procédure, vous allez entrer les éléments suivants :

| ÉTAPE DE LA PROCÉDURE D'INSTALLATION DE SITE | SÉLECTION |
|---|---|
| Étape 4 : la page **Clé du produit** | Sélectionnez **Évaluation**. |

| ÉTAPE DE LA PROCÉDURE D'INSTALLATION DE SITE | SÉLECTION |
|---|---|
| Étape 7 : **Téléchargements requis** | Sélectionnez **Télécharger les fichiers requis** et spécifier votre emplacement prédéfini. |
| Étape 10 : **Paramètres d'installation et du site** | - **Code du site :LAB**<br>- **Nom du site :Evaluation**<br>- **Dossier d'installation :** spécifiez votre emplacement prédéfini. |
| Étape 11 : **Installation du site principal** | Sélectionnez **Installer le site principal en tant que site autonome**, puis cliquez sur **Suivant**. |
| Étape 12 : **Installation de la base de données** | - **Nom du serveur SQL Server (nom de domaine complet) :** entrez ici votre nom de domaine complet.<br>- **Nom de l'instance :** laissez ce champ vide, car vous utiliserez l'instance par défaut de SQL que vous avez installée précédemment.<br>- **Port Service Broker :** conservez le port par défaut 4022. |
| Étape 13 : **Installation de la base de données** | Conservez ces paramètres par défaut. |
| Étape 14 : **Fournisseur SMS** | Conservez ces paramètres par défaut. |
| Étape 15 : **Paramètres de communication client** | Assurez-vous que l'option **Tous les rôles de système de site acceptent uniquement les communications HTTPS depuis les clients** n'est pas sélectionnée. |
| Étape 16 : **Rôles système de site** | Entrez votre nom de domaine complet et assurez-vous que l'option **Tous les rôles de système de site acceptent uniquement les communications HTTPS depuis les clients** est toujours désactivée. |

# Activer la publication pour le site Configuration Manager

Chaque site Configuration Manager publie ses propres informations de site sur le conteneur System Management, au sein de sa partition de domaine dans le schéma Active Directory. Des canaux bidirectionnels pour la communication entre Active Directory et Configuration Manager doivent être ouverts pour gérer ce trafic. Vous devez également activer la fonctionnalité Découverte de forêts pour déterminer certains composants de votre infrastructure réseau et Active Directory.

**Pour configurer des forêts Active Directory pour la publication :**

1. Dans le coin inférieur gauche de la console Configuration Manager, cliquez sur **Administration**.
2. Dans l'espace de travail **Administration** , développez **Configuration de la hiérarchie**, puis cliquez sur **Méthodes de découverte**.
3. Sélectionnez **Découverte de forêts Active Directory** et cliquez sur **Propriétés**.
4. Dans la boîte de dialogue **Propriétés** , sélectionnez **Activer la découverte de forêts Active Directory**. Une fois cette option activée, sélectionnez **Créer automatiquement les limites de site Active Directory lorsqu'elles sont découvertes**. Une boîte de dialogue s'affiche indiquant **Voulez-vous exécuter la découverte complète dès que possible ?** Cliquez sur **Oui**.
5. Dans le groupe **Méthode de découverte** en haut de l'écran, cliquez sur **Exécuter la découverte de forêt maintenant**, puis accédez à **Forêts Active Directory** dans la barre latérale. Votre forêt Active Directory

doit figurer dans la liste des forêts découvertes.

6. Accédez à la partie supérieure de l'écran, sous l'onglet **Général** .
7. Dans l'espace de travail **Administration** , développez **Configuration de la hiérarchie**, puis cliquez sur **Forêts Active Directory**.

**Pour permettre à un site Configuration Manager de publier des informations de site vers votre forêt Active Directory :**

1. Dans la console Configuration Manager, cliquez sur **Administration**.
2. Vous allez configurer une nouvelle forêt qui n'a pas encore été découverte.
3. Dans l'espace de travail **Administration** , cliquez sur **Forêts Active Directory**.
4. Sous l'onglet **Publication** des propriétés du site, sélectionnez votre forêt connectée, puis cliquez sur **OK** pour enregistrer la configuration.

# Technical Preview pour System Center Configuration Manager

10/07/2018 • 20 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Technical Preview)*

**Bienvenue dans System Center Configuration Manager Technical Preview**. Cette rubrique fournit des détails sur la préversion qui présente de nouvelles fonctions et fonctionnalités que nous développons actuellement. Chaque version Technical Preview inaugure de nouvelles fonctionnalités qui ne sont pas présentes dans la version Current Branch de Configuration Manager au moment où la version Technical Preview est publiée. Ces fonctionnalités seront incluses dans une mise à jour de la version Current Branch, mais avant de finaliser et d'ajouter les fonctionnalités, nous souhaitons que vous puissiez les tester et nous faire part de vos commentaires.

Comme il s'agit d'une version Technical Preview, les détails et les fonctionnalités sont susceptibles de changer.

Cet article contient des informations qui s'appliquent à toutes les versions Technical Preview. Il répertorie également chaque nouvelle fonctionnalité, ainsi que la version Technical Preview où la fonctionnalité apparaît pour la première fois, par exemple la version 1806 de juin 2018. Ces fonctionnalités sont détaillées dans des rubriques distinctes dédiées à chaque préversion.

Pour plus d'informations sur les nouveautés de la version Current Branch de Configuration Manager, consultez Nouveautés de System Center Configuration Manager.

## Configuration requise et limitations pour Technical Preview

> **IMPORTANT**
> La licence de la version Technical Preview est destinée uniquement aux environnements de laboratoire. Microsoft peut ne pas fournir de services de support technique, et certaines fonctionnalités peuvent ne pas être disponibles dans la préversion du logiciel. De plus, la préversion du logiciel peut utiliser des standards de sécurité, de confidentialité, d'accessibilité, de disponibilité et de fiabilité réduites ou différentes par rapport aux logiciels fournis dans le commerce.

La plupart des prérequis du produit sont abordés dans Configurations prises en charge pour System Center Configuration Manager. Les exceptions suivantes s'appliquent aux versions Technical Preview :

- Chaque installation reste active pendant 90 jours, puis devient inactive.
- L'anglais est la seule langue prise en charge.
- Seuls les indicateurs d'installation (commutateurs) suivants sont pris en charge :
  - **/silent**
  - **/testdbupgrade**
- Par défaut, quand vous utilisez la version Technical Preview, le point de connexion de service est installé en mode en ligne. Le basculement en mode hors connexion n'est pas pris en charge.
- Les articles dédiés à chaque version Technical Preview décrivent les limitations ou les spécifications supplémentaires, le cas échéant.
- Il n'existe aucune prise en charge pour la migration vers ou à partir de cette préversion.
- Il n'existe aucune prise en charge pour la mise à niveau vers cette préversion.

- Il n'existe aucune prise en charge pour la récupération de site à partir du dossier cd.latest.
- Il n'existe aucune prise en charge de mise à niveau vers une build de production (Current Branch) à partir de cette build de version Preview. Cependant, quand des mises à jour sont disponibles pour une version Preview, vous pouvez les rechercher et les installer à partir du nœud **Mises à jour et maintenance** de la console Configuration Manager. Pour obtenir une vidéo du processus de mise à niveau dans la console, consultez Installing ConfigMgr Update Packages sur youtube.com.
- Seul un site principal autonome est pris en charge. Il n'existe aucune prise en charge pour un site d'administration centrale, plusieurs sites principaux ou des sites secondaires.

Les produits et technologies suivants sont pris en charge par cette branche de Configuration Manager. Toutefois, leur inclusion dans ce contenu n'implique pas une extension de prise en charge d'un produit ou d'une version au-delà de leur cycle de vie individuel. L'utilisation de produits qui ont dépassé leur cycle de vie n'est pas prise en charge avec Configuration Manager. Pour plus d'informations sur les politiques de support Microsoft, consultez le site web Politique de support Microsoft .

- Seules les versions suivantes de SQL Server sont prises en charge :
  - SQL Server 2017 (avec mise à jour cumulative 2 et ultérieure) à compter de Configuration Manager version 1710
  - SQL Server 2016 (sans Service Pack et versions ultérieures)
  - SQL Server 2014 (avec Service Pack 1 et version ultérieure)
  - SQL Server 2012 (avec Service Pack 3 ou version ultérieure)
- Le site prend en charge jusqu'à 10 clients, qui doivent exécuter l'une des versions suivantes de Windows :
  - Windows 10
  - Windows 8.1
  - Windows 7

## Installer et mettre à jour la version Technical Preview

La version Technical Preview de System Center Configuration Manager se distingue de la version actuelle de System Center Configuration Manager.

Pour utiliser la version Technical Preview, vous devez d'abord installer une **version de référence** de la build de la version Technical Preview. Après avoir installé une version de base de référence, vous pouvez utiliser des **mises à jour dans la console** pour actualiser votre installation avec la préversion la plus récente. En règle générale, de nouvelles versions Technical Preview sont disponibles chaque mois.

Chaque préversion est prise en charge pendant la durée de disponibilité de trois versions successives. Autrement dit, quand la version 1708 est publiée, la version 1704 n'est plus prise en charge, mais les versions 1705, 1706 et 1707 le sont toujours. Quand une base de référence n'est plus prise en charge, elle l'est toujours pour l'installation d'un nouveau site Technical Preview jusqu'à ce qu'une nouvelle version de base de référence soit disponible, à condition que vous mettez ensuite à jour cette installation avec une version prise en charge. Effectuez une mise à jour avec la version la plus récente, puis répétez ce processus jusqu'à ce que vous puissiez installer la version la plus récente de la version Technical Preview.

> **TIP**
> Quand vous installez une mise à jour de la version Technical Preview, vous mettez à jour votre installation avec cette nouvelle version Technical Preview. Une installation de la version Technical Preview ne donne jamais la possibilité d'effectuer une mise à niveau vers une installation de la version Current Branch, ni de recevoir des mises à jour de la version Current Branch.

**Versions de référence actives de la version Technical Preview :**

Vous pouvez installer une version de référence dans un délai d'un an après sa date de publication. Toutefois, lorsque vous installez un nouveau site Technical Preview, nous vous recommandons d'utiliser la dernière version de base de référence disponible.

- **Technical Preview 1806** : Configuration Manager Technical Preview 1806 est disponible à la fois sous la forme d'une mise à jour dans la console et en tant que nouvelle version de référence. Téléchargez les versions de référence à partir du Centre d'évaluation TechNet.

## Envoi de commentaires

Faites-nous part de vos commentaires sur les capacités de nos versions Technical Preview. Pour plus d'informations, consultez Commentaires produit.

Si vous avez des idées sur de nouvelles fonctionnalités que vous aimeriez voir, n'hésitez pas à nous en faire part. Pour soumettre de nouvelles idées et voter pour les idées soumises par d'autres utilisateurs, visitez notre page dédiée à cet usage.

## Fonctionnalités fournies dans la dernière version Technical Preview

Voici la liste des fonctionnalités fournies par la version Technical Preview de Configuration Manager la plus récente. Les fonctionnalités disponibles dans une version Technical Preview antérieure restent disponibles dans les versions ultérieures. De même, les fonctionnalités qui ont été ajoutées à la version Current Branch de Configuration Manager restent disponibles dans les versions Technical Preview. Cliquez sur le contenu de chaque version Technical Preview pour en savoir plus sur une fonctionnalité spécifique.

**Technical Preview version 1806.2**

- Modifications apportées aux déploiements par phases
- Prise en charge de nouveaux formats de package d'application Windows
- Amélioration apportée à la sécurité Push du client
- Insights d'administration pour une maintenance proactive
- Transférer la charge de travail des applications mobiles pour les appareils cogérés
- Options de groupe de limites pour les téléchargements à partir de pairs
- Prise en charge des mises à jour de logiciels tiers pour les catalogues personnalisés
- Améliorations apportées aux fonctionnalités de gestion du cloud
- Nouveau rapport sur la conformité des mises à jour logicielles

## Fonctionnalités fournies dans les versions Technical Preview prises en charge récentes

Voici la liste des fonctionnalités fournies avec les versions Technical Preview de Configuration Manager précédentes qui sont encore prises en charge.

| FONCTIONNALITÉ | VERSION TECHNICAL PREVIEW | VERSION CURRENT BRANCH |
|---|---|---|
| Mises à jour des logiciels tiers | Tech Preview 1806 | |
| Configurer les paramètres Windows Defender SmartScreen pour Microsoft Edge | Tech Preview 1806 | |
| Synchroniser la stratégie MDM de Microsoft Intune pour un appareil cogéré | Tech Preview 1806 | |

| FONCTIONNALITÉ | VERSION TECHNICAL PREVIEW | VERSION CURRENT BRANCH |
|---|---|---|
| Transférer la charge de travail Office 365 vers Intune avec la cogestion | Tech Preview 1806 | |
| Package Conversion Manager | Tech Preview 1806 | |
| Déployer des mises à jour logicielles sans contenu | Tech Preview 1806 | |
| Intégration de l'Outil de personnalisation Office au programme d'installation d'Office 365 | Tech Preview 1806 | |
| Améliorations apportées à la passerelle de gestion cloud | Tech Preview 1806 | |
| Amélioration des communications clientes sécurisées | Tech Preview 1806 | |
| Améliorations apportées à l'infrastructure du Centre logiciel | Tech Preview 1806 | |
| Provisionner les packages d'application Windows pour tous les utilisateurs sur un appareil | Tech Preview 1806 | |
| Améliorations apportées au tableau de bord Surface | Tech Preview 1806 | |
| Révision de l'unité par défaut pour l'inventaire matériel | Tech Preview 1806 | |
| Créer un déploiement en plusieurs phases configurées manuellement pour une séquence de tâches | Tech Preview 1805 | |
| Prise en charge du point de distribution cloud pour Azure Resource Manager | Tech Preview 1805 | |
| Agir en fonction des insights de gestion | Tech Preview 1805 | |
| Transférer la charge de travail de configuration des appareils vers Intune avec la cogestion | Tech Preview 1805 | |
| Configurer les points de distribution pour utiliser le contrôle de surcharge du réseau | Tech Preview 1805 | |
| Tableau de bord de gestion cloud | Tech Preview 1805 | |
| CMPivot | Tech Preview 1805 | |

| FONCTIONNALITÉ | VERSION TECHNICAL PREVIEW | VERSION CURRENT BRANCH |
|---|---|---|
| Amélioration des communications clientes sécurisées | Tech Preview 1805 | |
| Améliorations concernant la prise en charge des mises à jour des logiciels tiers | Tech Preview 1805 | |
| Améliorations apportées à la séquence de tâches de mise à niveau sur place de Windows 10 | Tech Preview 1805 | |
| CMTrace installé avec le client | Tech Preview 1805 | |
| Améliorations apportées à la console Configuration Manager | Tech Preview 1805 | |
| Améliorations apportées à la fonctionnalité Commentaires de la console | Tech Preview 1805 | |
| Améliorations apportées aux points de distribution compatibles PXE | Tech Preview 1805 | |
| Améliorations apportées à l'inventaire matériel pour les valeurs d'entiers longs | Tech Preview 1805 | |
| Améliorations apportées à la maintenance de WSUS | Tech Preview 1805 | |
| Améliorations apportées à la prise en charge des certificats CNG | Tech Preview 1805 | |
| Configurer une bibliothèque de contenu à distance pour le serveur de site | Tech Preview 1804 | |
| Envoyer des commentaires à partir de la console Configuration Manager | Tech Preview 1804 | |
| Centre d'aide et de support | Tech Preview 1804 | |
| Kit de ressources de Configuration Manager | Tech Preview 1804 | |
| Désinstaller une application en cas de révocation de l'approbation | Tech Preview 1804 | |
| Exclure les conteneurs Active Directory de la découverte | Tech Preview 1804 | |
| Spécifier la visibilité du lien du site web Catalogue d'applications dans le Centre logiciel | Tech Preview 1804 | |

| FONCTIONNALITÉ | VERSION TECHNICAL PREVIEW | VERSION CURRENT BRANCH |
|---|---|---|
| Filtrer les règles de déploiement automatique par architecture de mise à jour logicielle | Tech Preview 1804 | |
| Améliorations apportées au déploiement de système d'exploitation | Tech Preview 1804 | |
| Prise en charge des points de distribution cloud comme source par les points de distribution d'extraction | Tech Preview 1803 | |
| Prise en charge du téléchargement partiel dans le cache d'homologue client pour réduire l'utilisation du réseau WAN | Tech Preview 1803 | |
| Fenêtres de maintenance dans le Centre logiciel | Tech Preview 1803 | |
| Onglet personnalisé pour une page web du Centre logiciel | Tech Preview 1803 | |
| Activer la prise en charge des mises à jour de logiciels tiers sur des clients | Tech Preview 1803 | |
| Activer le copier/coller des détails de composants à partir d'affichages d'analyse | Tech Preview 1803 | |
| Extensions SCAP | Tech Preview 1803 | |

## Fonctionnalités fournies dans les versions Technical Preview précédentes

Voici la liste des fonctionnalités spécifiques fournies avec les versions Technical Preview de Configuration Manager précédentes. Ces fonctionnalités restent disponibles dans les versions ultérieures, mais ne sont pas encore disponibles dans une version Current Branch.

| FONCTIONNALITÉ | VERSION TECHNICAL PREVIEW |
|---|---|
| Améliorations apportées aux points de distribution compatibles PXE | Tech Preview 1802 |
| Tableau de bord Cycle de vie du produit | Tech Preview 1802 |
| Service de répondeur PXE basé sur le client | Tech Preview 1712 |
| Rôle serveur site haute disponibilité | Tech Preview 1706 |
| Prise en charge du démarrage réseau PXE pour IPv6 | Tech Preview 1706 |
| Utiliser Azure Active Directory | Tech Preview 1702 |

| FONCTIONNALITÉ | VERSION TECHNICAL PREVIEW |
| --- | --- |
| Évaluation de la conformité des mises à jour Windows Update pour Entreprise | Tech Preview 1702 |
| Accès aux données de point de terminaison OData | Tech Preview 1612 |
| Améliorations apportées à Asset Intelligence | Tech Preview 1608 |
| Les utilisateurs finaux peuvent installer des applications à partir du portail d'entreprise | Tech Preview 1605 |

## Voir aussi

Nouveautés de System Center Configuration Manager
Présentation de System Center Configuration Manager

**TIP**

Pour plus d'informations sur les fonctionnalités Current Branch qui nécessitent un consentement pour être activées, consultez Fonctionnalités en préversion.
Pour plus d'informations sur les fonctionnalités Current Branch qui doivent être activées en premier, consultez Activation de fonctionnalités facultatives de mises à jour.

# Fonctionnalités de la préversion technique 1806.2 de System Center Configuration Manager

10/07/2018 • 29 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Technical Preview)*

Cet article présente les fonctionnalités disponibles dans la version 1806.2 de Configuration Manager Technical Preview. Vous pouvez installer cette version pour mettre à jour et ajouter de nouvelles fonctionnalités au site de votre préversion technique.

Consultez l'article Technical Preview avant d'installer cette mise à jour. Cet article vous permet de vous familiariser avec les limitations et les conditions générales liées à l'utilisation d'une version Technical Preview, et explique comment effectuer une mise à jour d'une version vers une autre et comment envoyer des commentaires.

## Problèmes connus dans cette préversion technique

**Les clients ne se mettent pas à jour automatiquement**

Lors de la mise à jour vers la version 1806.2, le site met également à jour SQL Native Client, ce qui peut occasionner un redémarrage en attente sur le serveur de site. En raison de ce délai, certains fichiers ne sont pas mis à jour, ce qui se répercute sur la mise à niveau automatique du client.

#### Solutions de contournement

Évitez ce problème en passant manuellement à SQL Native Client *avant de mettre à jour* Configuration Manager vers la version 1806.2. Pour plus d'informations, consultez la dernière mise à jour de maintenance pour SQL Server 2012 Native Client.

Si vous déjà mis à jour votre site, la mise à niveau automatique du client et l'installation Push du client ne fonctionneront pas. Vous devrez mettre à jour les clients pour pouvoir tester intégralement la plupart des nouvelles fonctionnalités. Mettez à jour manuellement vos clients de la préversion technique en suivant la procédure ci-dessous :

1. Localisez les fichiers sources du client dans le dossier **CMUClient** du répertoire d'installation de Configuration Manager sur le serveur de site. Par exemple,
   `C:\Program Files\Configuration Manager\CMUClient`
2. Copiez la totalité du dossier CMUClient sur l'appareil client. Par exemple, `C:\Temp\CMUClient`

   Cet emplacement peut être un partage réseau accessible à partir des clients.
3. Exécutez la ligne de commande suivante dans une invite de commandes avec élévation de privilèges :
   `C:\Temp\CMUClient\ccmsetup.exe /source:C:\Temp\CMUClient`

Si vous installez un nouveau client dans votre site version 1806.2 Technical Preview, suivez la même procédure.

> **IMPORTANT**
>
> N'utilisez pas le paramètre de ligne de commande `/MP` dans ce scénario. Ce paramètre est prioritaire sur `/source` et conduit ccmsetup à télécharger le contenu du client à partir du point de gestion ou du point de distribution.
>
> Des propriétés de ligne de commande comme SMSSITECODE ou CCMLOGLEVEL peuvent être utilisées, mais ne devraient pas être nécessaires pour la mise à niveau d'un client existant.

### La version 1806.2 indique Version 1806 dans À propos de Configuration Manager

Après la mise à niveau vers la version 1806.2 Technical Preview, lorsque vous ouvrez la fenêtre **À propos de Configuration Manager** dans le coin supérieur gauche de la console, elle affiche toujours **Version 1806**.

#### Solution de contournement

Utilisez la propriété **Version du site** pour déterminer la différence entre les versions 1806 et 1806.2 :

| VERSION DU SITE | VERSION |
|---|---|
| 5.0.**8672**.1000 | 1806 |
| 5.0.**8685**.1000 | 1806.2 |

**Vous trouverez ci-dessous les nouvelles fonctionnalités propres à cette version.**

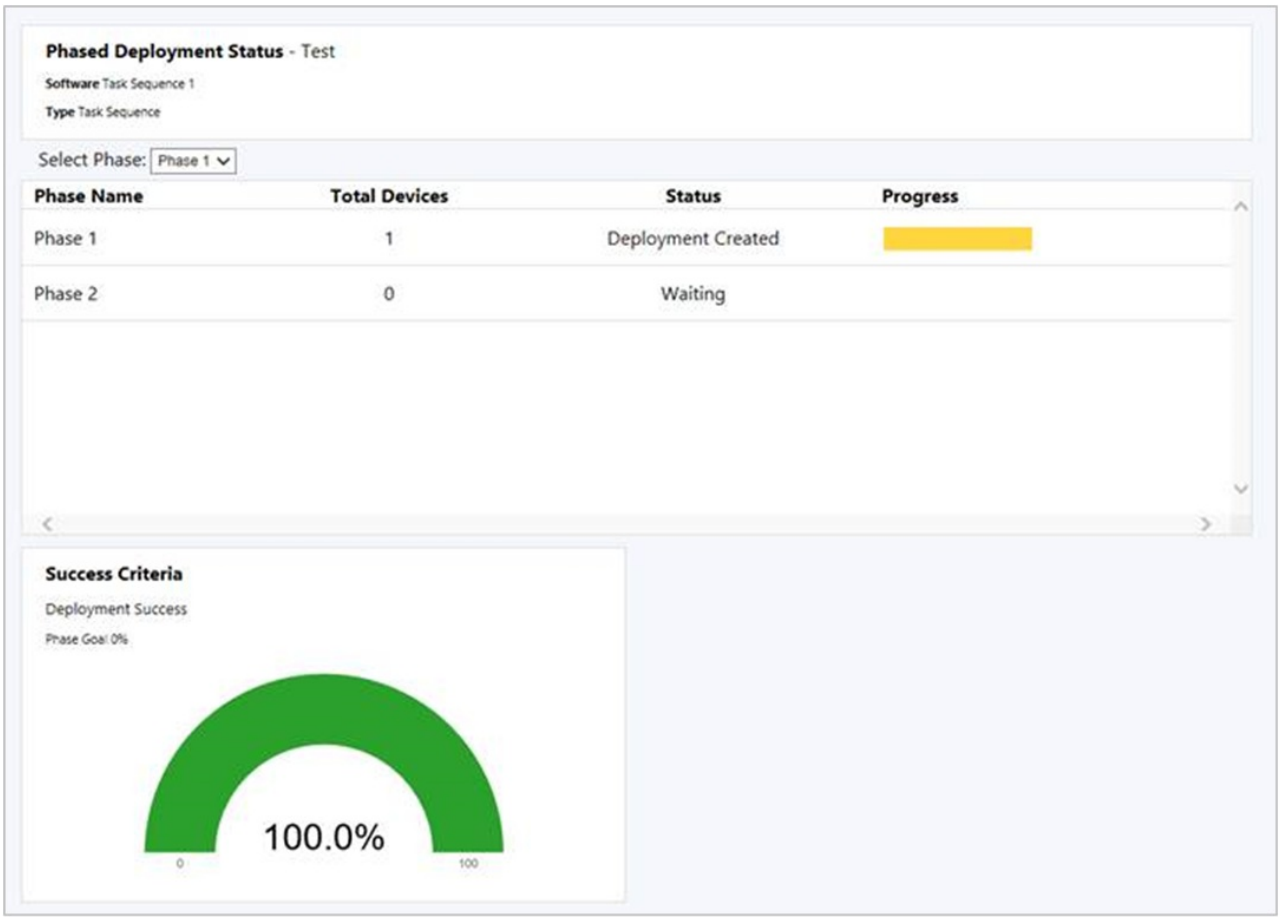
## Améliorations apportées aux déploiements par phases

Cette version intègre les améliorations suivantes du déploiement par phases :

- État du déploiement par phases
- Déploiement d'applications par phases
- Lancement graduel lors des déploiements par phases

### État du déploiement par phases

Les déploiements par phases ont maintenant une expérience de monitoring native. Dans le nœud **Déploiements** de l'espace de travail **Monitoring**, sélectionnez un déploiement par phases, puis cliquez sur **État du déploiement par phases** dans le ruban.




Ce tableau de bord montre les informations suivantes pour chaque phase du déploiement :

- **Nombre total d'appareils** : nombre d'appareils ciblés par cette phase.
- **État** : état actuel de cette phase. Chaque phase peut se trouver dans l'un des états suivants :
  - **Déploiement créé** : le déploiement par phases a créé un déploiement du logiciel sur la collection de cette phase. Les clients sont activement ciblés avec ce logiciel.
  - **En attente** : la phase précédente n'a pas encore rempli les critères de réussite pour que le déploiement passe à cette phase.
  - **Suspendu** : un administrateur a suspendu le déploiement.
- **Progression** : états de déploiement à partir des clients selon un code de couleurs. Par exemple : Réussite, En cours, Erreur, Exigences non remplies et Inconnu.

**Problème connu**

Le tableau de bord d'état du déploiement par phases affiche parfois plusieurs lignes pour une même phase.

### Déploiement d'applications par phases

Créez des déploiements par phases pour les applications. Ils permettent d'orchestrer un lancement coordonné et séquencé de logiciels en fonction de groupes et de critères personnalisables.

Dans la console de Configuration Manager, accédez à **Bibliothèque de logiciels**, développez **Gestion des applications** et sélectionnez **Applications**. Sélectionnez une application, puis cliquez sur **Créer un déploiement par phases** dans le ruban.

Le comportement d'un déploiement d'application par phases est la même que celui des séquences de tâches. Pour plus d'informations, voir Créer des déploiements par phases pour une séquence de tâches.

**Condition préalable**

Distribuez le contenu de l'application à un point de distribution avant de créer le déploiement par phases.

**Problème connu**

Vous ne pouvez pas créer de phases manuellement pour une application. L'Assistant crée automatiquement deux phases pour les déploiements d'applications.

### Lancement graduel lors des déploiements par phases

Lors d'un déploiement par phases, le lancement peut maintenant se produire progressivement dans chaque phase. Ce comportement limite les risques de problèmes de déploiement et diminue la charge sur le réseau causée par la distribution de contenu auprès des clients. Le site peut rendre le logiciel disponible progressivement en fonction de la configuration de chaque phase. Tous les clients d'une phase donnée ont une échéance qui dépend du moment de la mise à disposition du logiciel. La fenêtre entre la mise à disposition et l'échéance est la même pour tous les clients d'une phase.

Lorsque vous créez un déploiement par phases et que vous configurez manuellement une phase, configurez l'option **Rendre ce logiciel disponible progressivement sur cette période (en jours)** sur la page **Paramètres de la phase** de l'Assistant Ajouter une phase ou sur la page **Paramètres** page de l'Assistant Créer un déploiement par phases. La valeur par défaut de ce paramètre est **0** ; ainsi, par défaut, le déploiement n'est pas limité.

> **NOTE**
> Cette option n'est disponible à l'heure actuelle que pour les déploiements par phases de séquences de tâches.

## Prise en charge de nouveaux formats de package d'application Windows

Configuration Manager prend maintenant en charge le déploiement de nouveaux formats de package d'application Windows 10 (.msix) et d'ensemble d'applications (.msixbundle). Les dernières versions de Windows Insider Preview prennent actuellement en charge ces nouveaux formats.

Pour une vue d'ensemble de MSIX, voir Examen plus poussé de MSIX.

Pour savoir comment créer une application MSIX, voir Prise en charge de MSIX introduite dans la version 17682 d'Insider.

**Prérequis**

- un client Windows 10 ayant au moins la version 17682 de Windows Insider Preview ;
- un package d'application Windows au format MSIX.

**Essayez !**

Essayez d'effectuer les tâches. Envoyez-nous ensuite des commentaires pour nous indiquer comment cela a fonctionné.

1. Dans la console de Configuration Manager, créez une application.
2. Sélectionnez le **Type** de fichier d'installation de l'application **Package d'application Windows (*.appx, *.appxbundle, *.msix, *.msixbundle)**.
3. Déployez l'application sur le client qui a la dernière version de Windows Insider Preview.

## Amélioration apportée à la sécurité Push du client

Avec la méthode d'installation Push du client Configuration Manager, le serveur de site crée une connexion à distance au client pour lancer l'installation. À partir de cette version, le site peut exiger l'authentification mutuelle Kerberos en interdisant le recours à NTLM en secours avant d'établir la connexion. Cette amélioration permet de sécuriser la communication entre le serveur et le client.

En fonction de vos stratégies de sécurité, il est possible que votre environnement préfère ou requière déjà l'authentification Kerberos plutôt qu'une authentification NTLM plus ancienne. Pour plus d'informations sur l'aspect sécurité de ces protocoles d'authentification, voir Paramètre de stratégie de sécurité Windows pour restreindre l'authentification NTLM.

**Condition préalable**

Pour pouvoir utiliser cette fonctionnalité, il faut que les clients se trouvent dans une forêt Active Directory approuvée. Kerberos sous Windows s'appuie sur Active Directory pour l'authentification mutuelle.

**Essayez !**

Essayez d'effectuer les tâches. Envoyez-nous ensuite des commentaires pour nous indiquer comment cela a fonctionné.

Lors de la mise à niveau du site, le comportement existant est conservé. Une fois les propriétés d'installation Push du client *ouvertes*, le site active automatiquement la vérification Kerberos. Si nécessaire, vous pouvez autoriser la connexion à utiliser en secours une connexion NTLM moins sécurisée, ce qui n'est pas recommandé.

1. Dans la console Configuration Manager, accédez à l'espace de travail **Administration**, développez **Configuration du site**, puis sélectionnez **Sites**. Sélectionnez le site cible. Dans le ruban, cliquez sur **Paramètres d'installation du client** et sélectionnez **Installation Push du client**.

2. Le site vient d'activer la vérification Kerberos pour l'installation Push du client. Cliquez sur **OK** pour fermer la fenêtre.

3. Si votre environnement l'impose, examinez l'option **Autoriser le recours à NTLM en secours pour la connexion** sur l'onglet **Général** de la fenêtre Propriétés d'installation Push du client. Cette option est désactivée par défaut.

## Insights d'administration pour la maintenance proactive

Des insights d'administration supplémentaires sont disponibles dans cette version pour mettre en évidence les problèmes de configuration potentiels. Passez en revue les règles suivantes dans le nouveau groupe **Maintenance proactive** :

- **Éléments de configuration inutilisés** : éléments de configuration qui ne font pas partie d'une base de référence de configuration et datent de plus de 30 jours.
- **Images de démarrage inutilisées** : images de démarrage non référencées pour l'utilisation de séquences de tâches ou le démarrage PXE.
- **Groupes de limites sans système de site attribué** : sans systèmes de site attribué, les groupes de limites ne peuvent être utilisés que pour l'attribution de site.
- **Groupes de limites sans membres** : les groupes de limites ne sont pas applicables à l'attribution de site ou à la recherche de contenu s'ils n'ont aucun membre.
- **Points de distribution ne fournissant pas de contenu aux clients** : points de distribution qui n'ont pas distribué de contenu aux clients au cours des 30 derniers jours. Ces données s'appuient sur les rapports d'historique de téléchargement des clients.
- **Mises à jour non valides trouvées** : les mises à jour ayant passé la date d'expiration ne sont pas applicables dans le cadre du déploiement.

## Transférer la charge de travail des applications mobiles pour les appareils cogérés

Gérez des applications mobiles avec Microsoft Intune tout en continuant à utiliser Configuration Manager pour déployer des applications de bureau Windows. Pour transférer la charge de travail des applications modernes, accédez à la page de propriétés de cogestion. Déplacez le curseur de Configuration Manager vers Pilote ou Tout.

Une fois cette charge de travail transférée, toutes les applications disponibles déployées à partir d'Intune seront accessibles sur le Portail d'entreprise. Les applications déployées à partir de Configuration Manager sont disponibles dans le centre logiciel.

Pour plus d'informations, consultez les articles suivants :

- Cogestion pour les appareils Windows 10
- Qu'est-ce que la gestion des applications Microsoft Intune ?

## Options de groupe de limites pour les téléchargements à partir de pairs

Les groupes de limites intègrent maintenant des paramètres supplémentaires qui offrent davantage de contrôle sur la distribution du contenu dans l'environnement. Cette version ajoute les options suivantes :

- **Autoriser les téléchargements à partir de pairs dans ce groupe de limites** : ce paramètre est activé par défaut. Le point de gestion fournit aux clients une liste d'emplacements de contenu qui comprend des sources de pairs.

  Il existe deux scénarios courants dans lesquels il peut être envisageable de désactiver cette option :

  - Si votre groupe de limites comporte des limites provenant d'emplacements éloignés sur le plan géographique, comme un VPN. Deux clients peuvent se trouver dans le même groupe de limites, parce qu'ils sont connectés au moyen d'un VPN, alors qu'ils sont situés à des endroits très différents, ce qui ne convient pas pour le partage de contenu entre pairs.

- Si vous utilisez un seul grand groupe de limites pour l'attribution de site, qui ne fait référence à aucun point de distribution.

- **Lors des téléchargements à partir de pairs, utiliser seulement les pairs qui se trouvent dans le même sous-réseau** : ce paramètre dépend de celui qui est illustré ci-dessus. Lorsque cette option est activée, le point de gestion n'inclut dans la liste des emplacements de contenu que les sources de pairs qui se trouvent dans le même sous-réseau que le client.

  Quelques scénarios courants pour l'activation de cette option :

  - Votre conception de groupe de limites pour la distribution de contenu comprend un grand groupe de limites qui coïncide en partie avec d'autres groupes de limites plus petits. Avec ce nouveau paramètre, la liste des sources de contenu que le point de gestion fournit aux clients n'inclut que les sources de pairs provenant du même sous-réseau.

  - Vous avez un seul grand groupe de limites pour tous les emplacements de bureau distant. Lorsque cette option est activée, les clients ne partagent du contenu qu'au sein du sous-réseau qui se trouve à l'emplacement du bureau distant, plutôt que de prendre le risque de partager du contenu entre différents emplacements.

**Problème connu**

Si le client de la source de pairs a plusieurs adresses IP (IPv4, IPv6 ou les deux), la mise en cache partagé entre systèmes homologues ne fonctionne pas. La nouvelle option **Lors des téléchargements à partir de pairs, utiliser seulement les pairs qui se trouvent dans le même sous-réseau** n'a aucun effet si la source de pairs comporte plusieurs adresses IP.

## Prise en charge de mises à jour de logiciels tiers pour les catalogues personnalisés

Pour répondre à la demande que vous avez exprimée par le biais des commentaires UserVoice, cette nouvelle version comprend une meilleure prise en charge des mises à jour de logiciels tiers. La version 1806 Technical Preview prenait en charge les *catalogues de partenaires*, qui sont des catalogues référencés par des éditeurs de logiciels. Les catalogues que vous fournissez et qui ne sont pas inscrits auprès de Microsoft sont appelés catalogues *personnalisés*. Ajoutez des catalogues personnalisés dans la console de Configuration Manager.

**Prérequis**

- Configurez les mises à jour des logiciels tiers. Effectuez la phase 1 : Activer et configurer la fonctionnalité.
- Un catalogue personnalisé signé numériquement contenant des mises à jour logicielles signées numériquement.
- L'administrateur exige les autorisations suivantes :
  - Site : Créer, modifier

**Essayez !**

Essayez d'effectuer les tâches. Envoyez-nous ensuite des commentaires pour nous indiquer comment cela a fonctionné.

1. Dans la console de Configuration Manager, accédez à l'espace de travail **Bibliothèque de logiciels**, développez **Mises à jour logicielles**, puis sélectionnez le nœud **Catalogues de mises à jour de logiciels tiers**. Cliquez sur **Ajouter un catalogue personnalisé** dans le ruban.
2. Sur la page **Général**, spécifiez les informations suivantes :
   - **URL de téléchargement** : adresse HTTPS valide du catalogue personnalisé.

- **Éditeur** : nom de l'organisation qui publie le catalogue.
- **Nom** : nom du catalogue à afficher dans la console de Configuration Manager.
- **Description** : description du catalogue.
- **URL de support** (facultatif) : adresse HTTPS valide d'un site web d'aide sur le catalogue.
- **Contact de support** (facultatif) : coordonnées à contacter pour obtenir de l'aide sur le catalogue.

3. Effectuez toutes les étapes de l'Assistant. L'Assistant ajoute le nouveau catalogue avec un état désabonné.
4. Abonnez-vous au catalogue personnalisé avec l'action **S'abonner au catalogue** existante. Pour plus d'informations, voir Phase 2 : S'abonner à un catalogue tiers et synchroniser les mises à jour.

> **NOTE**
> Vous ne pouvez pas ajouter de catalogues utilisant la même URL de téléchargement, ni modifier les propriétés des catalogues. Si vous avez spécifié des propriétés incorrectes pour un catalogue personnalisé, supprimez-le avant de l'ajouter à nouveau.

#### Se désabonner d'un catalogue

Pour vous désabonner d'un catalogue, sélectionnez-le dans la liste, puis cliquez sur **Se désabonner du catalogue** dans le ruban. Le désabonnement d'un catalogue provoque les actions et les comportements suivants :

- Le site arrête la synchronisation des nouvelles mises à jour.
- Le site bloque les certificats associés pour le contenu de mise à jour et de signature du catalogue.
- Les mises à jour existantes ne sont pas supprimées, mais il n'est pas forcément possible de les publier ou de les déployer.

#### Supprimer un catalogue personnalisé

Supprimez les catalogues personnalisés à partir du même nœud de la console. Sélectionnez un catalogue personnalisé à l'état *Désabonné*, puis cliquez sur **Supprimer le catalogue personnalisé**. Si vous avez déjà mis en place un abonnement à ce catalogue, désabonnez-vous avant de le supprimer. Vous ne pouvez pas supprimer les catalogues de partenaires. La suppression d'un catalogue personnalisé a pour effet de le retirer de la liste des catalogues. Cette action n'affecte pas les mises à jour logicielles que vous avez publiées sur votre point de mise à jour logicielle.

#### Problème connu

L'action de suppression est grisée sur les catalogues personnalisés, ce qui empêche de supprimer des catalogues personnalisés dans la console. Pour contourner ce problème, utilisez l'outil **wbemtest** sur le serveur de site. Effectuez une requête sur l'instance que vous souhaitez supprimer avec le nom ou l'URL de téléchargement, par exemple : `select * from SMS_ISVCatalog where DownloadURL="http://www.contoso.com/catalog.cab"`. Dans la fenêtre de résultat de la requête, sélectionnez l'objet, puis cliquez sur **Supprimer**.

## Améliorations apportées aux fonctionnalités de gestion cloud

Cette version intègre les améliorations suivantes :

- Les fonctionnalités suivantes prennent maintenant en charge l'utilisation d'Azure U.S. Government Cloud :
  - l'intégration du site pour la **Gestion cloud** avec les Services Azure ;
  - le déploiement d'une Passerelle de gestion cloud avec Azure Resource Manager ;
  - le déploiement d'un point de distribution cloud avec Azure Resource Manager.
- Les clients utilisent Windows AutoPilot pour configurer Windows 10 sur des appareils joints à Azure Active Directory et connectés au réseau local. Pour installer ou mettre à niveau le client Configuration Manager sur

ces appareils, il n'est plus nécessaire de configurer un point de distribution cloud ou un point de distribution local sur **Autoriser les clients à se connecter anonymement**. Au lieu de cela, activez l'option de site **Utiliser des certificats générés par Configuration Manager pour les systèmes de site HTTP**, qui permet à un client joint à un domaine cloud de communiquer avec un point de distribution local compatible avec le protocole HTTP. Pour plus d'informations, voir Amélioration des communications clientes sécurisées.

## Nouveau rapport sur la conformité des mises à jour logicielles

L'affichage des rapports de conformité des mises à jour logicielles comporte généralement des données provenant de clients qui n'ont pas contacté le site récemment. Un nouveau rapport permet de filtrer les résultats de conformité d'un groupe de mises à jour logicielles donné sur les clients « sains ». Ce rapport affiche l'état de conformité plus réaliste des clients actifs de votre environnement.

Pour afficher le rapport, accédez à l'espace de travail **Monitoring**, développez **Reporting**, puis **Rapports** et **Mises à jour logicielles – Conformité A**, puis sélectionnez **Conformité 9 – Conformité et intégrité globales**. Spécifiez **Groupe de mises à jour**, **Nom de la collection** et l'état **d'intégrité du client**.

Le rapport comprend les parties suivantes :

- **Proportion de clients sains par rapport au nombre total de clients** : ce graphique à barres compare le nombre de clients « sains », qui ont communiqué avec le site au cours de la période indiquée, avec le nombre total de clients dans la collection spécifiée.
- **Vue d'ensemble de la conformité** : ce graphique à secteurs indique l'état de conformité global du groupe de mises à jour logicielles concerné sur les clients actifs dans la collection spécifiée.
- **5 principales mises à jour non conformes par ID d'article** : ce graphique à barres affiche les cinq principales mises à jour logicielles du groupe concerné qui ne sont pas conformes sur les clients actifs dans la collection spécifiée.
- La partie inférieure du rapport est un tableau plus détaillé, qui liste les mises à jour logicielles du groupe spécifié.

## Étapes suivantes

Pour obtenir des informations complémentaires sur l'installation ou la mise à jour de l'édition Technical Preview, consultez Technical Preview pour System Center Configuration Manager.

# Fonctionnalités de la version Technical Preview 1806 de System Center Configuration Manager

18/06/2018 • 38 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Technical Preview)*

Cet article présente les fonctionnalités disponibles dans la version Technical Preview 1806 de Configuration Manager. Vous pouvez installer cette version pour mettre à jour et ajouter de nouvelles fonctionnalités au site de votre préversion technique.

Consultez l'article Technical Preview avant d'installer cette mise à jour. Cet article vous permet de vous familiariser avec les limitations et les conditions générales liées à l'utilisation d'une version Technical Preview, et explique comment effectuer une mise à jour d'une version vers une autre et comment envoyer des commentaires.

## Problèmes connus dans cette préversion technique

**Impossible de mettre à niveau le site à l'aide de la bibliothèque de contenu distante**

Vous ne parvenez pas à mettre à niveau le site, et les erreurs suivantes sont journalisées dans **cmupdate.log** :

```
Failed to find any valid drives
GetContentLibraryParameters failed; 0x80070057
ERROR: Failed to process configuration manager update.
```

Dans cette version, ce problème se produit lorsque la bibliothèque de contenu se trouve à un emplacement distant.

**Solution de contournement**

Déplacez la bibliothèque de contenu vers un lecteur local du serveur de site. Pour plus d'informations, consultez Configurer une bibliothèque de contenu à distance pour le serveur de site.

**Vous trouverez ci-dessous les nouvelles fonctionnalités propres à cette version.**

## Mises à jour des logiciels tiers

Pour répondre à la demande que vous avez exprimée par le biais des commentaires UserVoice, cette nouvelle version comprend une meilleure prise en charge des mises à jour de logiciels tiers. Pour certains scénarios courants, vous n'avez plus besoin d'utiliser l'éditeur de mise à jour System Center (SCUP). Le nouveau nœud **Catalogues de mises à jour de logiciels tiers** de la console Configuration Manager vous permet de vous abonner à des catalogues tiers, de publier leurs mises à jour sur votre point de mise à jour logicielle, puis de les déployer sur les clients.

Cette version comprend les catalogues de mise à jour de logiciels tiers suivants :

| ÉDITEUR | NOM DU CATALOGUE |
|---|---|
| HP | Catalogue de mises à jour des clients HP |

SCUP continue de prendre en charge les autres catalogues et scénarios. La liste des catalogues qui se trouve sous le nœud Catalogues de mises à jour de logiciels tiers de la console Configuration Manager est une liste dynamique. Elle est donc mise à jour dès que de nouveaux catalogues sont disponibles et pris en charge.

**Prérequis**

- Configurez la gestion des mises à jour de logiciels avec un point de mise à jour logicielle HTTPS. Pour plus d'informations, consultez Préparer la gestion des mises à jour logicielles.
  - Dans cette version, le point de mise à jour logicielle doit se trouver sur le serveur de site pour cette fonctionnalité.
- Suffisamment d'espace disque sur le point de mise à jour logicielle où se trouve le dossier WSUSContent pour stocker le contenu binaire source des mises à jour de logiciels tiers. La quantité de stockage nécessaire varie en fonction du fournisseur, du type de mise à jour, ainsi que des mises à jour que vous publiez en vue de leur déploiement. Si vous devez déplacer le dossier WSUSContent vers un lecteur qui contient davantage d'espace, consultez ce billet de blog de l'équipe du support WSUS : How to change the location where WSUS stores updates locally.
- Activez puis déployez le paramètre client Activer les mises à jour de logiciels tiers dans le groupe **Mises à jour logicielles**.
- Le serveur de site nécessite un accès Internet au site download.microsoft.com via le port HTTPS 443. Le service de synchronisation des mises à jour de logiciels tiers doit être en cours d'exécution sur le serveur de site. Ce service met à jour la liste des catalogues tiers disponibles, télécharge les catalogues lorsque vous vous y abonnez et télécharge les mises à jour lorsque celles-ci sont publiées. Si nécessaire, configurez les paramètres du proxy Internet sous l'onglet **Proxy** des propriétés du rôle de système de site, sur l'ordinateur du serveur de site.

**Essayez !**

Essayez d'effectuer les tâches. Envoyez-nous ensuite des commentaires pour nous indiquer comment cela a fonctionné.

##### Phase 1 : Activer et configurer la fonctionnalité

Pour activer et configurer la fonctionnalité à utiliser, effectuez les opérations suivantes *une fois pour chaque hiérarchie* :

1. Dans la console de Configuration Manager, accédez à l'espace de travail **Administration**. Développez **Configuration du site**, puis sélectionnez le nœud **Sites**.
2. Sélectionnez le site de niveau supérieur dans la hiérarchie. Dans le ruban, cliquez sur **Configurer les composants de site**, puis sélectionnez **Point de mise à jour logicielle**.
3. Passez l'onglet **Mises à jour tierces**. Sélectionnez l'option **Activer les mises à jour de logiciels tiers**. Pour plus d'informations sur les options de certificat, consultez Améliorations concernant la prise en charge des mises à jour des logiciels tiers.

> **NOTE**
> Si vous utilisez l'option par défaut, qui permet de gérer le certificat avec Configuration Manager, un nouveau certificat de type **Third-party WSUS Signing** (Signature WSUS tierce) est créé sous le nœud **Certificats**, sous **Sécurité**, dans l'espace de travail **Administration**.

##### Phase 2 : S'abonner à un catalogue tiers et synchroniser les mises à jour

Procédez aux étapes suivantes pour *chaque catalogue tiers* auquel vous voulez vous abonner :

1. Dans la console Configuration Manager, accédez à l'espace de travail **Bibliothèque de logiciels**. Développez **Mises à jour logicielles**, puis sélectionnez le nœud **Catalogues de mises à jour de logiciels tiers**.
2. Sélectionnez le catalogue auquel vous abonner, puis cliquez sur **S'abonner au catalogue** dans le ruban.
3. Examinez et approuvez le certificat du catalogue.

> **NOTE**
>
> Lorsque vous vous abonnez à un catalogue de mises à jour de logiciels tiers, le certificat que vous examinez et approuvez dans l'Assistant est ajouté au site. Ce certificat appartient au type **Catalogue des mises à jour de logiciels tiers**. Vous pouvez le gérer dans le nœud **Certificats**, situé sous **Sécurité**, dans l'espace de travail **Administration**.

4. Effectuez toutes les étapes de l'Assistant.

> **TIP**
>
> Après un premier abonnement, le catalogue doit commencer à télécharger les mises à jour immédiatement. Ensuite, dans cette version, il effectue une resynchronisation toutes les 24 heures. Si vous ne souhaitez pas attendre que le catalogue télécharge automatiquement les mises à jour, cliquez sur **Synchroniser maintenant** dans le ruban.
>
> Une fois le catalogue téléchargé, les métadonnées des produits doivent être synchronisées avec le point de mise à jour logicielle. Pour plus d'informations sur ce processus et sur le lancement manuel du téléchargement, consultez Synchroniser les mises à jour logicielles. À ce stade, vous pouvez voir les mises à jour des logiciels tiers sous le nœud **Toutes les mises à jour**.

5. Ensuite, configurez le point de mise à jour logicielle **Produits** pour le catalogue tiers auquel vous vous êtes abonné. Pour plus d'informations, consultez Configurer les classifications et les produits à synchroniser. Lorsque les critères des produits sont modifiés, vous devez effectuer une nouvelle synchronisation des mises à jour logicielles.

Pour que vous puissiez voir les résultats de la conformité des clients, ceux-ci doivent analyser et évaluer les mises à jour. Vous pouvez déclencher ce cycle manuellement sur un client, à partir du panneau de configuration Configuration Manager, en exécutant l'action **Cycle d'analyse des mises à jour de logiciels**. Pour plus d'informations sur ce processus, consultez Présentation des mises à jour logicielles.

#### Phase 3 : Déployer des mises à jour de logiciels tiers

Procédez aux étapes suivantes pour *chaque mise à jour de logiciel tiers* que vous souhaitez déployer sur les clients :

1. Dans la console Configuration Manager, accédez à l'espace de travail **Bibliothèque de logiciels**. Développez **Mises à jour logicielles**, puis sélectionnez le nœud **Toutes les mises à jour logicielles**.

> **TIP**
>
> Pour filtrer la liste des mises à jour, cliquez sur **Ajouter des critères**. Par exemple, ajoutez **Fournisseur** pour **Adobe Systems, Inc.** afin d'afficher toutes les mises à jour Adobe.

2. Sélectionnez les mises à jour dont ont besoin les clients. Cliquez sur **Publier le contenu des mises à jour de logiciels tiers** et surveillez la progression dans le journal SMS_ISVUPDATES_SYNCAGENT.log. Cette action télécharge les fichiers binaires de mise à jour du fournisseur, et les stocke dans le dossier WSUSContent situé sur le point de mise à jour logicielle. Elle fait également passer la mise à jour de l'état « métadonnées uniquement » à l'état « avec contenu et prête au déploiement ».

> **NOTE**
>
> Lorsque vous publiez le contenu de mises à jour de logiciels tiers, tous les certificats utilisés pour signer le contenu sont ajoutés au site. Ces certificats appartiennent au type **Contenu des mises à jour de logiciels tiers**. Vous pouvez les gérer dans le nœud **Certificats**, situé sous **Sécurité**, dans l'espace de travail **Administration**.

3. Déployez les mises à jour à l'aide du processus de gestion des mises à jour logicielles existant. Pour plus d'informations, consultez Déployer des mises à jour logicielles. Dans la page **Emplacement de téléchargement** de l'Assistant Déploiement des mises à jour logicielles, sélectionnez l'option par défaut **Télécharger les mises à jour logicielles à partir d'Internet**. Dans ce scénario, le contenu a déjà été publié sur le point de mise à jour logicielle, qui est utilisé pour télécharger le contenu du package de déploiement.

#### Surveillance de la progression du téléchargement des mises à jour de logiciels tiers

La synchronisation des mises à jour de logiciels tiers est gérée par le composant SMS_ISVUPDATES_SYNCAGENT, sur le serveur de site. Vous pouvez afficher les messages d'état de ce composant, ou lire des informations d'état plus détaillées dans le journal SMS_ISVUPDATES_SYNCAGENT.log. Ce journal se trouve sur le serveur de site dans le sous-dossier **Journaux** du répertoire d'installation du site. Par défaut, le chemin est le suivant : `C:\Program Files\Microsoft Configuration Manager\Logs`. Pour plus d'informations sur la surveillance du processus global de gestion des mises à jour logicielles, consultez Surveiller les mises à jour logicielles.

#### Problèmes connus

- Le service de synchronisation des mises à jour de logiciels tiers ne prend pas en charge le point de mise à jour logicielle configuré pour utiliser un **Compte de connexion du serveur WSUS**. Si ce compte est configuré sous l'onglet **Paramètres de compte et proxy** de la page Propriétés du point de mise à jour logicielle, vous verrez l'erreur suivante dans le journal SMS_ISVUPDATES_SYNCAGENT.log : `WSUS access account appears to be configured, it is not yet supported for third party updates sync.` Pour plus d'informations sur ce compte, consultez Compte de connexion de point de mise à jour logicielle.

- Ne confondez pas l'utilisation des autres outils tels que SCUP, avec cette nouvelle fonctionnalité intégrée de mise à jour des logiciels tiers. Le service de synchronisation des mises à jour de logiciels tiers ne peut pas publier le contenu des mises à jour de métadonnées uniquement qui ont été ajoutées à WSUS par une autre application, un autre outil ou un autre script, tel que SCUP. L'action **Publier le contenu des mises à jour de logiciels tiers** échoue avec ces mises à jour. Si vous avez besoin de déployer des mises à jour tierces qui ne sont pas encore prises en charge par cette fonctionnalité, utilisez l'intégralité de votre processus existant pour déployer ces mises à jour.

## Configurer les paramètres Windows Defender SmartScreen pour Microsoft Edge

Cette version ajoute les trois paramètres Windows Defender SmartScreen à la stratégie de paramètres de conformité du navigateur Microsoft Edge. Dans la page **Paramètres de SmartScreen**, la stratégie inclut désormais les paramètres supplémentaires suivants :

- **Autoriser SmartScreen** : spécifie si Windows Defender SmartScreen est autorisé. Pour plus d'informations, consultez la stratégie de navigateur AllowSmartScreen.
- **Les utilisateurs peuvent remplacer l'invite SmartScreen pour les sites** : spécifie si les utilisateurs peuvent ignorer les avertissements du filtre Windows Defender SmartScreen concernant les sites web potentiellement malveillants. Pour plus d'informations, consultez la stratégie de navigateur PreventSmartScreenPromptOverride.
- **Les utilisateurs peuvent remplacer l'invite SmartScreen pour les sites** : spécifie si les utilisateurs peuvent ignorer les avertissements du filtre Windows Defender SmartScreen concernant le téléchargement de fichiers non vérifiés. Pour plus d'informations, consultez la stratégie de navigateur PreventSmartScreenPromptOverrideForFiles.

## Synchroniser la stratégie MDM de Microsoft Intune pour un appareil cogéré

À compter de cette version, lorsque vous passez à une charge de travail en cogestion, les appareils cogérés sont automatiquement synchronisés avec la stratégie MDM de Microsoft Intune. Cette synchronisation est effectuée lorsque vous lancez l'action **Télécharger la stratégie d'ordinateur** à partir de Notification du client, dans la console Configuration Manager. Pour plus d'informations, consultez Lancer une récupération de stratégie client en utilisant une notification de client.

## Transférer la charge de travail Office 365 vers Intune avec la cogestion

Vous pouvez désormais transférer la charge de travail Office 365 de Configuration Manager vers Microsoft Intune après avoir activé la cogestion. Pour transférer cette charge de travail, accédez à la page de propriétés de cogestion et déplacez le curseur actuellement sur Configuration Manager vers Pilote ou Tout. Pour plus d'informations, consultez Cogestion pour les appareils Windows 10.

Il existe également une nouvelle condition globale : **Are Office 365 applications managed by Intune on the device ?** (Les applications Office 365 sont-elles gérées par Intune sur cet appareil ?). Cette condition est ajoutée par défaut dans le cadre d'une exigence pour les nouvelles applications Office 365. Si vous transférez cette charge de travail, les clients cogérés ne répondront pas à cette exigence de l'application. Par conséquent, n'installez pas Office 365 par le biais d'un déploiement Configuration Manager.

**Problème connu**

- Ce transfert de charge de travail concerne uniquement les déploiements Office 365. Configuration Manager continue de gérer les mises à jour Office 365. Pour obtenir plus d'informations, ainsi qu'une solution de contournement, consultez la section Le changement du paramètre client Office 365 ne s'applique pas dans les notes de publication de Configuration Manager version 1802.

## Package Conversion Manager

Package Conversion Manager est un nouvel outil intégré qui vous permet de convertir des packages Configuration Manager 2007 hérités en applications Configuration Manager Current Branch. Ensuite, vous pouvez utiliser les fonctionnalités des applications telles que les dépendances, les règles de spécification et l'affinité entre utilisateur et appareil.

> **TIP**
> La documentation héritée concernant les fonctionnalités existantes de Package Conversion Manager est disponible sur TechNet. Les informations pertinentes sont en cours de migration vers la bibliothèque docs.microsoft.com.

**Essayez !**

Essayez d'effectuer les tâches. Envoyez-nous ensuite des commentaires pour nous indiquer comment cela a fonctionné.

> **IMPORTANT**
> Si vous avez installé une ancienne version de Package Conversion Manager, désinstallez-la avant de mettre à niveau votre site. La nouvelle version intégrée ne nécessite pas d'installation, toutefois, elle peut créer un conflit avec les versions existantes.

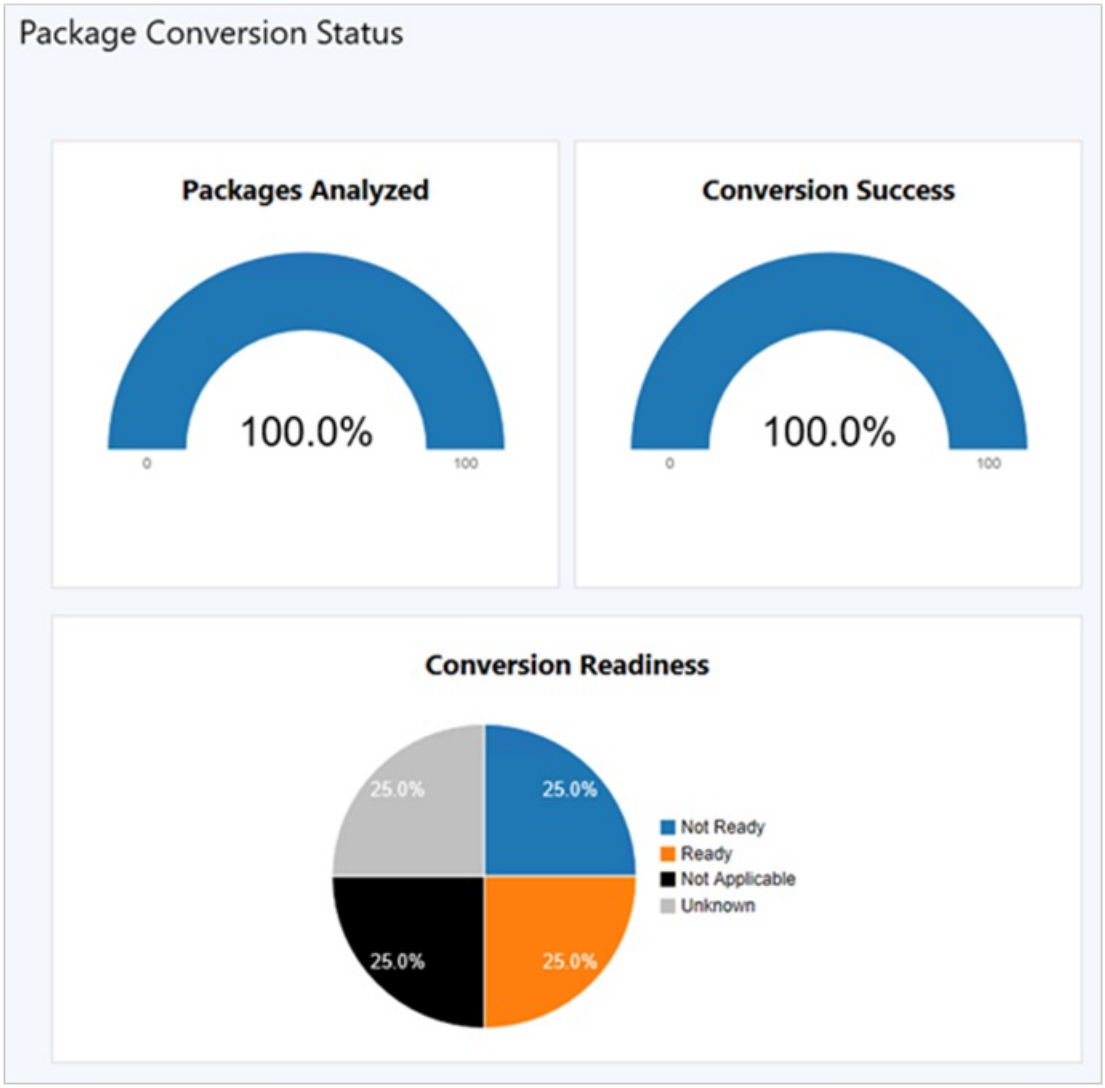
1. Dans la console Configuration Manager, accédez à l'espace de travail **Bibliothèque de logiciels**. Développez **Gestion des applications**, puis sélectionnez **Packages**.
2. Sélectionnez un package. Les trois options suivantes sont disponibles dans le groupe **Conversion de packages** du ruban :
   - **Analyser le package** : démarre le processus de conversion en analysant le package.

- **Convertir le package** : cette action permet de convertir facilement certains packages en applications.
- **Corriger et convertir** : certains packages nécessitent que les problèmes soient résolus avant leur conversion en applications.

Pour plus d'informations sur ces actions, consultez Comment analyser et convertir des packages.

3. Accédez à l'espace de travail **Monitoring** (Surveillance), puis sélectionnez **Package Conversion Status** (État de la conversion du package). Ce nouveau tableau de bord montre l'analyse globale, ainsi que l'état de conversion des packages du site. Une nouvelle tâche d'arrière-plan résume automatiquement les données d'analyse.

> **TIP**
> Package Conversion Manager ne nécessite pas qu'une analyse de packages soit planifiée. Cette action est désormais gérée par la tâche de totalisation intégrée.




## Déployer des mises à jour logicielles sans contenu

Vous pouvez désormais déployer des mises à jour logicielles sur vos appareils sans avoir à télécharger et à distribuer préalablement le contenu des mises à jour logicielles sur les points de distribution. Cette fonctionnalité est utile lorsque le contenu des mises à jour est très volumineux, ou si vous souhaitez que les clients obtiennent toujours le contenu via le service cloud Microsoft Update. Dans ce cas, les clients peuvent également télécharger le contenu auprès d'homologues qui disposent déjà du contenu nécessaire. Le client Configuration Manager continue de gérer le téléchargement de contenu. Vous pouvez donc utiliser la fonctionnalité de cache d'homologue Configuration Manager ou d'autres technologies telles que l'optimisation de la distribution. Cette fonctionnalité

prend en charge tous les types de mises à jour pris en charge par la gestion des mises à jour logicielles Configuration Manager, y compris les mises à jour Windows et Office.

**Essayez !**

Essayez d'effectuer les tâches. Envoyez-nous ensuite des commentaires pour nous indiquer comment cela a fonctionné.

1. Démarrez un déploiement de mises à jour logicielles comme vous le feriez habituellement. Pour plus d'informations, consultez Déployer des mises à jour logicielles.
2. Dans la page **Package de déploiement** de l'Assistant Déploiement des mises à jour logicielles, sélectionnez la nouvelle option **No deployment package** (Aucun package de déploiement).

**Problèmes connus**

- Une icône correspondant à une mise à jour déployée avec ce paramètre s'affiche avec une croix rouge, comme si la mise à jour n'était pas valide. Pour plus d'informations, consultez Icônes utilisées pour les mises à jour logicielles.
- Ce paramètre est intégré uniquement à l'Assistant Déploiement des mises à jour logicielles. Il n'est pas disponible pour les règles de déploiement automatique.

## Intégration de l'Outil de personnalisation Office au programme d'installation d'Office 365

L'outil de personnalisation Office est désormais intégré au programme d'installation d'Office 365 dans la console Configuration Manager. Lorsque vous créez un déploiement pour Office 365, vous pouvez désormais configurer dynamiquement les derniers paramètres de gestion Office. L'outil de personnalisation Office est mis à jour en même temps que les nouvelles builds d'Office 365. Vous pouvez désormais profiter des nouveaux paramètres de gestion d'Office 365 dès leur publication.

**Prérequis**

- L'ordinateur qui exécute la console Configuration Manager nécessite un accès Internet via le port HTTPS 443. L'Assistant Installation du client Office 365 utilise une API de navigateur web Windows standard pour ouvrir https://config.office.com. Si un serveur proxy Internet est utilisé, l'utilisateur doit pouvoir accéder à cette URL.

**Essayez !**

Essayez d'effectuer les tâches. Envoyez-nous ensuite des commentaires pour nous indiquer comment cela a fonctionné.

1. Dans la console Configuration Manager, accédez à l'espace de travail **Bibliothèque de logiciels**, puis sélectionnez le nœud **Gestion des clients Office 365**.
2. Dans le tableau de bord, cliquez sur la vignette **Programme d'installation d'Office 365** pour lancer l'Assistant Installation du client Office 365. Pour plus d'informations, consultez Déployer des applications Office 365.
3. Dans la page **Paramètres Office**, cliquez sur **Go To Office Web Page** (Accéder à la page web d'Office). Utilisez l'outil de personnalisation en ligne d'Office pour spécifier les paramètres de ce déploiement.
4. Lorsque vous avez terminé, cliquez sur **Envoyer** dans le coin supérieur droit. Terminez l'Assistant Installation du client Office 365.

## Améliorations apportées à la passerelle de gestion cloud

Dans cette version, les améliorations suivantes ont été apportées à la passerelle de gestion cloud :

**Ligne de commande de démarrage du client simplifiée**

Lorsque vous installez le client Configuration Manager via une passerelle de gestion cloud, le nombre de propriétés de ligne de commande nécessaires est désormais réduit. Lorsque vous vous préparez à la cogestion,

consultez Ligne de commande pour installer un client Configuration Manager pour obtenir des informations détaillées sur l'un des exemples de ce scénario.

Les propriétés de ligne de commande suivantes sont nécessaires pour tous les scénarios :

- CCMHOSTNAME
- SMSSITECODE

Les propriétés suivantes sont nécessaires lorsque vous utilisez Azure AD pour l'authentification client, au lieu de certificats d'authentification client PKI :

- AADCLIENTAPPID
- AADRESOURCEURI

La propriété suivante est nécessaire si le client doit revenir à l'intranet :

- SMSMP

L'exemple suivant comprend toutes les propriétés mentionnées ci-dessus :

```
ccmsetup.exe CCMHOSTNAME=CONTOSO.CLOUDAPP.NET/CCM_Proxy_MutualAuth/72186325152220500 SMSSiteCode=ABC
AADCLIENTAPPID=7506ee10-f7ec-415a-b415-cd3d58790d97 AADRESOURCEURI=https://contososerver
SMSMP=https://mp1.contoso.com
```

Pour plus d'informations, consultez Propriétés de l'installation du client.

**Télécharger du contenu à partir d'une passerelle de gestion cloud**

Auparavant, vous deviez déployer un point de distribution cloud et une passerelle de gestion cloud en leur attribuant un rôle distinct. Dans cette version, une passerelle de gestion cloud peut également distribuer du contenu Office aux clients. Cette fonctionnalité réduit le nombre de certificats nécessaires, ainsi que les coûts associés aux machines virtuelles Azure. Pour activer cette fonctionnalité, activez la nouvelle option **Allow CMG to function as a cloud distribution point and serve content from Azure storage** (Autoriser la passerelle de gestion cloud à fonctionner comme un point de distribution cloud et à distribuer du contenu à partir du stockage Azure) sous l'onglet **Paramètres** des propriétés de la passerelle de gestion cloud.

**Les certificat racines approuvés ne sont plus nécessaires avec Azure AD**

Lorsque vous créez une passerelle de gestion cloud, il n'est plus nécessaire de fournir un certificat racine approuvé dans la page Paramètres. Ce certificat n'est pas nécessaire lorsque vous utilisez Azure Active Directory (Azure AD) pour l'authentification client, mais il était auparavant nécessaire dans l'Assistant.

> **IMPORTANT**
> Si vous utilisez des certificats d'authentification client PKI, vous devez continuer d'ajouter un certificat racine approuvé pour la passerelle de gestion cloud.

## Amélioration des communications clientes sécurisées

Cette version améliore encore davantage les communications clientes sécurisées en supprimant les dépendances supplémentaires du compte d'accès réseau. Lorsque vous activez la nouvelle option de site **Utiliser les certificats générés par Configuration Manager pour les systèmes de site HTTP**, les scénarios suivants ne nécessitent pas de compte d'accès réseau pour télécharger le contenu à partir d'un point de distribution :

- Séquences de tâches exécutées à partir d'un support de démarrage ou d'un environnement PXE
- Séquence de tâches exécutées à partir du Centre logiciel

Ces séquences de tâches conviennent aux déploiements de système d'exploitation et aux déploiements personnalisés. Elles sont également prises en charge par les ordinateurs de groupe de travail.

## Améliorations apportées à l'infrastructure du Centre logiciel

Les rôles du catalogue d'applications ne sont plus nécessaires pour afficher les applications accessibles aux utilisateurs dans le Centre logiciel. Cette modification permet d'alléger l'infrastructure de serveur nécessaire pour fournir des applications aux utilisateurs. Le Centre logiciel s'appuie désormais sur le point de gestion pour obtenir ces informations, ce qui permet une meilleure mise à l'échelle des grands environnements par l'attribution de groupes de limites.

**Essayez !**

Essayez d'effectuer les tâches. Envoyez-nous ensuite des commentaires pour nous indiquer comment cela a fonctionné.

1. Supprimez tous les rôles de catalogue d'applications présents sur le site. Ces rôles incluent le point de service web du catalogue d'applications et le point de site web du catalogue d'applications.
2. Déployez une application en la rendant accessible à un regroupement d'utilisateurs.
3. Utilisez le Centre logiciel en tant qu'utilisateur ciblé pour parcourir, demander et installer l'application.

**Problème connu**

- Si vous utilisez un client joint à Azure Active Directory avec cette fonctionnalité, ne configurez pas le site sur **Utiliser les certificats générés par Configuration Manager pour les systèmes de site HTTP**. Il existe actuellement un conflit avec cette fonctionnalité. Pour plus d'informations sur ce paramètre, consultez Amélioration des communications clientes sécurisées.

## Provisionner les packages d'application Windows pour tous les utilisateurs sur un appareil

Vous pouvez désormais provisionner une application avec un package d'application Windows pour tous les utilisateurs d'un appareil. Un exemple courant de ce scénario est le provisionnement d'une application telle que « Minecraft : Education Edition » à partir de Microsoft Store pour Entreprises et Éducation, pour tous les appareils utilisés par les élèves d'une école. Auparavant, Configuration Manager ne prenait en charge l'installation de ces applications que pour un seul utilisateur. Quand il se connectait à un nouvel appareil, l'élève devait attendre pour accéder à une application. À présent que l'application est provisionnée pour tous les utilisateurs d'un appareil, ceux-ci peuvent l'utiliser plus rapidement.

> **IMPORTANT**
> Sachez que l'installation, le provisionnement et la mise à jour de plusieurs versions d'un même package d'application Windows sur un appareil peut entraîner des résultats inattendus. De tels résultats peuvent être obtenus lorsque vous utilisez Configuration Manager pour provisionner l'application, et que vous permettez aux utilisateurs de mettre à jour l'application à partir de Microsoft Store. Pour plus d'informations, consultez les instructions de la section Étapes suivantes pour gérer les applications à partir du Microsoft Store pour Entreprises.

Lorsque vous provisionnez une application sous licence hors connexion, Configuration Manager ne permet pas à Windows de la mettre automatiquement à jour à partir de Microsoft Store.

**Essayez !**

Essayez d'effectuer les tâches. Envoyez-nous ensuite des commentaires pour nous indiquer comment cela a fonctionné.

1. Créez une application. Cette application doit provenir d'un package d'application Windows ou être une application sous licence hors connexion que vous avez synchronisée à partir de Microsoft Store pour Entreprises et Éducation.

2. Dans la page **Informations générales** de l'Assistant Création d'une application, activez l'option **Provision**

**this application for all users on the device** (Provisionner cette application pour tous les utilisateurs de l'appareil).

> **TIP**
> Si vous modifiez une application existante, ce paramètre se trouve sous l'onglet **Expérience utilisateur** des propriétés de l'application.

3. Déployez l'application sur un regroupement d'appareils.
4. Connectez-vous à un appareil ciblé avec différents comptes d'utilisateurs, puis lancez l'application.

> **NOTE**
> Si vous devez désinstaller une application provisionnée sur des appareils auxquels les utilisateurs se sont déjà connectés, vous devez créer deux déploiements de désinstallation. Pour le premier déploiement de désinstallation, ciblez le regroupement d'appareils qui contient les appareils en question. Pour le deuxième déploiement, ciblez le regroupement d'utilisateurs qui contient les utilisateurs déjà connectés aux appareils sur lesquels l'application est provisionnée. Lorsque vous désinstallez une application provisionnée d'un appareil, Windows ne la désinstalle pas pour les utilisateurs.

## Améliorations apportées au tableau de bord Surface

Dans cette version, les améliorations suivantes ont été apportées au tableau de bord Surface :

- Le tableau de bord Surface affiche désormais la liste des appareils appropriés quand les sections de graphe sont sélectionnées.
  - En cliquant sur la vignette **Pourcentage d'appareils Surface**, vous affichez la liste des appareils Surface.
  - En cliquant sur une barre de la vignette **Top cinq des versions de microprogramme**, vous affichez la liste des appareils Surface avec la version de leur microprogramme.
- Lorsque vous affichez ces listes d'appareils dans le tableau de bord Surface, vous pouvez cliquer avec le bouton droit sur l'un des appareils et effectuer des actions courantes.

## Révision de l'unité par défaut pour l'inventaire matériel

Dans Configuration Manager version 1710, l'unité par défaut utilisée dans de nombreuses vues de rapports était passée des mégaoctets (Mo) aux gigaoctets (Go). En raison des améliorations apportées à l'inventaire matériel au niveau des valeurs d'entiers longs, et en vue de répondre à la demande des utilisateurs, nous sommes repassé aux mégaoctets pour l'unité par défaut.

## Étapes suivantes

Pour obtenir des informations complémentaires sur l'installation ou la mise à jour de l'édition Technical Preview, consultez Technical Preview pour System Center Configuration Manager.

# Fonctionnalités de la version Technical Preview 1805 de System Center Configuration Manager

26/06/2018 • 42 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Technical Preview)*

Cet article présente les fonctionnalités disponibles dans Configuration Manager Technical Preview version 1805. Vous pouvez installer cette version pour mettre à jour et ajouter de nouvelles fonctionnalités au site de votre préversion technique.

Consultez l'article Technical Preview avant d'installer cette mise à jour. Cet article vous permet de vous familiariser avec les limitations et les conditions générales liées à l'utilisation d'une version Technical Preview, et explique comment effectuer une mise à jour d'une version vers une autre et comment envoyer des commentaires.

**Vous trouverez ci-dessous les nouvelles fonctionnalités propres à cette version.**

## Créer un déploiement en plusieurs phases configurées manuellement pour une séquence de tâches

Il est désormais possible de créer un déploiement par phases configurées manuellement pour une séquence de tâches. Vous pouvez ajouter jusqu'à 10 phases supplémentaires sous l'onglet **Phases** de l'Assistant Création d'un déploiement par phases.

**Essayez !**

Suivez les instructions pour créer un déploiement en plusieurs phases que vous configurez manuellement. Envoyez-nous vos commentaires pour nous indiquer comment cela a fonctionné.

1. Dans l'espace de travail **Bibliothèque de logiciels**, développez **Systèmes d'exploitation**, puis sélectionnez **Séquences de tâches**.
2. Cliquez avec le bouton droit sur une séquence de tâches et sélectionnez **Créer un déploiement par phases**.
3. Sous l'onglet **Général**, donnez un nom et une description (facultative) au déploiement par phases, puis sélectionnez **Configurer manuellement toutes les phases**.
4. Sous l'onglet **Phases**, cliquez sur **Ajouter**.
5. Spécifiez un **nom** pour la phase, puis accédez au **Regroupement de phases** cible.
6. Sous l'onglet **Paramètres de phase**, choisissez une option pour chacun des paramètres de planification, puis sélectionnez **Suivant** quand vous avez terminé.
   - Critères de réussite de la phase précédente (cette option est désactivée pour la première phase).
     - **Pourcentage de réussite du déploiement** : spécifiez le pourcentage d'appareils qui exécutent le déploiement conformément aux critères de réussite de la phase précédente.
   - Conditions pour commencer cette phase de déploiement après la réussite de la phase précédente
     - **Commencer automatiquement cette phase après une période de report (en jours)** : choisissez le nombre de jours à attendre avant de passer à la phase suivante après la réussite de la

phase précédente.

    - **Commencer manuellement le déploiement de la deuxième phase** : vous ne devez pas commencer cette phase automatiquement après la réussite de la précédente.
- Dès qu'un appareil est ciblé, installer le logiciel
    - **Dès que possible** : l'échéance d'installation sur l'appareil correspond au moment où celui-ci est ciblé.
    - **Échéance (par rapport à la durée pendant laquelle l'appareil est ciblé)** : définit l'échéance d'installation sur un certain nombre de jours après le ciblage de l'appareil.

7. Exécutez l'Assistant Paramètres de phase.
8. Sous l'onglet **Phases** de l'Assistant Création d'un déploiement par phases, vous pouvez maintenant ajouter, supprimer, réorganiser ou modifier les phases du déploiement.
9. Exécutez l'Assistant Création d'un déploiement par phases.

## Prise en charge du point de distribution cloud pour Azure Resource Manager

Lors de la création d'une instance de point de distribution cloud, l'Assistant offre maintenant la possibilité de créer un **déploiement Azure Resource Manager**. Azure Resource Manager est une plateforme moderne permettant de gérer l'ensemble des ressources de la solution comme une seule entité, nommée groupe de ressources. Lors du déploiement d'un point de distribution cloud avec Azure Resource Manager, le site utilise Azure Active Directory (Azure AD) pour authentifier et créer les ressources cloud nécessaires. Le certificat de gestion Azure classique n'est pas nécessaire pour ce déploiement modernisé.

L'Assistant Point de distribution cloud propose toujours l'option de **déploiement de service classique** à l'aide d'un certificat de gestion Azure. Pour simplifier le déploiement et la gestion des ressources, nous vous recommandons d'utiliser le modèle de déploiement Azure Resource Manager pour tous les points de distribution cloud. Si possible, redéployez les points de distribution cloud existants avec Resource Manager.

Configuration Manager ne migre pas les points de distribution cloud classiques existants vers le modèle de déploiement Azure Resource Manager. Créez de nouveaux points de distribution cloud à l'aide de déploiements Azure Resource Manager, puis supprimez les points de distribution cloud classiques.

> **IMPORTANT**
> Cette fonctionnalité ne permet pas la prise en charge des fournisseurs de services cloud Azure. Les déploiements de points de distribution cloud avec Azure Resource Manager continuent d'utiliser le service cloud classique, que ne prend pas en charge le fournisseur de services cloud. Pour plus d'informations, consultez les services Azure disponibles auprès du fournisseur de services cloud Azure.

**Prérequis**

- Intégration à Azure AD. Découverte d'utilisateurs Azure AD non requise.
- Mêmes exigences pour le point de distribution cloud, à l'exception du certificat de gestion Azure.

**Essayez !**

Essayez d'effectuer les tâches. Envoyez-nous ensuite des commentaires pour nous indiquer comment cela a fonctionné.

1. Dans l'espace de travail **Administration** de la console Configuration Manager, développez **Services cloud**, puis sélectionnez **Points de distribution cloud**. Dans le ruban, cliquez sur **Créer un point de distribution cloud**.

2. Sur la page **Général**, sélectionnez **Déploiement Azure Resource Manager**. Cliquez sur **Se connecter** pour vous authentifier avec un compte Administrateur d'abonnement Azure. L'Assistant remplit automatiquement les champs restants à partir des informations de l'abonnement Azure AD stockées dans les prérequis de l'intégration. Si vous possédez plusieurs abonnements, sélectionnez celui que vous souhaitez utiliser. Cliquez sur **Suivant**.

3. Dans la page **Paramètres**, fournissez le **fichier de certificat** PKI de serveur. Ce certificat définit le **FQDN du service** du point de distribution cloud utilisé par Azure. Sélectionnez la **Région**, puis une option de groupe de ressources : soit **Nouveau**, soit **Existant**. Entrez le nom du nouveau groupe de ressources, ou sélectionnez un groupe de ressources existant dans la liste déroulante.

4. Effectuez toutes les étapes de l'Assistant.

> **NOTE**
> Pour l'application serveur Azure AD sélectionnée, Azure affecte l'autorisation **contributeur** de l'abonnement.

Suivez la progression du déploiement de service avec **cloudmgr.log** sur le point de connexion du service.

## Agir en fonction des insights de gestion

Certains insights de gestion permettent maintenant d'entreprendre des actions. En fonction de la règle, cette action montre l'un des comportements suivants :

- Dans la console, accède automatiquement au nœud dans lequel vous pouvez entreprendre des actions. Par exemple, si les insights de gestion recommandent de changer un paramètre client, le fait d'entreprendre une action vous redirige vers le nœud Paramètres du client. Vous pouvez entreprendre d'autres actions en modifiant l'objet de paramètres clients par défaut ou personnalisé.
- Accède à une vue filtrée selon une requête. Par exemple, le fait d'entreprendre une action avec la règle de regroupements vides montre simplement la liste des collections. De là, vous pouvez entreprendre d'autres actions, comme supprimer un regroupement ou modifier ses règles d'adhésion.

Les règles d'insights de gestion suivantes sont associées à des actions de cette version :

- Sécurité
  - Versions de client logiciel anti-programme malveillant non prises en charge
- Centre logiciel
  - Utiliser la nouvelle version du Centre logiciel
- Applications
  - Applications sans déploiements
- Gestion simplifiée
  - Versions de client non-CB
- Regroupements
  - Regroupements vides
- Services cloud
  - Mettre à jour les clients avec la dernière version de Windows 10

## Transférer la charge de travail de configuration des appareils vers Intune avec la cogestion

Vous pouvez désormais transférer la charge de travail de configuration des appareils de Configuration Manager vers Intune après avoir activé la cogestion. Le transfert de cette charge de travail vous permet d'utiliser Intune pour

déployer des stratégies MDM, tout en continuant à utiliser Configuration Manager pour déployer les applications.

Pour basculer cette charge de travail, accédez à la page de propriétés de cogestion et déplacez le curseur actuellement sur Configuration Manager vers **Pilote** ou **Tout**. Pour plus d'informations, consultez Cogestion pour les appareils Windows 10.

> **NOTE**
> Le fait de déplacer cette charge de travail déplace également les charges de travail **Accès aux ressources** et **Endpoint Protection**, qui constituent un sous-ensemble de la charge de travail de configuration des appareils.

Quand vous transférez cette charge de travail, vous pouvez encore déployer des paramètres Configuration Manager sur des appareils cogérés, même si Intune représente l'autorité de configuration des appareils. Cette exception peut être utilisée pour configurer les paramètres qui sont exigés par votre entreprise, mais qui ne sont pas encore disponibles dans Intune. Spécifiez cette exception sur une base de référence de configuration Configuration Manager. Activez l'option **Toujours appliquer cette base de référence, même aux clients cogérés** lors de la création de la base de référence, ou sous l'onglet **Général** des propriétés de la base de référence existante.

## Configurer les points de distribution pour utiliser le contrôle de surcharge du réseau

La fonctionnalité LEDBAT de Windows Server permet de gérer les transferts réseau d'arrière-plan. Pour les points de distribution qui exécutent des versions prises en charge de Windows Server, vous pouvez activer une option permettant d'ajuster le trafic réseau. Les clients utilisent uniquement la bande passante réseau lorsqu'elle est disponible.

Pour plus d'informations sur la fonctionnalité LEDBAT de Windows, consultez le billet de blog New transport advancements.

**Prérequis**

- Un point de distribution sur Windows Server, version 1709
- Un appareil client qui exécute au minimum Windows 10 version 1607

**Essayez !**

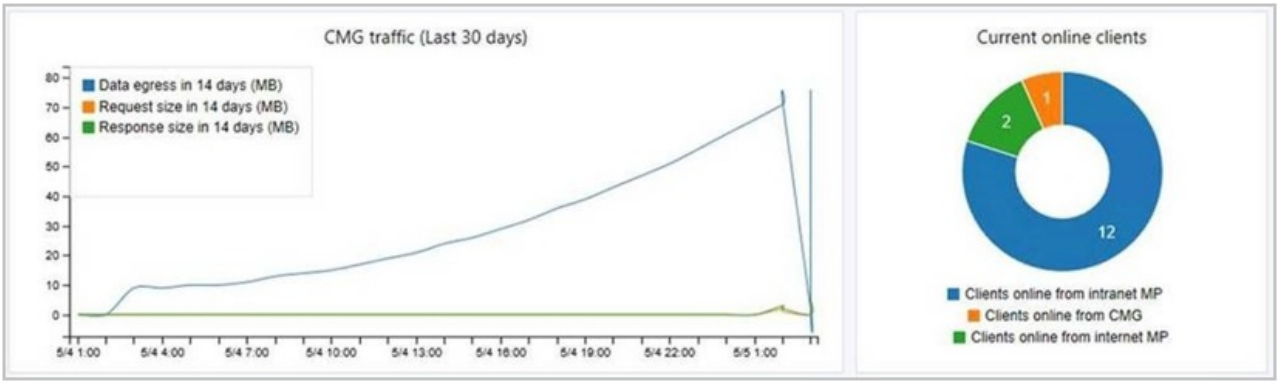
Essayez d'effectuer les tâches. Envoyez-nous ensuite des commentaires pour nous indiquer comment cela a fonctionné.

1. Dans la console de Configuration Manager, accédez à l'espace de travail **Administration**. Sélectionnez le nœud **Points de distribution**. Sélectionnez le point de distribution cible, puis cliquez sur **Propriétés** dans le ruban.
2. Sous l'onglet **Général**, activez l'option **Ajuster la vitesse de téléchargement pour utiliser la bande passante non utilisée (Windows LEDBAT)**.

## Tableau de bord de gestion cloud

Le nouveau **tableau de bord de gestion cloud** fournit une vue centralisée de l'utilisation de la passerelle de gestion cloud. Lorsque le site est intégré à Azure AD, il affiche également les données sur les utilisateurs cloud et les appareils.

La capture d'écran suivante montre une partie du tableau de bord de gestion cloud, comprenant deux des vignettes disponibles :




Cette fonctionnalité inclut également **l'analyseur de connexion de la passerelle de gestion cloud** pour la vérification en temps réel dans le cadre de la résolution des problèmes. L'utilitaire de la console vérifie l'état actuel du service, ainsi que le canal de communication qui passe par le point de connexion de la passerelle de gestion cloud vers les points de gestion qui autorisent le trafic de la passerelle.

**Prérequis**

- Une passerelle de gestion cloud active utilisée par les clients Internet
- Intégrer le site aux services Azure pour la gestion cloud

**Essayez !**

Essayez d'effectuer les tâches. Envoyez-nous ensuite des commentaires pour nous indiquer comment cela a fonctionné.

##### Tableau de bord de gestion cloud

Dans la console Configuration Manager, accédez à l'espace de travail **Surveillance**. Sélectionnez le nœud **Gestion cloud** et affichez les vignettes du tableau de bord.

##### Analyseur de connexion de la passerelle de gestion cloud

1. Dans la console de Configuration Manager, accédez à l'espace de travail **Administration**. Développez **Services cloud** et sélectionnez **Passerelle de gestion cloud**.
2. Sélectionnez l'instance cible de la passerelle de gestion cloud, puis sélectionnez **Analyseur de connexion** dans le ruban.
3. Dans la fenêtre Analyseur de connexion de la passerelle de gestion cloud, sélectionnez l'une des options suivantes pour l'authentification auprès du service :
   a. **Utilisateur AD Azure** : cette option permet de simuler la communication comme avec une identité d'utilisateur cloud connectée à un appareil Windows 10 joint à Azure AD. Cliquez sur **Connexion** pour entrer les informations d'identification du compte d'utilisateur Azure AD de manière sécurisée.
   b. **Certificat client** : cette option permet de simuler la communication comme avec un client Configuration Manager disposant d'un certificat d'authentification client.
4. Cliquez sur **Démarrer** pour démarrer l'analyse. Les résultats sont affichés dans la fenêtre de l'analyseur. Sélectionnez une entrée pour afficher plus de détails dans le champ Description.

## CMPivot

Configuration Manager met à disposition un grand magasin de données d'appareils centralisé, que les clients utilisent pour générer des rapports. Toutefois, ces données peuvent être obsolètes.

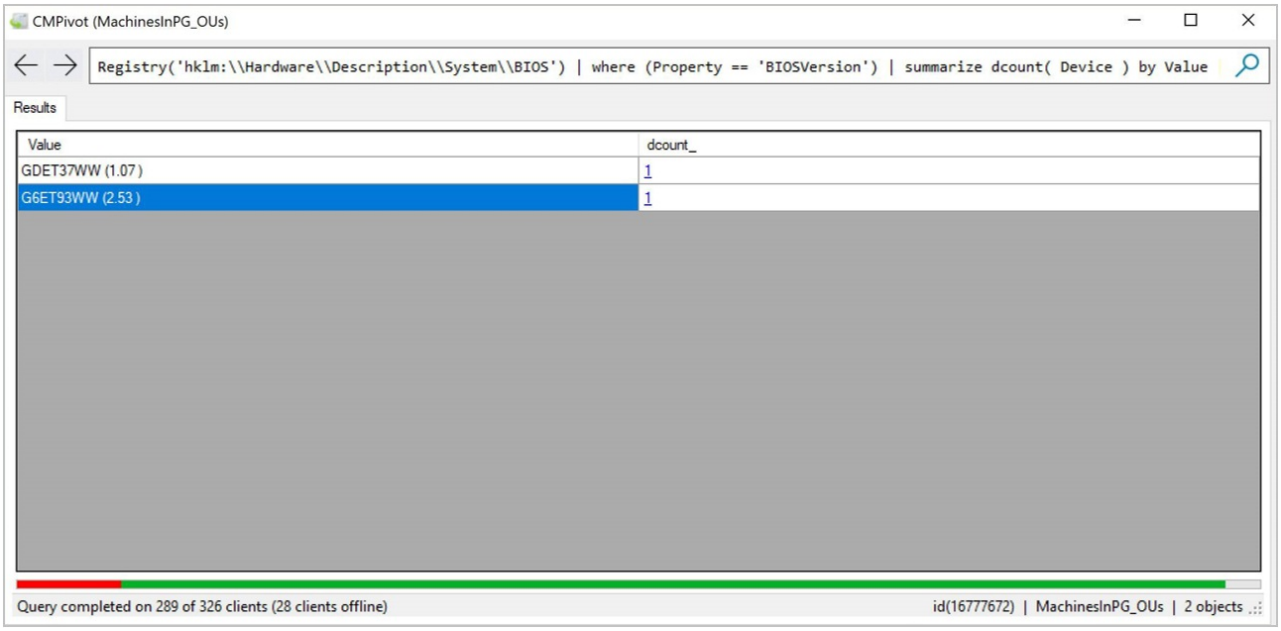
CMPivot est un nouvel utilitaire de console qui donne accès à l'état en temps réel des appareils de votre environnement. Il exécute immédiatement une requête sur tous les appareils actuellement connectés du regroupement cible, et retourne les résultats. Vous pouvez ensuite filtrer et regrouper ces données dans l'outil. En fournissant les données en temps réel des clients en ligne, vous pouvez répondre plus rapidement aux questions

métier, résoudre les problèmes et corriger les incidents de sécurité.

Par exemple, si vous souhaitez limiter les vulnérabilités d'exécution spéculative côté canal, l'une des exigences est de mettre à jour le BIOS système. Vous pouvez utiliser CMPivot pour interroger rapidement les informations du BIOS système et rechercher les clients non conformes.

Dans cette capture d'écran, CMPivot affiche deux versions distinctes du BIOS avec chacune un appareil. Vous pouvez utiliser cet exemple de requête lorsque vous essayez CMPivot :

```
Registry('hklm:\\Hardware\\Description\\System\\BIOS') | where (Property == 'BIOSVersion') | summarize dcount(
Device ) by Value
```




Vous pouvez cliquer sur le nombre d'appareils pour explorer les appareils. Lorsque vous affichez des appareils dans CMPivot, vous pouvez cliquer sur l'un d'eux, puis sélectionner les actions de notification clientes suivantes :

- Exécuter un script
- Contrôle à distance
- Explorateur de ressources

Quand vous cliquez avec le bouton droit sur un appareil, vous pouvez également faire pivoter la vue de l'appareil pour afficher l'un des attributs suivants :

- Commandes de démarrage automatique
- Produits installés
- Processus
- Services
- Utilisateurs
- Connexions actives
- Mises à jour manquantes

**Prérequis**

- Les clients cibles doivent être mis à jour vers la dernière version.
- L'administrateur Configuration Manager a besoin d'autorisations pour exécuter des scripts. Pour plus d'informations, consultez Créer des rôles de sécurité pour les scripts.

**Essayez !**

Essayez d'effectuer les tâches. Envoyez-nous ensuite des commentaires pour nous indiquer comment cela a fonctionné.

1. Dans la console Configuration Manager, accédez à l'espace de travail **Actifs et conformité**, puis sélectionnez **Regroupements d'appareils**. Sélectionnez un regroupement cible, puis cliquez sur **Démarrer CMPivot** dans le ruban pour lancer l'outil.

2. L'interface fournit davantage d'informations sur l'utilisation de l'outil.

   - Vous pouvez entrer manuellement des chaînes de requête en haut de la page, ou cliquer sur les liens de la documentation intégrée.
   - Cliquez sur l'une des **Entités** pour l'ajouter à la chaîne de requête.
   - Les liens concernant les **opérateurs de table**, les **fonctions d'agrégation** et les **fonctions scalaires** ouvrent une documentation de référence de langage dans le navigateur web. CMPivot utilise le même langage de requête que Azure Log Analytics.

## Amélioration des communications clientes sécurisées

L'utilisation de la communication HTTPS est recommandée pour tous les chemins de communication Configuration Manager, mais peut se révéler difficile pour certains clients en raison des frais liés à la gestion des certificats PKI. L'intégration à Azure Active Directory (Azure AD) permet d'éviter une partie de ces exigences de certificat.

Cette version comprend des améliorations concernant la façon dont les clients communiquent avec les systèmes de site. Ces améliorations avaient deux principaux objectifs :

- Sécuriser les communications clientes sans avoir besoin de certificats d'authentification serveur PKI
- Permettre aux clients d'accéder de manière sécurisée au contenu des points de distribution sans avoir besoin d'un compte d'accès réseau

> **NOTE**
> L'utilisation des certificats PKI est toujours possible pour les clients qui le souhaitent.

### Scénarios

Les scénarios suivants bénéficient de ces améliorations :

#### Scénario 1 : Client vers point de gestion

Les appareils joints à Azure AD peuvent communiquer via une passerelle de gestion cloud avec un point de gestion configuré pour HTTP. Le serveur de site génère un certificat pour le point de gestion afin de lui permettre de communiquer via un canal sécurisé.

> **NOTE**
> Ce comportement est différent de celui trouvé dans Configuration Manager Current Branch version 1802, qui nécessite un point de gestion HTTPS pour ce scénario. Pour plus d'informations, consultez Activer le point de gestion pour HTTPS.

#### Scénario 2 : Client vers point de distribution

Un groupe de travail ou un client joint à Azure AD peut télécharger du contenu via un canal sécurisé à partir d'un point de distribution configuré pour HTTP.

#### Scénario 3 : Identité des appareils Azure AD

Un appareil joint à Azure AD ou un appareil Azure AD hybride peuvent communiquer de manière sécurisée avec leur site attribué, sans qu'un utilisateur Azure AD ne soit connecté. L'identité d'appareil cloud est désormais suffisante pour s'authentifier auprès du point de gestion et de la passerelle de gestion cloud.

### Prérequis

- Un point de gestion configuré pour les connexions clientes HTTP. Définissez cette option sous l'onglet **Général** des propriétés du rôle de système de site.
- Un point de distribution configuré pour les connexions clientes HTTP. Définissez cette option sous l'onglet **Général** des propriétés du rôle de système de site. N'activez pas l'option **Autoriser les clients à se connecter anonymement**.
- Une passerelle de gestion cloud
- Intégrer le site à Azure AD pour la gestion cloud
    - Si vous avez déjà effectué cette intégration pour votre site, vous devez mettre à jour l'application Azure AD. Dans la console Configuration Manager, accédez à l'espace de travail **Administration**, développez **Services cloud**, puis sélectionnez **Locataires Azure Active Directory**. Sélectionnez le locataire Azure AD, sélectionnez l'application web dans le volet **Applications**, puis cliquez sur **Mettre à jour les paramètres d'application** dans le ruban.
- Un client exécutant Windows 10 version 1803 et joint à Azure AD (cette exigence concerne seulement le scénario 3).

**Essayez !**

Essayez d'effectuer les tâches. Envoyez-nous ensuite des commentaires pour nous indiquer comment cela a fonctionné.

1. Dans la console Configuration Manager, accédez à l'espace de travail **Administration**, développez **Configuration du site**, puis sélectionnez **Sites**. Sélectionnez le site, puis cliquez sur **Propriétés** dans le ruban.
2. Passez à l'onglet **Communication de l'ordinateur client**. Sélectionnez l'option **HTTPS ou HTTP**, puis activez la nouvelle option **Use Configuration Manager-generated certificates for HTTP site systems** (Utiliser des certificats générés par Configuration Manager pour les systèmes de site HTTP).

Consultez l'ancienne liste des scénarios pour valider.

> **TIP**
> Dans cette version, un délai maximal de 30 minutes est nécessaire pour que le point de gestion reçoive puis configure le nouveau certificat du site.

Vous pouvez voir ces certificats dans la console Configuration Manager. Accédez à l'espace de travail **Administration**, développez **Sécurité**, puis sélectionnez le nœud **Certificats**. Recherchez le certificat racine **Émission de SMS**, ainsi que les certificats de rôle serveur de site émis par ce certificat racine.

**Problèmes connus**

- L'utilisateur ne voit pas les applications disponibles dans le Centre logiciel.
- Les scénarios de déploiement de système d'exploitation nécessitent toujours un compte d'accès réseau.
- Le fait d'activer puis de désactiver rapidement et à plusieurs reprises l'option **Use Configuration Manager-generated certificates for HTTP site systems** (Utiliser des certificats générés par Configuration Manager pour les systèmes de site HTTP) peut empêcher la liaison du certificat aux rôles de système de site. Aucun certificat émis par le certificat Émission de SMS n'est lié à un site web dans Windows Server Internet Information Services (IIS). Pour contourner ce problème, supprimez tous les certificats émis par le certificat Émission de SMS dans le magasin de certificats **SMS** de Windows, puis redémarrez le service smsexec.

## Améliorations concernant la prise en charge des mises à jour des

## logiciels tiers

Nous avons pris en compte vos commentaires UserVoice concernant la prise en charge des mises à jour des logiciels tiers et avons amélioré l'intégration à l'éditeur de mise à jour System Center (SCUP ). Configuration Manager Technical Preview version 1803 permet désormais de lire le certificat à partir de WSUS pour les mises à jour tierces, puis de déployer ce certificat sur des clients. Toutefois, vous devez encore utiliser l'outil SCUP pour créer et gérer le certificat pour la signature des mises à jour de logiciels tiers.

Dans cette version, vous pouvez paramétrer le site Configuration Manager pour qu'il configure automatiquement le certificat. Le site communique avec WSUS pour générer un certificat à cet effet. Configuration Manager continue alors à déployer ce certificat sur les clients. Cette nouvelle fonctionnalité évite d'avoir à utiliser l'outil SCUP pour créer et gérer le certificat.

Pour plus d'informations sur l'utilisation générale de l'outil SCUP, consultez Éditeur de mise à jour System Center.

**Prérequis**

- Activez puis déployez le paramètre client **Activer les mises à jour de logiciels tiers** dans le groupe **Mises à jour logicielles**.
- Si WSUS se trouve sur un serveur autre que celui du point de mise à jour logicielle, vous devez effectuer l'une des actions suivantes sur le serveur WSUS distant :
  - Activez le service d'accès à distance au Registre dans Windows
    ou
  - Dans la clé de Registre `HKLM\Software\Microsoft\Update Services\Server\Setup`, créez un DWORD nommé **EnableSelfSignedCertificates** avec la valeur `1`.

**Essayez !**

Essayez d'effectuer les tâches. Envoyez-nous ensuite des commentaires pour nous indiquer comment cela a fonctionné.

1. Dans la console de Configuration Manager, accédez à l'espace de travail **Administration**. Développez **Configuration du site** et sélectionnez **Sites**. Sélectionnez le site de niveau supérieur, cliquez sur **Configurer les composants de site** dans le ruban, puis sélectionnez **Point de mise à jour logicielle**.

2. Passez l'onglet **Mises à jour tierces**. Sélectionnez l'option **Activer les mises à jour de logiciels tiers**, puis sélectionnez l'option **Configuration Manager automatically manages the certificate** (Configuration Manager gère automatiquement le certificat).

3. Suivez le flux de travail SCUP typique pour importer un catalogue de mise à jour de logiciels tiers, puis déployez les mises à jour sur les clients.

## Améliorations apportées à la séquence de tâches de mise à niveau sur place de Windows 10

Le modèle de séquence de tâches par défaut pour la mise à niveau sur place de Windows 10 comprend un nouveau groupe, ainsi que des actions qu'il est recommandé d'ajouter en cas d'échec de la mise à niveau. Ces actions facilitent la résolution des problèmes.

**Groupes de nouveau disponibles sous Exécuter des actions en cas d'échec**

- **Collecter les journaux** : pour collecter les journaux du client, ajoutez des étapes dans ce groupe.
  - L'une des pratiques courantes consiste à copier les fichiers journaux sur un partage réseau. Pour établir cette connexion, utilisez l'étape Se connecter à un dossier réseau.
  - Pour effectuer la copie, utilisez un script personnalisé ou un utilitaire en suivant l'étape Exécuter la ligne de commande ou Exécuter le script PowerShell.
  - Les fichiers à collecter peuvent inclure les journaux suivants :

`%_SMSTSLogPath%\*.log`

`%SystemDrive%\$Windows.~BT\Sources\Panther\setupact.log`

- Pour plus d'informations sur setupact.log et sur les autres journaux d'installation de Windows, consultez Journaux d'installation de Windows.
- Pour plus d'informations sur les journaux du client Configuration Manager, consultez Journaux du client Configuration Manager.
- Pour plus d'informations sur _SMSTSLogPath et sur d'autres variables utiles, consultez Variables intégrées de séquence de tâches.

- **Exécuter les outils de diagnostic** : pour exécuter d'autres outils de diagnostic, ajoutez des étapes dans ce groupe. Ces outils doivent être automatisés pour collecter des informations supplémentaires à partir du système, dès que possible après un échec.

  - Un exemple est l'outil Windows SetupDiag. Il s'agit d'un outil de diagnostic autonome que vous pouvez utiliser pour obtenir des informations détaillées sur la raison de l'échec d'une mise à niveau Windows 10.
    - Dans Configuration Manager, créez un package pour l'outil.
    - Ajoutez l'étape Exécuter la ligne de commande au groupe de votre séquence de tâches. Utilisez l'option **Package** pour référencer l'outil. La chaîne suivante est un exemple de **ligne de commande** :
      `SetupDiag.exe /Output:"%_SMSTSLogPath%\SetupDiagResults.log" /Mode:Online`

## CMTrace installé avec le client

Désormais, l'outil d'affichage des journaux CMTrace est automatiquement installé avec le client Configuration Manager. Il est ajouté au répertoire d'installation du client, qui est par défaut `%WinDir%\ccm\cmtrace.exe`.

> **NOTE**
> CMTrace *n'est pas* automatiquement inscrit auprès de Windows pour ouvrir l'extension de fichier .log.

## Améliorations apportées à la console Configuration Manager

Nous avons apporté les améliorations suivantes à la console Configuration Manager :

- Les listes d'appareils sous Ressources et conformité, Appareils, affichent désormais l'utilisateur actuellement connecté. Cette valeur est synchronisée avec l'état du client. Elle est supprimée lorsque l'utilisateur se déconnecte. Si aucun utilisateur n'est connecté, la valeur est vide.

**Problèmes connus**

La valeur de l'utilisateur actuellement connecté est vide dans le nœud Appareils ou lorsque vous affichez une liste d'appareils sous le nœud Regroupements d'appareils. Pour contourner ce problème, téléchargez ce script SQL. Exécutez sp_BgbUpdateLiveData.sql sur le serveur de bases de données de site, puis redémarrez les services smsexec et sms_notification_server sur le point de gestion.

## Améliorations apportées à la fonctionnalité Commentaires de la console

Dans cette version, les améliorations suivantes ont été apportées à la fonctionnalité Commentaires de la console Configuration Manager :

- Désormais, la boîte de dialogue Commentaires mémorise vos paramètres précédents, tels que les options sélectionnées et votre adresse de messagerie.

- Les commentaires hors connexion sont maintenant pris en charge. Enregistrez vos commentaires dans la

console, puis chargez-les vers Microsoft à partir d'un système connecté à Internet. Utilisez le nouvel outil de chargement des commentaires hors connexion qui se trouve ici : `cd.latest\SMSSETUP\Tools\UploadOfflineFeedback\UploadOfflineFeedback.exe`. Pour afficher les options de ligne de commande disponibles et nécessaires, exécutez l'outil avec l'option `--help`. Le système connecté a besoin d'accéder à **petrol.office.microsoft.com**.

**Problèmes connus**

Lorsque vous utilisez la commande **Envoyer un sourire** ou **Envoyer un smiley mécontent** à partir de la console sur un ordinateur connecté à Internet, le message suivant « Erreur lors de l'envoi des commentaires » peut s'afficher. Si vous cliquez sur **Plus de détails**, le texte suivant apparaît : `{"Message":""}`. Cette erreur est due à un problème connu au niveau de la réponse provenant du système de commentaires back-end. Vous pouvez ignorer cette erreur. Microsoft a bien reçu vos commentaires. (Si les détails affichent un autre message, utilisez l'option de commentaires hors connexion pour réessayer d'envoyer vos commentaires à une date ultérieure.)

## Améliorations apportées aux points de distribution compatibles PXE

Cette version comprend les améliorations suivantes lorsque vous utilisez l'option **Activer un répondeur PXE sans service de déploiement Windows** sur un point de distribution :

- Les règles du Pare-feu Windows sont automatiquement créées sur le point de distribution quand vous activez cette option.
- Améliorations apportées à la journalisation des composants

## Amélioration apportées à l'inventaire matériel pour les valeurs d'entiers longs

La version actuelle de l'inventaire matériel est limitée aux entiers supérieurs à 4 294 967 296 (2^32). Cette limite peut être atteinte pour les attributs, tels que les tailles de disque dur en octets. Le point de gestion ne traite pas les valeurs d'entiers supérieures à cette limite. De fait, aucune valeur n'est stockée dans la base de données. La nouvelle version prend désormais en charge les entiers de longueur 18 446 744 073 709 551 616 (2^64).

Pour les propriétés dont la valeur ne change pas, comme la taille totale du disque, vous pouvez ne pas voir immédiatement la valeur après la mise à niveau du site. La plupart des inventaires matériels se présentent sous la forme d'un état d'écart. Le client envoie uniquement les valeurs qui changent. Pour contourner ce comportement, ajoutez une autre propriété à la même classe. Avec cette action, le client met à jour toutes les propriétés de la classe qui ont changé.

## Améliorations apportées à la maintenance de WSUS

L'Assistant de nettoyage WSUS refuse désormais les mises à jour qui ont expiré ou qui ont été remplacées selon les règles de remplacement. Ces règles sont définies dans les propriétés de composant du point de mise à jour logicielle.

**Essayez !**

Essayez d'effectuer les tâches. Envoyez-nous ensuite des commentaires pour nous indiquer comment cela a fonctionné.

1. Dans la console de Configuration Manager, accédez à l'espace de travail **Administration**. Développez **Configuration du site** et sélectionnez **Sites**. Sélectionnez le site de niveau supérieur, cliquez sur **Configurer les composants de site** dans le ruban, puis sélectionnez **Point de mise à jour logicielle**.

2. Passez à l'onglet **Règles de remplacement**. Activez l'option **Exécutez l'Assistant de nettoyage WSUS**. Spécifiez le comportement de remplacement souhaité.

3. Examinez le fichier WSyncMgr.log.

## Améliorations apportées à la prise en charge des certificats CNG

À compter de cette version, utilisez les certificats CNG pour les rôles serveurs HTTPS suivants :

- Point d'enregistrement de certificat, y compris le serveur NDES avec le module de stratégie Configuration Manager

## Étapes suivantes

Pour obtenir des informations complémentaires sur l'installation ou la mise à jour de l'édition Technical Preview, consultez Technical Preview pour System Center Configuration Manager.

# Fonctionnalités de Technical Preview 1804 pour System Center Configuration Manager

26/06/2018 • 26 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Technical Preview)*

Cet article présente les fonctionnalités disponibles dans Technical Preview version 1804 pour Configuration Manager. Vous pouvez installer cette version pour mettre à jour et ajouter de nouvelles fonctionnalités au site de votre préversion technique.

Consultez l'article Technical Preview avant d'installer cette mise à jour. Cet article vous permet de vous familiariser avec les limitations et les conditions générales liées à l'utilisation d'une version Technical Preview, et explique comment effectuer une mise à jour d'une version vers une autre et comment envoyer des commentaires.

## Problèmes connus dans cette préversion technique

**Le lien pour télécharger les mises à jour ne fonctionne pas**

Si vous exécutez le programme d'installation à partir du support, la page initiale inclut un lien intitulé **Get the latest Configuration Manager updates** (Obtenir les dernières mises à jour de Configuration Manager), qui ne fonctionne pas dans cette version. Ce lien permet de télécharger les fichiers requis pour le programme d'installation.

**Solution de contournement**

Pour télécharger les fichiers requis pour le programme d'installation, exécutez l'Assistant Installation. Dans la page Téléchargements requis, utilisez l'option pour **télécharger les fichiers requis**.

**HTTPS ne peut pas être activé sur le point de service web du catalogue des applications**

Si HTTPS est activé sur le point de service web du catalogue des applications :

- Les applications déployées comme étant disponibles pour les utilisateurs ne s'affichent pas dans le Centre logiciel
- L'erreur suivante s'affiche dans awebsctl.log :

```
Call to HttpSendRequestSync failed for port 443 with status code 500, text: Internal Server Error
```

**Solution de contournement**

Reconfigurez le point de service web du catalogue des applications pour qu'il communique à l'aide de connexions HTTP.

**Vous trouverez ci-dessous les nouvelles fonctionnalités propres à cette version.**

## Configurer une bibliothèque de contenu à distance pour le serveur de site

Pour libérer de l'espace disque sur votre serveur de site principal, vous devez déplacer sa bibliothèque de contenu vers un autre emplacement de stockage. Vous pouvez déplacer la bibliothèque de contenu sur un autre disque du serveur de site, sur un serveur distinct ou sur des disques à tolérance de panne dans un réseau de zone de stockage (SAN). Nous recommandons l'utilisation d'un réseau SAN qui fournit un stockage élastique capable de croître ou de se réduire au fil du temps pour répondre à vos besoins en termes de contenu.

Cette bibliothèque de contenu à distance est un nouveau prérequis pour la haute disponibilité au niveau du rôle serveur de site.

> **NOTE**
> Cette action déplace uniquement la bibliothèque de contenu sur le serveur de site. Elle n'affecte pas l'emplacement de la bibliothèque de contenu sur les points de distribution.

**Prérequis**

- Le compte de l'ordinateur du serveur de site doit disposer d'autorisations en **lecture** et en **écriture** pour le chemin d'accès réseau vers lequel vous déplacez la bibliothèque de contenu. Aucun composant n'est installé sur le système à distance.

**Essayez !**

Essayez d'effectuer les tâches. Envoyez-nous ensuite des commentaires pour nous indiquer comment cela a fonctionné.

1. Dans la console de Configuration Manager, accédez à l'espace de travail **Administration**. Développez **Configuration du site** et sélectionnez **Sites**. Dans l'onglet **Résumé** en bas du volet d'informations, vous noterez l'apparition d'une nouvelle colonne pour la **Bibliothèque de contenu**.
2. Sur le ruban, cliquez sur **Gérer la bibliothèque de contenu**.
3. Sélectionnez **Sur un partage réseau** et entrez un chemin d'accès réseau valide. Ce chemin d'accès est l'emplacement vers lequel le site déplace la bibliothèque de contenu. Cliquez sur **OK**.
4. Notez la propriété **État** dans la colonne Bibliothèque de contenu dans le volet d'informations. Elle se met à jour pour afficher la progression du site en termes de déplacement de la bibliothèque de contenu. Lors de l'opération, le pourcentage de progression s'affiche. En cas d'état d'erreur, elle affiche l'erreur. Les erreurs courantes incluent `access denied` ou `disk full`. Lorsque l'opération est terminée, `OK` s'affiche. Consultez **distmgr.log** pour plus d'informations. Pour plus d'informations, consultez Journaux serveur du serveur de site et du système de site.

Si vous avez besoin redéplacer la bibliothèque de contenu vers le serveur de site, répétez ce processus, mais sélectionnez l'option **Local vers serveur de site**.

> **TIP**
> Pour déplacer le contenu vers un autre disque du serveur de site, utilisez l'outil **Transfert de bibliothèque de contenu**. Pour plus d'informations, consultez Kit de ressources Configuration Manager.

## Envoyer des commentaires à partir de la console Configuration Manager

Envoyer un sourire ! Vous pouvez maintenant communiquer directement avec l'équipe Configuration Manager sur vos expériences. L'envoi de commentaires est facile à partir de la console Configuration Manager. Nous voulons recevoir tous vos commentaires : les éloges, les problèmes et les suggestions.

**Essayez !**

Essayez d'effectuer les tâches. Envoyez-nous ensuite des **commentaires** pour nous indiquer comment cela a fonctionné.

1. Dans la console Configuration Manager, cliquez sur le bouton en forme de sourire dans l'angle supérieur droit au-dessus du ruban.

2. Sélectionnez l'une des options disponibles dans la liste déroulante :

   - **Envoyer un sourire** : vous avez beaucoup apprécié quelque chose ! Pour cette option, entrez des commentaires détaillés. Puis, incluez éventuellement une capture d'écran et votre adresse e-mail.
   - **Envoyer un smiley mécontent** : vous avez rencontré un problème dans la console ou quelque chose n'a pas fonctionné comme prévu. Pour cette option, entrez des informations détaillées sur le problème produit potentiel. Puis, incluez éventuellement une capture d'écran, votre adresse e-mail et les données de diagnostic.
   - **Envoyer une suggestion** : vous avez une idée pour modifier et améliorer Configuration Manager. Cette option ouvre notre site UserVoice dans votre navigateur web.

Ces commentaires sont envoyés directement à l'équipe produit Microsoft pour Configuration Manager. Bien que l'utilisation du concentrateur de commentaires de Windows 10 soit toujours prise en charge, nous vous encourageons à utiliser la fonction de commentaires dans la console.

Les informations anonymes suivantes sont toujours incluses avec les commentaires à des fins de contexte :

- Version et langue de la console Configuration Manager
- Version de site Configuration Manager
- ID de support, également connu comme ID de hiérarchie
- Version et langue du système d'exploitation du système sur lequel la console est en cours d'exécution
- L'emplacement exact dans la console où vous avez cliqué sur le sourire

Ces données sont cohérentes avec la collecte de nos données de diagnostic et d'utilisation. Pour plus d'informations, consultez Données de diagnostic et d'utilisation.

**Problèmes connus**

Si vous essayez d'envoyer des commentaires à partir d'un appareil qui n'a pas accès à Internet, l'application risque de se fermer. Pour envoyer un sourire ou un smiley mécontent, assurez-vous que l'appareil est en mesure d'accéder à petrol.office.microsoft.com.

## Centre d'aide et de support

Utilisez le Centre d'aide et de support pour la résolution des problèmes client, l'affichage des journaux en temps réel ou la capture de l'état d'un ordinateur client Configuration Manager pour une analyse ultérieure. Le Centre d'aide et de support est un outil unique permettant de consolider de nombreux outils administrateur de résolution des problèmes. Un aperçu de la dernière version du Centre d'aide et de support avec des correctifs de bogues, des améliorations et une préversion de notre nouvelle visionneuse de journal est disponible dans la version Technical Preview. Recherchez le programme d'installation du Centre d'aide et de support sur le serveur de site dans le dossier **cd.latest\SMSSETUP\Tools\SupportCenter**.

> **TIP**
> La documentation héritée pour les fonctionnalités existantes dans le Centre d'aide et de support est disponible sur TechNet. Les informations pertinentes sont en cours de migration vers la bibliothèque docs.microsoft.com.

**Nouvelles fonctionnalités du Centre d'aide et de support**

- Une nouvelle visionneuse du journal, OneTrace. Elle fonctionne de la même que CMTrace et inclut des améliorations, telles qu'une vue à onglets et des fenêtres ancrables.
- Une nouvelle fonctionnalité de collecteur de données collecte des journaux de diagnostic à partir de

l'ordinateur local ou d'un client Configuration Manager à distance. Elle fournit un diagnostic en temps réel de l'inventaire (en remplacement de Client Spy), de la stratégie (en remplacement de Policy Spy) et du cache client.

## Kit de ressources de Configuration Manager

Les outils du serveur et du client Configuration Manager sont désormais inclus avec la version Technical Preview. Vous les trouverez dans le dossier **cd.latest\SMSSETUP\Tools** du serveur de site. Aucune installation supplémentaire n'est requise.

**Outils de serveur**

- **Gestionnaire de travaux DP** : permet de résoudre les problèmes relatifs aux travaux de distribution de contenu aux points de distribution
- **Visionneuse d'évaluation de collection** : afficher les détails d'évaluation de la collection
- **Explorateur de la bibliothèque de contenu** : afficher le contenu du magasin d'instances unique de la bibliothèque de contenu
- **Transfert de la bibliothèque de contenu** : transfère la bibliothèque de contenu entre des disques
- **Outil de propriété du contenu** : modifie la propriété des packages orphelins. Ces packages existent dans le site sans serveur de site propriétaire.
- **Outil d'administration et d'audit en fonction du rôle** : permet aux administrateurs d'auditer la configuration des rôles

**Outils clients**

- **CMTrace** : afficher les journaux
- **Outil de monitoring de déploiement** : résoudre les problèmes liés aux applications, mises à jour et déploiements de ligne de base
- **Policy Spy** : afficher les affectations de stratégies
- **Outil Power Viewer** : afficher l'état de la fonctionnalité de gestion de l'alimentation
- **Outil Send Schedule** : déclencher des planifications et des évaluations des lignes de base DCM

> **IMPORTANT**
>
> Le Centre d'aide et de support est recommandé dans la plupart des cas d'utilisation, car il inclut des fonctionnalités identiques ou améliorée pour les outils suivants :
>
> - Client Spy
> - CMTrace[1]
> - Outil de monitoring de déploiement
> - Policy Spy
> - Outil Send Schedule
>
> [1] CMTrace ne dépend pas de .NET ou de WPF (Windows Presentation Foundation), donc il est toujours utilisé dans les images de démarrage Windows PE.

**Problèmes connus**

Certains outils client et serveur peuvent se fermer de manière inattendue à l'ouverture. Ce problème est dû à un fichier manquant sur le support. Pour contourner le problème, copiez le fichier **Microsoft.Diagnostics.Tracing.EventSource.dll** à partir du répertoire AdminConsole\bin dans les répertoires SMSSETUP\Tools\ClientTools et ServerTools. Ce fichier doit être la même version que celle utilisée par la console

Configuration Manager. D'autres versions risquent de ne pas fonctionner.

## Désinstaller une application en cas de révocation de l'approbation

Le comportement a changé lorsque vous révoquez une approbation pour une application. Maintenant, lorsque vous refusez la requête visant l'application, le client désinstalle l'application sur l'appareil de l'utilisateur.

**Prérequis**

- Activez la fonctionnalité **Approuver les demandes d'application pour les utilisateurs appareil par appareil**.

**Essayez !**

Essayez d'effectuer les tâches. Envoyez-nous ensuite des commentaires pour nous indiquer comment cela a fonctionné.

1. Dans la console Configuration Manager, déployez pour un utilisateur une application qui nécessite une approbation. Dans l'onglet **Paramètres de déploiement** du déploiement, activez l'option **Un administrateur doit approuver une demande pour cette application sur l'appareil**.
2. Sur le client Configuration Manager dans le Centre logiciel, l'utilisateur demande l'approbation pour installer l'application.
3. Dans la console Configuration Manager, approuvez la demande de cet utilisateur pour installer l'application sur l'appareil. Les demandes d'approbation d'application sont affichées dans l'espace de travail **Bibliothèque de logiciels**, sous **Gestion d'applications** dans le nœud **Demandes d'approbation**.
4. Sur le client dans le Centre logiciel, l'utilisateur installe l'application.
5. Dans la console Configuration Manager, refusez la demande de l'utilisateur pour installer l'application sur l'appareil.

**Problèmes connus**

- Une fois que l'utilisateur a installé l'application sur le client, mettez à jour la stratégie de l'utilisateur. Dans le Centre logiciel, basculez vers l'onglet **Options**, développez **Maintenance de l'ordinateur** et cliquez sur **Stratégie de synchronisation**.
- Le point de service web du catalogue des applications doit être de type HTTP. Pour plus d'informations, consultez Problèmes connus dans cette préversion technique.

## Exclure les conteneurs Active Directory de la détection

Pour réduire le nombre d'objets détectés, vous pouvez désormais exclure des conteneurs spécifiques de la détection de systèmes Active Directory. Cette fonctionnalité est le résultat de vos commentaires sur UserVoice.

**Essayez !**

Essayez d'effectuer les tâches. Envoyez-nous ensuite des commentaires pour nous indiquer comment cela a fonctionné.

1. Dans la console de Configuration Manager, accédez à l'espace de travail **Administration**. Développez **Configuration de la hiérarchie** et sélectionnez **Méthodes de découverte**. Sélectionnez **Découverte de système Active Directory** et cliquez sur **Propriétés** dans le ruban.
2. Cliquez sur l'icône Nouveau pour spécifier un nouveau conteneur Active Directory.
3. Dans la boîte de dialogue Conteneur Active Directory, accédez au **Chemin d'accès** ou entrez-le dans la section Emplacement pour démarrer la détection.
4. Dans la section Options de recherche, activez l'option **Rechercher de manière récursive les conteneurs**

**enfants Active Directory**. Puis, cliquez sur **Ajouter** pour sélectionner les sous-conteneurs à exclure de cette détection.

5. Dans la boîte de dialogue Sélectionner un nouveau conteneur, sélectionnez un conteneur enfant à exclure. Cliquez sur **OK** pour fermer la boîte de dialogue Sélectionner un nouveau conteneur.
6. Cliquez sur **OK** pour fermer la boîte de dialogue Conteneur Active Directory.
7. Dans la fenêtre Propriétés de découverte de système Active Directory, consultez le chemin d'accès du conteneur Active Directory où démarre la détection. La colonne **Récursive** affiche **Oui** et la nouvelle colonne **A des exclusions** affiche également **Oui**. Cliquez sur **OK** pour fermer la fenêtre Propriétés de découverte de système Active Directory.

## Spécifier la visibilité du lien du site web Catalogue d'applications dans le Centre logiciel

Vous pouvez désormais contrôler si le lien vers **Ouvrir le site web Catalogue d'applications** s'affiche dans le nœud **État d'installation** du Centre logiciel.

> **NOTE**
> La prise en charge de l'expérience utilisateur du site web du catalogue d'applications se termine avec la première mise à jour publiée après le 1er juin 2018. Pour plus d'informations, consultez Fonctionnalités supprimées et déconseillées.

**Essayez !**

Essayez d'effectuer les tâches. Envoyez-nous ensuite des commentaires pour nous indiquer comment cela a fonctionné.

1. Dans la console de Configuration Manager, créez une stratégie personnalisée de paramètres d'appareils clients sur le nœud **Paramètres clients** de l'espace de travail **Administration**.
2. Sélectionnez le groupe **Centre logiciel**.
3. Pour **Paramètres du Centre logiciel**, cliquez sur **Personnaliser**.
4. Activez l'option **Masquer le lien du site web du catalogue d'applications dans le Centre logiciel**.

Pour plus d'informations sur les paramètres client, consultez Configurer les paramètres client.

## Filtrer les règles de déploiement automatique par architecture de mise à jour logicielle

Vous pouvez désormais filtrer les règles de déploiement automatique pour exclure les architectures comme Itanium et ARM64.

**Essayez !**

Essayez d'effectuer les tâches. Envoyez-nous ensuite des commentaires pour nous indiquer comment cela a fonctionné.

1. Dans la console de Configuration Manager, accédez à l'espace de travail **Bibliothèque de logiciels**. Développez **Mises à jour logicielles** et sélectionnez **Règles de déploiement automatique**. Sur le ruban, sélectionnez **Créer une règle de déploiement automatique**.
2. Renseignez les paramètres appropriés dans l'onglet **Général** et l'onglet **Paramètres de déploiement**.
3. Dans l'onglet **Mises à jour logicielles**, sélectionnez **Architecture**, puis cliquez sur **Éléments à rechercher** dans les **critères de recherche**.

4. Sélectionnez les architectures à inclure dans la règle de déploiement automatique.

5. Cliquez sur **Suivant** et poursuivez la création de la règle de déploiement automatique.

> **IMPORTANT**
> N'oubliez pas qu'il existe des applications 32 bits (x86) et des composants exécutés sur des systèmes 64 bits (x64). Sauf si vous êtes certain de ne pas besoin de x86, activez-le aussi lorsque vous choisissez x64.

**Problèmes connus**

Après avoir ajouté les critères de l'architecture, la page des propriétés de la règle de déploiement automatique affiche **Titre** dans les critères de recherche. La règle de déploiement automatique fonctionne toujours comme prévu et sélectionne les mises à jour logicielles correctes. Toutefois, vous ne pouvez pas inclure à la fois les critères **Architecture** et **Titre** pour l'instant.

## Améliorations apportées au déploiement de système d'exploitation

Les améliorations suivantes, inspirées notamment par vos commentaires User Voice, ont été apportées au déploiement des systèmes d'exploitation.

- Masquer les données sensibles stockées dans des variables de séquence de tâches : dans l'étape Définir la variable de séquence de tâches, sélectionnez la nouvelle option **Ne pas afficher cette valeur**. Par exemple, lorsque vous spécifiez un mot de passe. Les comportements suivants s'appliquent lorsque vous activez cette option :
  - La valeur de la variable n'est pas affichée dans le fichier smsts.log.
  - La console Configuration Manager et le fournisseur SMS traitent cette valeur de la même façon que d'autres secrets comme les mots de passe.
  - La valeur n'est pas incluse lorsque vous exportez la séquence de tâches.
  - L'éditeur de la séquence de tâches ne lit pas cette valeur lorsque vous modifiez l'étape. Tapez à nouveau la valeur entière pour apporter des modifications.

  > **IMPORTANT**
  > Les variables et leurs valeurs sont enregistrées avec la séquence de tâches en tant que XML et obscurcies dans la base de données. Lorsque le client demande une stratégie de séquence de tâches à partir du point de gestion, elle est chiffrée en transit et lorsqu'elle est stockée sur le client. Toutefois, toutes les valeurs des variables sont en texte brut dans l'environnement de la séquence de tâches dans la mémoire pendant l'exécution sur le client. Si la séquence de tâches inclut une étape pour extraire la valeur de la variable, cette sortie est au format texte brut. Ce comportement nécessite une action explicite par l'administrateur afin d'inclure une étape de ce type dans la séquence de tâches.

- Masquer le nom du programme pendant l'étape Exécuter la commande d'une séquence de tâches : pour empêcher l'affichage ou la consignation de données potentiellement sensibles, définissez la variable de la séquence de tâches **OSDDoNotLogCommand** sur `TRUE`. Cette variable masque le nom du programme dans le fichier smsts.log au cours de l'étape Exécuter la ligne de commande d'une séquence de tâches.

## Améliorations apportées à la console Configuration Manager

- Les informations de l'utilisateur principal sont désormais visibles lorsque vous affichez les membres d'une collection sous **Ressources et conformité**, **Collections d'appareils**.

## Étapes suivantes

Pour obtenir des informations complémentaires sur l'installation ou la mise à jour de l'édition Technical Preview, consultez Technical Preview pour System Center Configuration Manager.

# Fonctionnalités de Technical Preview 1803 pour System Center Configuration Manager

22/06/2018 • 15 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Technical Preview)*

Cet article présente les fonctionnalités disponibles dans Technical Preview version 1803 pour Configuration Manager. Vous pouvez installer cette version pour mettre à jour et ajouter de nouvelles fonctionnalités au site de votre préversion technique.

Consultez l'article Technical Preview avant d'installer cette mise à jour. Cet article vous permet de vous familiariser avec les limitations et les conditions générales liées à l'utilisation d'une version Technical Preview, et explique comment effectuer une mise à jour d'une version vers une autre et comment envoyer des commentaires.

**Vous trouverez ci-dessous les nouvelles fonctionnalités propres à cette version.**

## Prise en charge des points de distribution cloud comme source par les points de distribution d'extraction

De nombreux clients utilisent des points de distribution d'extraction dans des bureaux distants ou des filiales pour télécharger du contenu à partir d'un point de distribution source sur le réseau WAN. Si vos bureaux distants ont une meilleure connexion à Internet, ou pour réduire la charge sur vos liaisons WAN, vous pouvez désormais utiliser un point de distribution cloud dans Microsoft Azure comme source. Quand vous ajoutez une source sous l'onglet **Point de distribution d'extraction** des propriétés de point de distribution, tout point de distribution cloud du site est maintenant répertorié comme point de distribution disponible. Le comportement des deux rôles système de site reste inchangé par ailleurs.

**Prérequis**

- Le point de distribution d'extraction a besoin d'un accès Internet pour communiquer avec Microsoft Azure.
- Le contenu doit être distribué au point de distribution cloud source.

> **NOTE**
> Cette fonctionnalité implique des frais sur votre abonnement Azure pour le stockage de données et la sortie de réseau. Pour plus d'informations, consultez le Coût d'utilisation d'une distribution cloud.

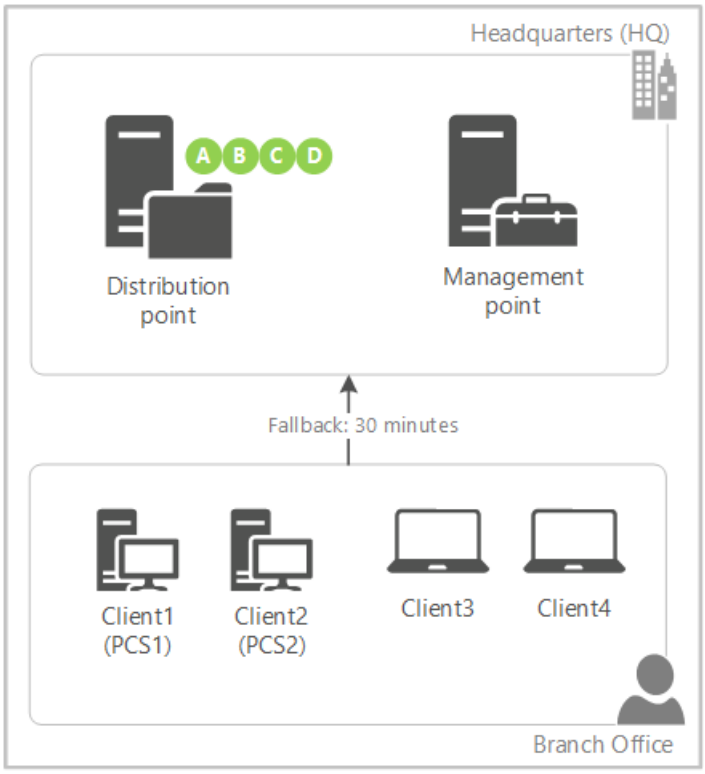
## Prise en charge du téléchargement partiel dans le cache d'homologue client pour réduire l'utilisation du réseau WAN

Les sources de cache d'homologue client peuvent désormais diviser le contenu en plusieurs parties. Ces parties diminuent le transfert de réseau afin de réduire l'utilisation du réseau WAN. Le point de gestion fournit un suivi plus détaillé des parties du contenu. Il essaie de supprimer plusieurs téléchargements du même contenu par groupe de limites.

**Exemple de scénario**

Contoso a un seul site principal avec deux groupes de limites : un siège social et une filiale. Il existe une relation de repli de 30 minutes entre les groupes de limites. Le point de gestion et le point de distribution du site se trouvent

uniquement dans la limite du siège social. L'emplacement de la filiale n'a aucun point de distribution local. Deux des quatre clients au niveau de la filiale sont configurés comme sources de cache d'homologue.




1. Vous ciblez un déploiement avec du contenu sur les quatre clients de la filiale. Vous avez distribué du contenu uniquement au point de distribution.
2. Client3 et Client4 n'ont pas de source locale pour le déploiement. Le point de gestion indique aux clients de patienter 30 minutes avant de revenir au groupe de limites distantes.
3. Client1 (PCS1) est la première source de cache d'homologue pour actualiser la stratégie avec le point de gestion. Étant donné que ce client est activé comme source de cache d'homologue, le point de gestion lui indique de commencer immédiatement le téléchargement de la partie A à partir du point de distribution.
4. Quand Client2 (PCS2) contacte le point de gestion, comme la partie A est déjà en cours mais pas encore terminée, le point de gestion lui indique de commencer immédiatement le téléchargement de la partie B à partir du point de distribution.
5. PCS1 termine le téléchargement de la partie A et en avertit immédiatement le point de gestion. Comme la partie B est déjà en cours mais pas encore terminée, le point de gestion lui indique de commencer le téléchargement de la partie C à partir du point de distribution.
6. PCS2 termine le téléchargement de la partie B et en avertit immédiatement le point de gestion. Le point de gestion lui indique de commencer le téléchargement de la partie D à partir du point de distribution.
7. PCS1 termine le téléchargement de la partie C et en avertit immédiatement le point de gestion. Le point de gestion l'informe qu'aucune autre partie n'est disponible à partir du point de distribution distant. Le point de gestion lui indique de télécharger la partie B à partir de son homologue local, PCS2.
8. Ce processus se poursuit jusqu'à ce que les deux sources de cache d'homologue client aient toutes les parties de l'une et de l'autre. Le point de gestion établit la priorité des parties à partir du point de distribution distant avant d'indiquer aux sources de cache d'homologue de télécharger des parties à partir des homologues locaux.
9. Client3 est le premier à actualiser la stratégie au terme de la période de repli de 30 minutes. Il vérifie de nouveau auprès du point de gestion, qui indique au client des nouvelles sources locales. Au lieu de télécharger le contenu en totalité à partir du point de distribution sur le réseau WAN, il télécharge le contenu en totalité à partir de l'une des sources de cache d'homologue client. Les clients établissent la priorité des sources d'homologue local.

> **NOTE**
> Si le nombre de sources de cache d'homologue client est supérieur au nombre de parties du contenu, le point de gestion indique aux sources de cache d'homologue supplémentaires d'attendre une action de repli comme un client normal.

**Essayez !**

Essayez d'effectuer les tâches. Envoyez ensuite des **commentaires** à partir de l'onglet **Accueil** du ruban et faites-nous savoir comment cela a fonctionné.

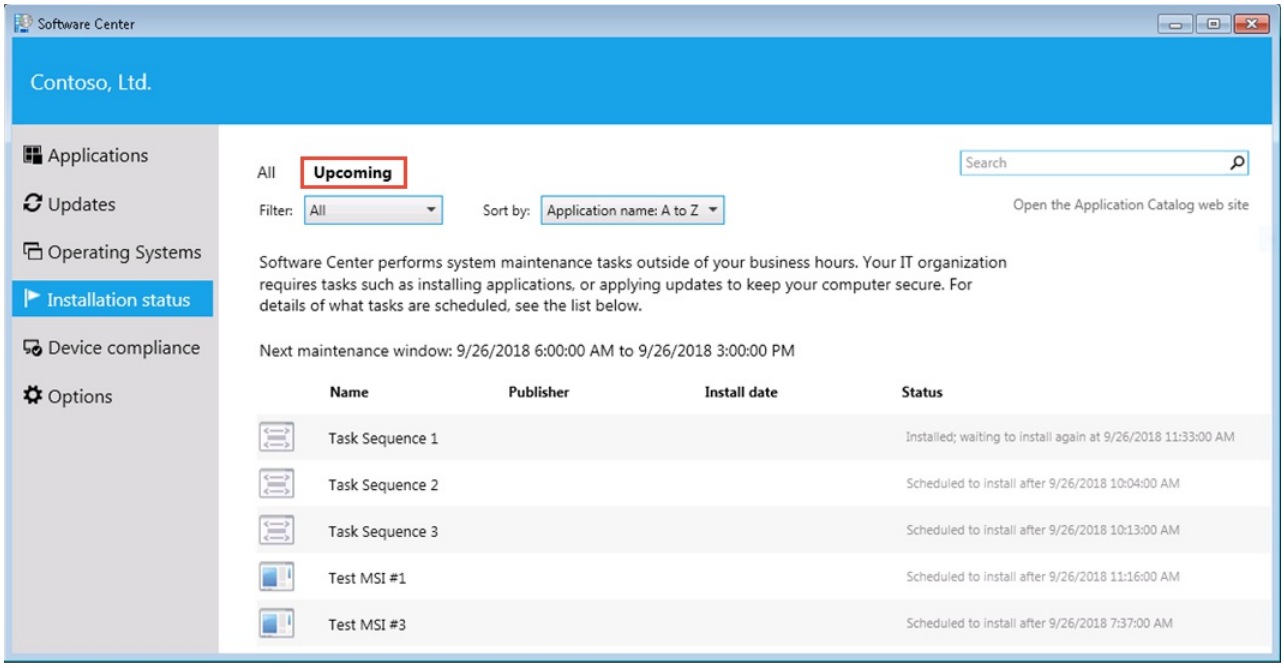
1. Configurez normalement des groupes de limites et des sources de cache d'homologue.
2. Dans la console Configuration Manager, accédez à l'espace de travail **Administration**, développez **Configuration du site**, puis sélectionnez **Sites**. Cliquez sur **Paramètres de hiérarchie** dans le ruban.
3. Sous l'onglet **Général**, activez l'option permettant de **configurer les sources de cache d'homologue client pour diviser du contenu en parties**.
4. Créez un déploiement obligatoire avec du contenu.

   > **NOTE**
   > Cette fonctionnalité fonctionne uniquement quand le client télécharge le contenu en arrière-plan, comme avec un déploiement obligatoire. Les téléchargements à la demande, comme quand l'utilisateur installe un déploiement disponible dans le Centre logiciel, se comportent comme d'habitude.

5. Pour les voir gérer le téléchargement du contenu en parties, examinez le fichier **ContentTransferManager.log** sur la source de cache d'homologue client et le fichier **MP_Location.log** sur le point de gestion.

## Fenêtres de maintenance dans le Centre logiciel

Le Centre logiciel affiche maintenant la fenêtre de maintenance planifiée suivante. Sous l'onglet État de l'installation, passez de la vue Tous à la vue À venir. Elle affiche la période et la liste des déploiements qui sont planifiés. La liste est vide s'il n'existe aucune fenêtre de maintenance future.




## Onglet personnalisé pour une page web du Centre logiciel

Vous pouvez maintenant créer un onglet personnalisé pour ouvrir une page web dans le Centre logiciel. Cette fonctionnalité vous permet d'afficher du contenu à vos utilisateurs finaux d'une façon cohérente et fiable. La liste suivante comprend quelques exemples :

- Contacter le service informatique : informations sur la façon de contacter le service informatique de votre organisation
- Centre de support informatique : actions informatiques en libre-service telles que la recherche dans une base de connaissances ou l'ouverture d'un ticket de support.
- Documentation pour les utilisateurs finaux : articles destinés aux utilisateurs de votre organisation sur différents sujets informatiques comme l'utilisation d'applications ou la mise à niveau vers Windows 10.

**Essayez !**

Essayez d'effectuer les tâches. Envoyez ensuite des **commentaires** à partir de l'onglet **Accueil** du ruban et faites-nous savoir comment cela a fonctionné.

1. Dans la console Configuration Manager, sur le nœud **Paramètres clients** de l'espace de travail **Administration**, ouvrez la stratégie **Paramètres client par défaut**.
2. Sélectionnez le groupe **Centre logiciel**.
3. Pour **Paramètres du Centre logiciel**, cliquez sur **Personnaliser**.
4. Passez à l'onglet **Onglets**.
5. Activez l'option permettant de **spécifier un onglet personnalisé pour le Centre logiciel**.
   a. Entrez un nom dans le champ de texte **Nom de l'onglet**. C'est le nom que voit l'utilisateur dans le Centre logiciel.
   b. Entrez une URL valide dans le champ de texte**URL du contenu**. Cette URL est le contenu que le Centre logiciel affiche quand les utilisateurs cliquent sur cet onglet.

> **TIP**
> Le Centre logiciel utilise des composants Internet Explorer pour le rendu de la page web.

## Activer la prise en charge des mises à jour de logiciels tiers sur des clients

Vous pouvez maintenant activer la configuration des clients Configuration Manager pour les mises à jour de logiciels tiers. Quand vous **activez les mises à jour de logiciels tiers** pour les propriétés du composant de point de mise à jour logicielle, le point de mise à jour logicielle télécharge le certificat de signature utilisé par WSUS pour les mises à jour tierces.

Le fait de sélectionner l'option **Activer les mises à jour de logiciels tiers** dans les paramètres clients effectue les opérations suivantes :

- Sur le client, cela définit la stratégie pour « Autoriser les mises à jour signées provenant d'un emplacement intranet du service de mise à jour Microsoft ».
- Cela installe le certificat de signature dans la banque d'éditeurs approuvés sur le client.

**Essayez !**

Essayez d'effectuer les tâches. Envoyez ensuite des **commentaires** à partir de l'onglet **Accueil** du ruban et faites-nous savoir comment cela a fonctionné.

1. Sur le site le plus haut dans la hiérarchie Configuration Manager, accédez au nœud **Administration**, développez **Configuration du site**, puis **Sites**.
2. Cliquez avec le bouton droit sur votre serveur de site le plus en haut et sélectionnez **Configurer les composants de site**, puis **Point de mise à jour logicielle**.

3. Cliquez sur l'onglet **Mises à jour tierces**, puis cochez **Activer les mises à jour de logiciels tiers**.
4. Ouvrez **Paramètres client**, puis accédez aux paramètres de **Mises à jour logicielles**.
5. Vérifiez que l'option **Activer les mises à jour de logiciels tiers** a la valeur **Oui**.

## Activer le copier/coller des détails de composants à partir d'affichages d'analyse

Suite à vos commentaires User Voice, vous pouvez maintenant activer la fonctionnalité copier/coller dans le volet des détails de composants dans les affichages d'analyse de l'état du déploiement et de la distribution.

## Extensions SCAP

La préversion des Extensions SCAP est disponible dans le dossier Cd.latest sous SMSSETUP\TOOLS\ConfigMgrSCAPExtension\ConfigMgrExtensionsForSCAP.msi. Cette préversion des Extensions SCAP peut être installée sur toutes les versions actuellement prises en charge de Configuration Manager Current Branch et LTSB 1606. Pour plus d'informations, consultez À propos des Extensions SCAP (Security Content Automation Protocol).

## Étapes suivantes

Pour obtenir des informations complémentaires sur l'installation ou la mise à jour de l'édition Technical Preview, consultez Technical Preview pour System Center Configuration Manager.

# Migrer des données entre hiérarchies dans System Center Configuration Manager

22/06/2018 • 15 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Transférez des données d'une hiérarchie source prise en charge vers une hiérarchie de destination System Center Configuration Manager en procédant à une migration. Quand vous migrez des données d'une hiérarchie source :

- Vous accédez aux données des bases de données de site que vous identifiez dans l'infrastructure source, puis vous transférez ces données vers votre environnement actuel.
- La migration ne modifie pas les données de la hiérarchie source, mais découvre les données et en enregistre une copie dans la base de données de la hiérarchie de destination.

Tenez compte des points suivants quand vous planifiez votre stratégie de migration :

- Vous pouvez migrer une infrastructure Configuration Manager 2007 SP2 existante vers System Center Configuration Manager.
- Vous pouvez migrer certaines données ou toutes les données prises en charge à partir d'un site source.
- Vous pouvez migrer les données d'un seul site source vers plusieurs sites dans la hiérarchie de destination.
- Vous pouvez déplacer des données de plusieurs sites sources vers un seul site dans la hiérarchie de destination.

## Concepts de migration

Vous pouvez rencontrer les concepts et les termes suivants quand vous utilisez la migration.

| CONCEPT OU TERME | PLUS D'INFORMATIONS |
|---|---|
| Hiérarchie source | Hiérarchie qui exécute une version prise en charge de Configuration Manager et qui contient les données à migrer. Quand vous configurez la migration, vous identifiez la hiérarchie source au moment de spécifier le site de niveau supérieur de cette hiérarchie. Une fois que vous avez spécifié une hiérarchie source, le site de niveau supérieur de la hiérarchie de destination recueille les données de la base de données du site source désigné afin d'identifier les données que vous pouvez migrer.<br><br>Pour plus d'informations, consultez Hiérarchies sources dans Planification d'une stratégie de hiérarchie source dans System Center Configuration Manager. |
| Sites source | Sites de la hiérarchie source comportant des données vous pouvez migrer vers votre hiérarchie de destination.<br><br>Pour plus d'informations, consultez Sites sources dans Planification d'une stratégie de hiérarchie source dans System Center Configuration Manager. |

| CONCEPT OU TERME | PLUS D'INFORMATIONS |
| --- | --- |
| Hiérarchie de destination | Hiérarchie System Center Configuration Manager dans laquelle une migration est exécutée pour importer les données d'une hiérarchie source. |
| Collecte des données | Processus continu d'identification des informations d'une hiérarchie source que vous pouvez migrer vers votre hiérarchie de destination. Configuration Manager vérifie la hiérarchie source selon une planification établie pour identifier les modifications apportées aux informations de la hiérarchie source que vous avez déjà migrées et que vous pourriez souhaiter mettre à jour dans la hiérarchie de destination.<br><br>Pour plus d'informations, consultez Collecte de données dans Planification d'une stratégie de hiérarchie source dans System Center Configuration Manager. |
| Tâches de migration | Processus de configuration des objets spécifiques à migrer et de gestion de la migration de ces objets vers la hiérarchie de destination.<br><br>Pour plus d'informations, consultez Planification d'une stratégie pour les tâches de migration dans System Center Configuration Manager. |
| Migration des clients | Processus de transfert d'informations que les clients utilisent depuis la base de données du site source vers la base de données de la hiérarchie de destination. Cette migration des données est ensuite suivie d'une mise à niveau du logiciel client sur les périphériques à la version du logiciel client à partir de la hiérarchie de destination.<br><br>Pour plus d'informations, voir Planification d'une stratégie de migration de clients dans System Center Configuration Manager. |
| Points de distribution partagés | Points de distribution de la hiérarchie source qui sont partagés avec la hiérarchie de destination tout au long de la période de migration.<br><br>Pendant la période de migration, les clients attribués aux sites de la hiérarchie de destination peuvent obtenir du contenu auprès des points de distribution partagés.<br><br>Pour plus d'informations, consultez Partager des points de distribution entre une hiérarchie source et une hiérarchie de destination dans Planification d'une stratégie de migration de déploiement de contenu dans System Center Configuration Manager. |
| Surveillance de la migration | Processus de surveillance des activités de migration. Vous surveillez la progression de la migration et son bon déroulement à partir du nœud **Migration** de l'espace de travail **Administration**.<br><br>Pour plus d'informations, consultez Planification de la surveillance de la migration dans System Center Configuration Manager. |

| CONCEPT OU TERME | PLUS D'INFORMATIONS |
| --- | --- |
| Arrêter la collecte de données | Processus consistant à arrêter la collecte de données auprès des sites source. Quand vous n'avez plus de données à migrer à partir d'une hiérarchie source, ou si vous voulez suspendre les activités liées à la migration, vous pouvez configurer la hiérarchie de destination pour arrêter la collecte de données à partir de la hiérarchie source.<br><br>Pour plus d'informations, consultez Collecte de données dans Planification d'une stratégie de hiérarchie source dans System Center Configuration Manager. |
| Nettoyer les données de migration | Processus de finalisation de la migration à partir d'une hiérarchie source en supprimant les informations relatives à la migration à partir de la base de données des hiérarchies de destination.<br><br>Pour plus d'informations, voir Planification d'une migration complète vers System Center 2012 Configuration Manager. |

## Flux de travail standard de migration

Pour configurer un flux de travail standard de migration :

1. Spécifiez une hiérarchie source prise en charge.
2. Configurez la collecte des données. La collecte de données permet à Configuration Manager de récupère des informations sur les données qui peuvent être migrées à partir de la hiérarchie source.

   Configuration Manager répète automatiquement le processus de collecte de données selon une planification simple, jusqu'à ce que vous arrêtiez ce processus. Par défaut, il se répète toutes les quatre heures, de telle sorte que Configuration Manager peut identifier les modifications apportées aux données de la hiérarchie source que vous pourriez souhaiter migrer. La collecte de données est également nécessaire pour partager des points de distribution entre la hiérarchie source et la hiérarchie de destination.
3. Créez des tâches de migration pour migrer des données entre la hiérarchie source et la hiérarchie de destination.
4. Vous pouvez arrêter le processus de collecte de données à tout moment, à l'aide de la commande **Arrêter la collecte de données** . Quand vous arrêtez la collecte de données, Configuration Manager n'identifie plus les modifications apportées aux données de la hiérarchie source et ne peut plus partager de points de distribution entre la hiérarchie source et la hiérarchie de destination. En règle générale, cette commande est utilisée lorsque vous n'avez plus l'intention de migrer des données ni de partager des points de distribution à partir de la hiérarchie source.
5. Si vous le souhaitez, après avoir arrêté la collecte de données sur tous les sites pour la hiérarchie source, vous pouvez nettoyer les données de migration à l'aide de la commande **Nettoyer les données de migration** . Cette commande supprime de la base de données de la hiérarchie de destination l'ensemble des données historiques relatives à la migration à partir d'une hiérarchie source.

Après avoir migré les données d'une hiérarchie source Configuration Manager que vous n'utiliserez plus pour gérer votre environnement, vous pouvez désactiver cette hiérarchie source et son infrastructure.

## Scénarios de migration

Configuration Manager prend en charge les scénarios de migration ci-suivants.

> **NOTE**
> L'expansion d'une hiérarchie contenant un site autonome en hiérarchie contenant un site d'administration centrale n'est pas considérée comme une migration. Pour plus d'informations sur l'expansion de hiérarchie, consultez Étendre un site principal autonome dans Utiliser l'Assistant Installation pour installer des sites.

### Migration à partir de hiérarchies Configuration Manager 2007

Quand vous migrez des données à partir de Configuration Manager 2007, vous pouvez pérenniser les investissements liés à votre infrastructure de site existante et profiter des avantages suivants :

| AVANTAGE | PLUS D'INFORMATIONS |
|---|---|
| Améliorations de la base de données du site | La base de données System Center Configuration Manager assure une prise en charge complète d'Unicode. |
| Réplication de la base de données entre sites | La réplication dans System Center Configuration Manager s'appuie sur Microsoft SQL Server. Les performances des transferts de données de site à site sont ainsi améliorées. |
| Gestion centrée sur l'utilisateur | Les utilisateurs constituent l'élément central des tâches de gestion dans System Center Configuration Manager. Par exemple, vous pouvez distribuer un logiciel à un utilisateur, même si vous ne connaissez pas le nom du périphérique pour cet utilisateur. En outre, System Center Configuration Manager offre aux utilisateurs beaucoup plus de contrôle sur les logiciels qui sont installés sur leurs appareils et sur le moment où ils le sont. |
| Simplification de la hiérarchie | Dans System Center Configuration Manager, le type de site d'administration centrale et les modifications apportées au comportement du site principal et des sites secondaires vous permettent de créer une hiérarchie de site plus simple, plus économique en bande passante réseau et nécessitant un nombre de serveurs moins important. |
| Administration basée sur des rôles | Ce modèle de sécurité central dans System Center Configuration Manager offre une gestion et une sécurité pour toute la hiérarchie, qui correspondent à vos exigences administratives et opérationnelles. |

> **NOTE**
> Compte tenu de l'évolution de la conception amorcée par System Center 2012 Configuration Manager, vous ne pouvez pas mettre à niveau une infrastructure Configuration Manager 2007 vers System Center Configuration Manager. La mise à niveau sur place de System Center 2012 Configuration Manager vers System Center Configuration Manager est prise en charge.

### Migration à partir d'une hiérarchie Configuration Manager 2012 ou d'une autre hiérarchie System Center Configuration Manager

Le processus de migration de données d'une hiérarchie System Center 2012 Configuration Manager ou System Center Configuration Manager est identique. Vous pouvez notamment migrer les données de plusieurs hiérarchies sources vers une seule hiérarchie de destination, par exemple, quand votre société obtient des ressources supplémentaires qui sont déjà gérées par Configuration Manager. Par ailleurs, vous pouvez migrer des données d'un environnement de test vers votre environnement de production Configuration Manager. Vous pérennisez ainsi les investissements liés à l'environnement de test Configuration Manager.

## Rubriques supplémentaires relatives à la migration :

- Planification de la migration vers System Center Configuration Manager
- Configuration des hiérarchies sources et des sites sources pour la migration vers System Center Configuration Manager
- Opérations de migration vers System Center Configuration Manager
- Sécurité et confidentialité pour la migration vers System Center Configuration Manager

## Voir aussi

Commencer à utiliser System Center Configuration Manager

# Planifier la migration vers System Center Configuration Manager

22/06/2018 • 3 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Avant de migrer des données vers une hiérarchie de destination System Center Configuration Manager, familiarisez-vous avec les sites et les hiérarchies dans Configuration Manager. Pour plus d'informations sur les sites et les hiérarchies, consultez Principes de base de System Center Configuration Manager.

Avant de migrer des données à partir d'une hiérarchie source prise en charge, vous devez installer une hiérarchie System Center Configuration Manager comme hiérarchie de destination.

Une fois la hiérarchie de destination installée, avant de commencer à migrer les données, configurez les fonctionnalités de gestion et les fonctions que vous voulez utiliser dans votre hiérarchie de destination.

En outre, vous devrez peut-être anticiper un éventuel chevauchement entre la hiérarchie source et votre hiérarchie de destination. Supposons par exemple que vous configurez une hiérarchie source pour utiliser les mêmes emplacements réseau ou les mêmes limites que votre hiérarchie de destination, que vous installez ensuite de nouveaux clients sur votre hiérarchie de destination et que vous utilisez l'affectation de site automatique. Dans ce scénario, comme un client Configuration Manager nouvellement installé peut sélectionner un site à rejoindre dans l'une ou l'autre des hiérarchies, le client risque d'être incorrectement affecté à votre hiérarchie source. Par conséquent, au lieu d'utiliser la fonctionnalité d'affectation de site automatique, prévoyez plutôt d'affecter chaque nouveau client de la hiérarchie de destination à un site spécifique de cette hiérarchie.

Pour plus d'informations sur les affectations de site, consultez Considérations sur l'affectation de sites aux clients dans Interopérabilité entre les différentes versions de System Center Configuration Manager.

## Rubriques liées à la planification

Utilisez les rubriques suivantes pour planifier la migration d'une hiérarchie source prise en charge vers une hiérarchie de destination System Center Configuration Manager :

- Prérequis de la migration dans System Center Configuration Manager
- Listes de vérification de l'administrateur pour la planification de la migration dans System Center Configuration Manager
- Déterminer s'il faut migrer des données vers System Center Configuration Manager
- Planifier une stratégie de hiérarchie source dans System Center Configuration Manager
- Listes de vérification de l'administrateur pour la planification de la migration dans System Center Configuration Manager
- Planifier une stratégie de migration de clients dans System Center Configuration Manager
- Planifier une stratégie de migration de déploiement de contenu dans System Center Configuration Manager
- Planifier la migration d'objets Configuration Manager vers System Center Configuration Manager
- Planifier la surveillance de la migration dans System Center Configuration Manager

- Planifier la fin de la migration dans System Center Configuration Manager

# Prérequis de la migration dans System Center Configuration Manager

22/06/2018 • 11 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Pour migrer à partir d'une hiérarchie source prise en charge, vous devez avoir accès à chaque site source Configuration Manager applicable et aux autorisations dans le site de destination System Center Configuration Manager pour configurer et exécuter des opérations de migration.

Pour mieux comprendre les versions de Configuration Manager prises en charge pour la migration et les configurations requises, aidez-vous des informations figurant dans les sections suivantes.

- Versions de Configuration Manager prises en charge pour la migration
- Langues de site source prises en charge pour la migration
- Configurations requises pour la migration

## Versions de Configuration Manager prises en charge pour la migration

Vous pouvez migrer des données à partir d'une hiérarchie source qui exécute une des versions suivantes de Configuration Manager :

- Configuration Manager 2007 SP2 (Pour la migration, il importe peu que le site source dispose de Configuration Manager 2007 R2 ou R3. Tant que le site source exécute SP2, les sites dotés du module complémentaire R2 ou R3 sont pris en charge pour la migration vers System Center Configuration Manager).
- System Center 2012 Configuration Manager SP2 ou System Center 2012 R2 Configuration Manager SP1

  > **TIP**
  > En plus de la migration, vous pouvez utiliser une mise à niveau sur place des sites exécutant System Center 2012 Configuration Manager vers System Center Configuration Manager.

- Une hiérarchie System Center Configuration Manager présentant une version identique ou inférieure à celle de System Center Configuration Manager.

  Par exemple, si vous disposez d'une hiérarchie de destination qui exécute System Center Configuration Manager version 1606, vous pouvez utiliser la migration pour copier des données à partir d'une hiérarchie source qui exécute la version 1606 ou 1602. Toutefois, vous ne pouvez pas migrer des données depuis une hiérarchie source exécutant la version 1610.

## Langues de site source prises en charge pour la migration

Quand vous migrez des données entre hiérarchies Configuration Manager, celles-ci sont stockées dans la hiérarchie de destination dans un format indépendant de la langue pour System Center Configuration Manager. Étant donné que Configuration Manager 2007 ne stocke pas les données dans un format indépendant de la langue, le processus de migration doit convertir les objets dans ce format pendant la migration à partir de

Configuration Manager 2007. Par conséquent, seuls les sites sources Configuration Manager 2007 installés avec les langues suivantes sont pris en charge pour la migration :

- Anglais
- Français
- Allemand
- Japonais
- Coréen
- Russe
- Chinois simplifié
- Chinois traditionnel

Quand vous migrez des données à partir d'une hiérarchie System Center 2012 Configuration Manager ou System Center Configuration Manager, il n'existe aucune limitation de langue du site source. Les objets dans la base de données du site source sont déjà dans un format indépendant de la langue.

## Configurations requises pour la migration

Voici les configurations requises pour la migration :

- **Pour configurer, exécuter et surveiller la migration dans la console Configuration Manager :**

  Dans le site de destination, le rôle de sécurité d'administration **Administrateur d'infrastructure**doit être affecté à votre compte. Ce rôle de sécurité accorde des autorisations pour gérer toutes les opérations de migration, notamment la création de tâches de migration, le nettoyage, la surveillance ainsi que le partage et la mise à niveau de points de distribution.

- **Collecte des données :**

  Pour permettre au site de destination de collecter des données, vous devez configurer les deux comptes d'accès de site source suivants pour l'utilisation avec chaque site source :

  - **Compte de site source** : ce compte est utilisé pour accéder au fournisseur SMS du site source.
    - Pour un site source Configuration Manager 2007 SP2, ce compte nécessite une autorisation **Lecture** sur tous les objets du site source.
    - Pour un site source System Center 2012 Configuration Manager ou System Center Configuration Manager, ce compte requiert une autorisation **Lecture** sur tous les objets du site source. Pour accorder cette autorisation au compte, vous utilisez l'administration basée sur des rôles. Pour plus d'informations sur l'utilisation de l'administration basée sur des rôles, consultez Principes de base de l'administration basée sur des rôles pour System Center Configuration Manager.
  - **Compte de base de données de site source** : ce compte permet d'accéder à la base de données SQL Server du site source, et nécessite des autorisations **Connect**, **Execute**et **Select** sur la base de données du site source.

  Vous pouvez configurer ces comptes lorsque vous configurez une nouvelle hiérarchie source, la collecte de données d'un site source supplémentaire ou lorsque vous reconfigurez les informations d'identification d'un site source. Ces comptes peuvent utiliser un compte d'utilisateur de domaine, ou vous pouvez définir le compte d'ordinateur du site de niveau supérieur de la hiérarchie de destination.

> **IMPORTANT**
> Si vous utilisez le compte d'ordinateur Configuration Manager pour l'un des comptes d'accès, vérifiez que ce compte est membre du groupe de sécurité **Utilisateurs du modèle COM distribué** dans le domaine du site source.

Lorsque vous collectez des données, les protocoles réseau suivants sont utilisés :

- NetBIOS/SMB - 445 (TCP)
- RPC (WMI) - 135 (TCP)
- SQL Server : les ports TCP utilisés par les bases de données de site source et de destination.

- **Migrer des mises à jour logicielles :**

  Avant de migrer des mises à jour logicielles, vous devez configurer votre hiérarchie de destination avec un point de mise à jour logicielle. Pour plus d'informations, consultez Planification de la migration des mises à jour logicielles.

- **Partager des points de distribution :**

  Pour partager des points de distribution depuis un site source, au moins un site principal ou le site d'administration centrale dans la hiérarchie de destination doit utiliser les mêmes numéros de port pour les demandes des clients que le site source. Pour plus d'informations sur les ports pour les demandes des clients, consultez Comment configurer les ports de communication des clients dans System Center Configuration Manager

  Pour chaque site source, uniquement les points de distribution installés sur les serveurs système de site qui sont configurés avec un nom de domaine complet sont partagés.

  En outre, pour partager un point de distribution depuis un site source System Center 2012 Configuration Manager ou System Center Configuration Manager, le **compte de site source** (qui accède au fournisseur SMS du serveur de site source) doit disposer de l'autorisation **Modifier** sur l'objet **Site** sur le site source. Vous accordez cette autorisation au compte à l'aide de l'administration basée sur les rôles. Pour plus d'informations sur l'utilisation de l'administration basée sur des rôles, consultez Principes de base de l'administration basée sur des rôles pour System Center Configuration Manager.

- **Mettre à niveau ou réaffecter des points de distribution :**

  Le **compte d'accès de site source** configuré pour collecter des données depuis le fournisseur SMS du site source doit disposer des autorisations suivantes :

  - Pour mettre à niveau un point de distribution Configuration Manager 2007, le compte nécessite des autorisations **Lecture**, **Exécuter** et **Supprimer** sur la classe **Site** sur le serveur de site Configuration Manager 2007 afin de pouvoir supprimer correctement le point de distribution du site source Configuration Manager 2007.
  - Pour réattribuer un point de distribution System Center 2012 Configuration Manager ou System Center Configuration Manager, le compte doit avoir l'autorisation **Modifier** sur l'objet **Site** sur le site source. Vous accordez cette autorisation au compte à l'aide de l'administration basée sur les rôles. Pour plus d'informations sur l'utilisation de l'administration basée sur des rôles, consultez Principes de base de l'administration basée sur des rôles pour System Center Configuration Manager.

    Pour mettre à niveau un point de distribution ou le réaffecter à une nouvelle hiérarchie, les ports qui sont configurés pour les demandes clients sur le site qui gère le point de distribution dans la hiérarchie source doivent correspondre aux ports qui sont configurés pour les demandes client sur le site de destination qui gérera le point de distribution. Pour plus d'informations sur les ports pour

les demandes des clients, consultez Comment configurer les ports de communication des clients dans System Center Configuration Manager.

# Listes de vérifications de l'administrateur pour la planification de la migration dans System Center Configuration Manager

22/06/2018 • 16 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez les listes de contrôle de l'administrateur suivantes pour vous aider à planifier votre stratégie de migration vers System Center Configuration Manager.

## Liste de contrôle de l'administrateur pour la planification de la migration

Pour les étapes de planification de la prémigration, utilisez la liste de vérification suivante :

- **Évaluez l'environnement actuel :**

  Identifiez quelles sont les spécifications d'entreprise existantes respectées par la hiérarchie source et élaborez des plans visant à respecter ces spécifications dans la hiérarchie de destination.

- **Passez en revue les fonctionnalités de la version de Configuration Manager que vous utilisez et les modifications qu'elle apporte, puis utilisez ces informations pour concevoir votre hiérarchie de destination :**

  Pour plus d'informations, consultez Principes de base de System Center Configuration Manager et Nouveautés dans System Center Configuration Manager

- **Déterminez le modèle de sécurité administrative à utiliser dans le cadre de l'administration basée sur des rôles :**

  Pour plus d'informations, consultez Principes de base de l'administration basée sur des rôles pour System Center Configuration Manager.

- **Évaluez la topologie de votre réseau et d'Active Directory :** Examinez la structure de votre domaine et la topologie de votre réseau et réfléchissez à la façon dont ceci influence vos tâches de conception et de migration des hiérarchies.

- **Finalisez la conception de votre hiérarchie de destination :**

  Prenez une décision quant au placement d'un site d'administration centrale, de sites principaux, de sites secondaires et d'options de distribution de contenu.

- **Mappez votre hiérarchie aux ordinateurs que vous utiliserez pour les sites et les serveurs de site de la hiérarchie de destination :**

  Identifiez les ordinateurs qui seront utilisés par les sites et les serveurs de système de site de la hiérarchie de destination, puis vérifiez qu'ils disposent d'une capacité suffisante pour respecter les spécifications opérationnelles actuelles et futures.

- **Planifiez votre stratégie de migration d'objets :**

  Planifiez l'utilisation des tâches de migration disponibles pour migrer différents objets (limites de site, regroupements, publications et déploiements). Pour plus d'informations, consultez Types de tâches de

migration dans Planification d’une stratégie pour les tâches de migration dans System Center Configuration Manager

Configuration Manager migre uniquement les objets que vous sélectionnez. Tous les objets qui ne sont pas migrés et qui sont requis dans la hiérarchie de destination doivent être recréés dans cette dernière.

Les objets qui peuvent migrer sont affichés lorsque vous configurez des tâches de migration.

- **Planifiez votre stratégie de migration de clients :**

  Lorsque vous migrez des clients vers la hiérarchie de destination, envisagez d'utiliser une approche contrôlée, qui limite la consommation de la bande passante réseau et des ressources de traitement côté serveur. Pour plus d’informations sur la planification d’une stratégie de migration de client, consultez Planification d’une stratégie de migration de clients dans System Center Configuration Manager.

- **Planifiez les données d’inventaire et de conformité :**

  Configuration Manager ne prend pas en charge la migration des données d’inventaire matériel, d’inventaire logiciel ou de conformité de gestion de la configuration souhaitée pour les mises à jour logicielles ou les clients.

  En revanche, une fois que le client a été migré vers son nouveau site dans la hiérarchie de destination et qu'il a reçu la stratégie relative à ces configurations, il envoie ces informations à son site attribué. Par le biais de cette opération, les données de compatibilité et d'inventaire actuelles sont ajoutées à base de données du site de destination.

- **Planifiez la fin de la migration à partir de la hiérarchie source :**

  Décidez à quel moment les objets et les clients seront migrés. Au terme de la migration, vous pouvez envisager de retirer les serveurs de site de la hiérarchie source.

## Liste de contrôle de l’administrateur pour la migration de la hiérarchie

Utilisez la liste de vérification suivante pour faciliter la planification d'une hiérarchie de destination avant une migration.

- **Identifiez les ordinateurs à utiliser dans la hiérarchie de destination :**

  Configuration Manager ne prend pas en charge une mise à niveau sur place de l’infrastructure Configuration Manager 2007. Vous utilisez alors la migration pour déplacer les données de Configuration Manager 2007 vers System Center Configuration Manager. Ce déplacement vous oblige à utiliser un déploiement côte à côte et à installer System Center Configuration Manager sur de nouveaux ordinateurs.

  De même, quand vous procédez à une migration à partir d’une autre hiérarchie System Center Configuration Manager, vous devez installer une nouvelle hiérarchie de destination qui correspond à un déploiement côte à côte vers votre hiérarchie source.

- **Créez votre hiérarchie de destination :**

  Pour préparer la migration, installez et configurez une hiérarchie de destination System Center Configuration Manager comprenant un site principal. Par exemple :

  - Installez un site d’administration centrale, puis installez au moins un site principal enfant.
  - Si vous ne prévoyez pas d'utiliser un site d'administration centrale, installez un site principal autonome.

- **Si vous souhaitez migrer les informations relatives aux mises à jour logicielles, configurez un point de mise à jour logicielle dans la hiérarchie de destination et synchronisez les mises à jour logicielles :**

Pour pouvoir migrer les informations relatives aux mises à jour logicielles figurant dans la hiérarchie source, vous devez au préalable configurer et synchroniser les mises à jour logicielles dans la hiérarchie de destination.

- **Installez et configurez des rôles système de site supplémentaires dans la hiérarchie de destination :**

  Configurez les rôles de système de site et les systèmes de site supplémentaires dont vous avez besoin.

- **Vérifiez le bon fonctionnement de la hiérarchie de destination :**

  Vérifiez les points suivants :

  - Si la hiérarchie de destination comporte plusieurs sites, vérifiez que la réplication de la base de données entre les sites fonctionne correctement. La réplication de la base de données ne s'applique pas aux sites principaux autonomes.
  - Vérifiez que tous les rôles de système de site installés fonctionnent correctement.
  - Vérifiez que les clients Configuration Manager que vous installez dans la hiérarchie de destination peuvent communiquer avec le site qui leur a été affecté.

## Liste de contrôle de l'administrateur pour la migration

Utilisez la liste de vérification suivante pour migrer les données de la hiérarchie source vers la hiérarchie de destination.

- **Activez la migration dans la hiérarchie de destination :**

  Configurez une hiérarchie source en indiquant le site de niveau supérieur de cette hiérarchie. Pour plus d'informations sur la spécification du site source, consultez Planification d'une stratégie de hiérarchie source dans System Center Configuration Manager.

- **Si la hiérarchie source exécute Configuration Manager 2007 SP2, sélectionnez et configurez des sites supplémentaires dans la hiérarchie source :**

  Pour chacun des sites supplémentaires de la hiérarchie source Configuration Manager 2007 SP2 dont vous souhaitez collecter les données, vous devez configurer des informations d'identification en vue de la collecte de données. Quand vous configurez chaque site source, le processus de collecte de données démarre immédiatement et se poursuit tout au long de la période de migration, jusqu'à ce que vous arrêtiez la collecte de données pour ce site. La collecte de données permet de vérifier que vous pouvez migrer les objets de la hiérarchie source qui ont été ajoutés ou mis à jour depuis la collecte de données précédente.

  > **NOTE**
  > Quand la hiérarchie source exécute System Center 2012 Configuration Manager ou une version ultérieure, il est inutile de configurer des sites sources supplémentaires.

- **Configurez le partage du point de distribution :**

  Vous pouvez partager des points de distribution entre les deux hiérarchies, afin de mettre le contenu des objets que vous migrez à la disposition des clients de la hiérarchie de destination. Ceci garantit que le même contenu reste disponible pour les clients dans les deux hiérarchies et que vous pouvez conserver ce contenu jusqu'à l'arrêt de la collecte de données et la fin de la migration.

  Pour plus d'informations sur les points de distribution partagés, consultez Partager les points de distribution entre les hiérarchies sources et de destination dans Planification d'une stratégie de migration de déploiement de contenu dans System Center Configuration Manager.

- **Créez et exécutez des tâches de migration afin de migrer les objets associés aux clients dans la hiérarchie source :**

  Créez des tâches de migration pour migrer des objets entre des hiérarchies. Les configurations requises pour chaque tâche de migration varient selon les données à migrer.

  Par exemple, lorsque vous migrez du contenu, quelle que soit la tâche de migration utilisée, vous devez attribuer la propriété de la gestion de ce contenu à un site de la hiérarchie de destination. Le site attribué accédera à l'emplacement du fichier source d'origine relatif au contenu et devra distribuer ce contenu auprès des points de distribution de la hiérarchie de destination.

  Pour plus d'informations, consultez Créer et modifier des tâches de migration pour System Center Configuration Manager dans Opérations de migration vers System Center Configuration Manager.

- **Migrez les clients vers la hiérarchie de destination :**

  Le processus de migration des clients dépend de votre scénario de migration :

  - Quand vous migrez des clients qui n'utilisent pas la même version du client que la hiérarchie de destination, vous devez mettre à niveau le logiciel client. La mise à niveau consiste à supprimer le client Configuration Manager actuel, puis à installer la nouvelle version du client, qui correspond à celle du site de destination.

  - Lorsque vous migrez des clients qui utilisent la même version du client que la hiérarchie de destination, le client n'est pas mis à niveau, ni réinstallé. En revanche, il est réattribué à un site principal dans la hiérarchie de destination.

  Lorsque vous migrez un client vers la hiérarchie de destination, le client est associé à ses données, que vous avez précédemment migrées vers cette hiérarchie de destination.

  Pour plus d'informations, voir Planification d'une stratégie de migration de clients dans System Center Configuration Manager.

- **Mettez à niveau ou réaffectez des points de distribution partagés :**

  Quand vous n'avez plus à prendre en charge des clients dans votre hiérarchie source, vous pouvez mettre à niveau des points de distribution partagés depuis un site source Configuration Manager 2007 ou réaffecter des points de distribution partagés à partir d'un site source System Center 2012 Configuration Manager ou System Center Configuration Manager. Lorsque vous mettez à niveau ou réaffectez un point de distribution, le rôle de système de site est transféré vers un site principal de la hiérarchie de destination et le point de distribution est supprimé du site source de la hiérarchie source. Quand vous mettez à niveau ou que vous réaffectez un point de distribution partagé, le contenu reste sur l'ordinateur du point de distribution et vous n'avez pas besoin de redéployer le contenu sur de nouveaux points de distribution de la hiérarchie de destination.

  Vous pouvez également mettre à niveau un point de distribution colocalisé sur un serveur de site secondaire Configuration Manager 2007. Cette opération supprime le site secondaire et conserve un seul point de distribution dans la hiérarchie de destination.

  Pour plus d'informations sur les points de distribution partagés, consultez Partager les points de distribution entre les hiérarchies sources et de destination dans Planification d'une stratégie de migration de déploiement de contenu dans System Center Configuration Manager.

- **Terminez la migration :**

  Une fois que vous avez migré les données et les clients de tous les sites de la hiérarchie source et que vous avez mis à niveau les points de distribution concernés, vous pouvez terminer la migration. Pour cela, vous arrêtez la collecte de données pour tous les sites source de la hiérarchie source. Vous pouvez ensuite supprimer toutes les informations de migration dont vous n'avez pas besoin et retirer l'infrastructure de

votre hiérarchie source. Pour plus d'informations, voir Planification d'une migration complète vers System Center 2012 Configuration Manager.

# Déterminer s'il faut migrer des données vers System Center Configuration Manager

22/06/2018 • 9 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Dans System Center Configuration Manager, la migration offre un moyen de transférer des données et des configurations créées dans des versions de Configuration Manager prises en charge vers votre nouvelle hiérarchie. La migration vous permet d'effectuer les opérations suivantes :

- Combiner plusieurs hiérarchies en une seule.
- Déplacer les données et les configurations d'un déploiement de laboratoire vers votre déploiement de production.
- Déplacer des données et la configuration à partir d'une version antérieure de Configuration Manager, telle que Configuration Manager 2007, qui n'a pas de chemin de mise à niveau vers System Center Configuration Manager, ou à partir de System Center 2012 Configuration Manager (qui prend en charge un chemin de mise à niveau vers System Center Configuration Manager).

À l'exception du rôle de système de site du point de distribution et des ordinateurs hébergeant les points de distribution, aucune infrastructure (sites, rôles de système de site ou ordinateurs hébergeant un rôle de système de site) ne peut être migrée ou transférée, ni partagée entre des hiérarchies.

Il est impossible de migrer l'infrastructure de serveur, mais vous pouvez migrer des clients Configuration Manager entre des hiérarchies. La migration des clients consiste notamment à migrer les données utilisées par les clients à partir de la hiérarchie source vers la hiérarchie de destination, puis à installer ou à réaffecter le logiciel client afin que le client communique ensuite avec la nouvelle hiérarchie.

Une fois qu'un client a été installé dans la nouvelle hiérarchie et qu'il a envoyé ses données, son identifiant Configuration Manager unique permet à Configuration Manager d'associer plus facilement les données que vous avez migrées précédemment avec chaque ordinateur client.

La fonctionnalité fournie par la migration permet de pérenniser les investissements effectués en matière de configurations et de déploiements tout en vous permettant de tirer pleinement parti des principales modifications du produit introduites dans System Center 2012 Configuration Manager et poursuivies dans System Center Configuration Manager. Ces modifications comprennent une hiérarchie Configuration Manager simplifiée qui utilise moins de sites et de ressources ainsi que l'amélioration du traitement avec l'utilisation du code 64 bits natif qui s'exécute sur du matériel 64 bits.

Pour plus d'informations sur les versions de Configuration Manager prises en charge par la migration, consultez Prérequis de la migration dans System Center Configuration Manager.

Les sections suivantes expliquent comment planifier les données que vous pouvez migrer et celles qui ne peuvent pas l'être :

- Données que vous pouvez migrer vers System Center Configuration Manager
- Données que vous ne pouvez pas migrer vers System Center Configuration Manager

## Données que vous pouvez migrer vers System Center Configuration Manager

Le processus de migration peut migrer la plupart des objets entre des hiérarchies Configuration Manager prises en charge. Les instances migrées de certains objets à partir d'une version prise en charge de Configuration Manager 2007 doivent être modifiées, de façon à ce qu'elles respectent le schéma et le format d'objet de System Center 2012 Configuration Manager.

Ces modifications n'affectent pas les données contenues dans la base de données du site source. Les objets migrés à partir d'une version prise en charge de System Center 2012 Configuration Manager ou de System Center Configuration Manager ne nécessitent aucune modification.

Voici des objets qui peuvent migrer en fonction de la version de Configuration Manager utilisée dans la hiérarchie source. Certains objets, telles les requêtes, ne migrent pas. Si vous souhaitez continuer à utiliser ces objets qui ne migrent pas, vous devez les recréer dans la nouvelle hiérarchie. D'autres objets, notamment certaines données des clients, sont recréés automatiquement dans la nouvelle hiérarchie quand vous gérez les clients de cette hiérarchie.

**Objets que vous pouvez migrer à partir de la version Current Branch de System Center Configuration Manager ou de System Center 2012 Configuration Manager**

- Applications pour System Center 2012 Configuration Manager et versions ultérieures
- Environnement virtuel App-V de System Center 2012 Configuration Manager et versions ultérieures
- Personnalisations Asset Intelligence
- Limites
- Regroupements : pour migrer des regroupements à partir d'une version prise en charge de System Center 2012 Configuration Manager ou de System Center Configuration Manager, vous utilisez une tâche de migration d'objets.
- Paramètres de compatibilité :
  - Lignes de base de configuration
  - Éléments de configuration
- Déploiements
- Déploiement de système d'exploitation :
  - Images de démarrage
  - Packages de pilotes
  - Pilotes
  - Images
  - Packages
  - Séquences de tâches
- Résultats de la recherche : critères de recherche enregistrés
- Mises à jour logicielles :
  - Déploiements
  - Packages de déploiement
  - Modèles
  - Listes des mises à jour logicielles
- Packages de distribution de logiciels

- Règles de contrôle de logiciel
- Packages d'application virtuelle

**Objets que vous pouvez migrer à partir de Configuration Manager 2007 SP2**

- Publications
- Applications pour System Center 2012 Configuration Manager et versions ultérieures
- Environnement virtuel App-V de System Center 2012 Configuration Manager et versions ultérieures
- Personnalisations Asset Intelligence
- Limites
- Regroupements : vous migrez des regroupements à partir d'une version prise en charge de Configuration Manager 2007 en utilisant une tâche de migration du regroupement.
- Paramètres de compatibilité (désignés par l'expression « gestion de la configuration souhaitée » dans Configuration Manager 2007) :
  - Lignes de base de configuration
  - Éléments de configuration
- Déploiement de système d'exploitation :
  - Images de démarrage
  - Packages de pilotes
  - Pilotes
  - Images
  - Packages
  - Séquences de tâches
- Résultats de la recherche : dossiers de recherche
- Mises à jour logicielles :
  - Déploiements
  - Packages de déploiement
  - Modèles
  - Listes des mises à jour logicielles
- Packages de distribution de logiciels
- Règles de contrôle de logiciel
- Packages d'application virtuelle

## Données que vous ne pouvez pas migrer vers System Center Configuration Manager

Vous ne pouvez pas migrer les types d'objets suivants :

- Informations de préparation de client AMT

- Fichiers stockés sur les clients, notamment :
  - Données d'inventaire et historique client
  - Fichiers dans le cache du client
- Requêtes
- Droits de sécurité Configuration Manager 2007 et instances pour le site et les objets
- Rapports Configuration Manager 2007 de SQL Server Reporting Services
- Rapports web de Configuration Manager 2007
- Rapports System Center 2012 Configuration Manager et System Center Configuration Manager
- Administration basée sur des rôles System Center 2012 Configuration Manager et System Center Configuration Manager :
  - Rôles de sécurité
  - Étendues de sécurité

# Planifier une stratégie de hiérarchie source dans System Center Configuration Manager

22/06/2018 • 17 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Avant de configurer une tâche de migration dans votre environnement System Center Configuration Manager, vous devez configurer une hiérarchie source et collecter des données depuis au moins un site source de cette hiérarchie. Servez-vous des sections suivantes pour planifier la configuration de hiérarchies sources et de sites sources, ainsi que pour déterminer la manière dont Configuration Manager collecte les informations à partir des sites sources de la hiérarchie source.

## Hiérarchies sources

Une hiérarchie source est une hiérarchie Configuration Manager qui contient les données à migrer. Quand vous configurez la migration et spécifiez une hiérarchie source, vous spécifiez le site de niveau supérieur de cette hiérarchie. Ce site est également appelé un site source. Les sites supplémentaires à partir desquels vous pouvez migrer des données dans la hiérarchie source sont également appelés des sites source.

- Quand vous configurez une tâche de migration pour migrer des données à partir d'une hiérarchie source Configuration Manager 2007, vous la configurez pour migrer les données d'un ou plusieurs sites sources spécifiques de la hiérarchie source.
- Quand vous configurez une tâche de migration pour migrer les données d'une hiérarchie source qui exécute System Center 2012 Configuration Manager ou version ultérieure, vous devez uniquement spécifier le site de niveau supérieur.

Vous pouvez configurer une seule hiérarchie source à la fois.

- Si vous configurez une nouvelle hiérarchie source, cette hiérarchie devient automatiquement la hiérarchie source actuelle et remplace la hiérarchie source précédente.
- Quand vous configurez une hiérarchie source, vous devez spécifier son site de niveau supérieur, ainsi que les informations d'identification nécessaires à Configuration Manager pour se connecter au fournisseur SMS et à la base de données du site source.
- Configuration Manager utilise ces informations d'identification pour collecter des données et récupérer des informations sur les objets et les points de distribution à partir du site source.
- Dans le cadre du processus de collecte des données, les sites enfants de la hiérarchie source sont identifiés.
- Si la hiérarchie source est une hiérarchie Configuration Manager 2007, vous pouvez configurer ces sites supplémentaires comme sites sources, avec des informations d'identification distinctes pour chaque site source.

Même si vous pouvez configurer plusieurs hiérarchies sources successivement, la migration est active pour une seule hiérarchie source à la fois.

- Si vous configurez une hiérarchie source supplémentaire avant d'effectuer la migration à partir de la hiérarchie source actuelle, Configuration Manager annule les tâches de migration actives et reporte les tâches de migration planifiées pour la hiérarchie source actuelle.

- La nouvelle hiérarchie source configurée devient alors la hiérarchie source actuelle, et la hiérarchie source d'origine devient inactive.
- Vous pouvez ensuite configurer les informations d'identification de connexion, les sites sources supplémentaires et les tâches de migration pour la nouvelle hiérarchie source.

Si vous restaurez une hiérarchie source inactive et que vous n'avez pas utilisé **Nettoyer les données de migration** précédemment, vous pouvez afficher les tâches de migration configurées pour cette hiérarchie source. Cependant, avant de pouvoir continuer la migration à partir de cette hiérarchie, vous devez reconfigurer les informations d'identification pour vous connecter à chaque site source applicable et replanifier les tâches de migration qui n'ont pas été terminées.

Caution

Si vous migrez des données à partir de plusieurs hiérarchies source, chaque hiérarchie source supplémentaire doit contenir un ensemble unique de codes de site.

Pour plus d'informations sur la configuration d'une hiérarchie source, consultez Configuration des hiérarchies sources et des sites sources pour la migration vers System Center Configuration Manager

## Sites source

Les sites source sont des sites dans la hiérarchie source qui contiennent des données à migrer. Le site de niveau supérieur de la hiérarchie source est toujours le premier site source. Lorsque la migration collecte des données à partir du premier site source d'une nouvelle hiérarchie source, elle découvre des informations à propos des sites supplémentaires dans cette hiérarchie.

À la fin de la collecte de données du site source initial, les actions suivantes que vous effectuez dépendent de la version du produit de la hiérarchie source.

**Sites sources exécutant Configuration Manager 2007 SP2**

Une fois les données collectées à partir du site source initial de la hiérarchie Configuration Manager 2007 SP2, vous n'avez pas à configurer de sites sources supplémentaires pour créer des tâches de migration. Toutefois, pour pouvoir migrer les données à partir de sites supplémentaires, vous devez configurer les sites supplémentaires comme des sites sources, et System Center Configuration Manager doit collecter les données à partir de ces sites.

Pour collecter des données à partir de sites supplémentaires, vous devez configurer individuellement chaque site comme un site source. Vous devez définir les informations d'identification pour la connexion de System Center Configuration Manager au fournisseur SMS et à la base de données de site de chaque site source. Après avoir configuré les informations d'identification d'un site source, le processus de collecte de données commence pour ce site.

Quand vous configurez des sites sources supplémentaires dans une hiérarchie source Configuration Manager 2007 SP2, vous devez configurer les sites sources du haut vers le bas, ce qui signifie que vous configurez les sites de niveau inférieur en dernier. Vous pouvez configurer des sites sources dans une branche de la hiérarchie à tout moment, mais vous devez configurer un site comme site source pour pouvoir configurer ses sites enfants comme sites sources.

> **NOTE**
> Seuls les sites principaux d'une hiérarchie Configuration Manager 2007 SP2 sont pris en charge pour la migration.

**Sites sources exécutant System Center 2012 Configuration Manager ou version ultérieure**

Une fois les données collectées à partir du site source initial de la hiérarchie System Center 2012 Configuration Manager ou version ultérieure, vous n'avez pas à configurer de sites sources supplémentaires dans cette

hiérarchie source. En effet, contrairement à Configuration Manager 2007, ces versions de Configuration Manager utilisent une base de données partagée qui vous permet d'identifier, puis de migrer tous les objets disponibles à partir du site source initial.

Quand vous configurez les comptes d'accès pour collecter des données, vous devez peut-être accorder l'accès **Compte fournisseur SMS du site source** à plusieurs ordinateurs de la hiérarchie source. Cela peut être nécessaire lorsque le site source prend en charge plusieurs instances du fournisseur SMS, chacune sur un ordinateur différent. Lorsque la collecte des données commence, le site de niveau supérieur de la hiérarchie de destination contacte le site de niveau supérieur de la hiérarchie source pour identifier les emplacements du fournisseur SMS de ce site. Seule la première instance du fournisseur SMS est identifiée. Si le processus de collecte des données ne peut pas accéder au fournisseur SMS à l'emplacement identifié, le processus échoue et ne tente pas de se connecter à d'autres ordinateurs qui exécutent une instance du fournisseur SMS pour le site.

## Collecte des données

Dès que vous avez spécifié une hiérarchie source, configuré les informations d'identification de chaque site source supplémentaire dans une hiérarchie source ou partagé les points de distribution d'un site source, Configuration Manager commence à collecter des données à partir du site source.

La collecte de données se répète ensuite selon une planification simple pour maintenir la synchronisation avec les modifications apportées aux données dans le site source. Par défaut, le processus se répète toutes les quatre heures. Vous pouvez modifier la planification du cycle en modifiant les **Propriétés** du site source. Le processus de collecte de données initial doit vérifier tous les objets de la base de données Configuration Manager, ce qui peut prendre un certain temps. Les processus de collecte de données suivants identifient uniquement les modifications apportées aux données et ils s'exécutent plus rapidement.

Pour collecter des données, le site de niveau supérieur dans la hiérarchie de destination se connecte au fournisseur SMS et à la base de données du site source pour récupérer une liste d'objets et les points de distribution. Ces connexions utilisent les comptes d'accès de site source. Pour plus d'informations sur les configurations nécessaires pour la collecte des données, consultez Prérequis de la migration dans System Center Configuration Manager.

Vous pouvez démarrer et arrêter le processus de collecte des données à l'aide de **Collecter les données maintenant** et **Arrêter la collecte de données** dans la console Configuration Manager.

Une fois que vous avez utilisé **Arrêter la collecte de données** pour un site source pour une raison quelconque, vous devez reconfigurer les informations d'identification du site pour pouvoir collecter à nouveau les données de ce site. Configuration Manager ne peut pas identifier les nouveaux objets ni les modifications apportées aux objets migrés tant que vous ne reconfigurez pas le site source.

> **NOTE**
> Avant de développer un site principal autonome dans une hiérarchie avec un site d'administration centrale, vous devez arrêter toutes les collectes des données. Vous pouvez reconfigurer la collecte des données quand le développement du site est terminé.

### Collecter les données maintenant

Après l'exécution du processus initial de collecte des données d'un site, le processus se répète pour identifier les objets mis à jour depuis le dernier cycle de collecte des données. Vous pouvez également utiliser l'action **Collecter les données maintenant** dans la console Configuration Manager pour démarrer immédiatement le processus et réinitialiser l'heure de début du cycle suivant.

Lorsqu'un processus de collecte de données aboutit pour un site source, vous pouvez partager les points de distribution à partir du site source et configurer des tâches de migration pour migrer les données depuis le site. La collecte des données est un processus répétitif pour la migration et il se poursuit jusqu'à ce que vous

changiez la hiérarchie source ou utilisiez **Arrêter la collecte de données** pour mettre fin au processus de collecte des données du site.

**Arrêter la collecte de données**

Vous pouvez utiliser **Arrêter la collecte de données** pour mettre fin à la collecte des données d'un site source quand vous ne souhaitez plus que Configuration Manager identifie les objets nouveaux et modifiés du site. Cette action empêche également Configuration Manager de proposer aux clients de la hiérarchie de destination des points de distribution partagés de la source en tant qu'emplacements pour le contenu que vous avez migré.

Pour arrêter la collecte des données de chaque site source, vous devez exécuter **Arrêter la collecte de données** sur les sites sources de niveau inférieur, puis répéter le processus sur chaque site parent. Le site de niveau supérieur de la hiérarchie source doit être le dernier site sur lequel vous arrêtez la collecte des données. Vous devez arrêter la collecte des données sur chaque site enfant avant d'effectuer cette action sur un site parent. En règle générale, vous arrêtez la collecte de données uniquement lorsque vous êtes prêt à exécuter le processus de migration.

Quand vous arrêtez la collecte des données d'un site source, les informations collectées précédemment sur les objets et les regroupements du site peuvent toujours être utilisées quand vous configurez de nouvelles tâches de migration. Toutefois, vous ne voyez pas les nouveaux objets ou regroupements, ni les modifications apportées aux objets existants. Si vous reconfigurez le site source et recommencez à collecter les données, vous voyez les informations et l'état des objets précédemment migrés.

# Planifier une stratégie pour les tâches de migration dans System Center Configuration Manager

22/06/2018 • 33 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez des tâches de migration pour configurer les données spécifiques que vous souhaitez migrer vers votre environnement System Center Configuration Manager. Les tâches de migration identifient les objets que vous envisagez de migrer, et elles s'exécutent sur le site de niveau supérieur dans votre hiérarchie de destination. Vous pouvez configurer une ou plusieurs tâches de migration par site source. Ceci vous permet de migrer tous les objets simultanément ou des sous-ensembles limités de données avec chaque tâche.

Vous pouvez créer des tâches de migration une fois que Configuration Manager a collecté avec succès les données d'un ou de plusieurs sites à partir de la hiérarchie source. Vous pouvez migrer des données dans n'importe quel ordre à partir des sites source contenant des données. Avec un site source Configuration Manager 2007, vous ne pouvez migrer les données qu'à partir du site où un objet a été créé. Avec les sites sources exécutant System Center 2012 Configuration Manager ou ultérieur, toutes les données que vous pouvez migrer sont disponibles sur le site de plus haut niveau de la hiérarchie source.

Avant de migrer des clients entre hiérarchies, vérifiez que les objets que les clients utilisent ont été migrés et que ces objets sont disponibles dans la hiérarchie de destination. Par exemple, quand vous migrez depuis une hiérarchie source Configuration Manager 2007 SP2, vous pouvez recevoir une publication pour du contenu déployé sur un regroupement personnalisé qui a un client. Dans ce cas, nous vous recommandons de migrer le regroupement, la publication et le contenu associé avant de migrer le client. Ces données ne peut pas être associées au client dans la hiérarchie de destination si le contenu, le regroupement et la publication ne sont pas migrés avant la migration du client. Si un client n'est pas associé aux données liées à une publication et à un contenu exécutés précédemment, le contenu peut être proposé au client pour l'installation dans la hiérarchie de destination, ce qui peut être inutile. Si le client est migré après la migration des données, il est associé à ce contenu et à cette publication, et sauf si la publication est récurrente, le contenu n'est plus proposé pour la publication migrée.

Pour certains objets, la migration des données de la hiérarchie source vers la hiérarchie de destination ne suffit pas. Par exemple, pour pouvoir migrer les mises à jour logicielles des clients vers votre hiérarchie de destination, vous devez déployer un point de mise à jour logicielle actif, configurer le catalogue des produits et synchroniser le point de mise à jour logicielle avec WSUS (Windows Server Update Services) dans la hiérarchie de destination.

Utilisez les sections suivantes pour planifier vos tâches de migration.

- Types de tâche de migration
- Planification générale de toutes les tâches de migration
- Planification des tâches de migration de regroupements
- Planification des tâches de migration d'objets
- Planification des tâches de migration d'objets déjà migrés

## Types de tâches de migration

Configuration Manager prend en charge les types de tâche de migration suivants. Chaque type de tâche est conçu pour vous aider à définir les objets que vous pouvez inclure dans cette tâche.

**Migration de regroupements** (prise en charge uniquement pour la migration depuis Configuration Manager 2007 SP2) : Migre les objets liés aux regroupements de votre choix. Par défaut, la migration d'un regroupement inclut tous les objets qui sont associés aux membres du regroupement. Vous pouvez exclure des instances d'objet spécifiques lors de l'utilisation d'une tâche de migration de regroupement.

**Migration d'objets** : Migre des objets individuels de votre choix. Vous sélectionnez uniquement les données à migrer.

**Migration d'objets déjà migrés** : Migre les objets que vous avez déjà migrés, quand ces objets ont été mis à jour dans la hiérarchie source après leur dernière migration.

#### Objets que vous pouvez migrer

Tous les objets ne peuvent pas migrer en fonction du type de tâche de migration. La liste suivant indique le type des objets que vous pouvez migrer à l'aide de chaque type de tâche de migration.

> **NOTE**
> Les tâches de migration de regroupements sont disponibles uniquement quand vous migrez des objets à partir d'une hiérarchie source Configuration Manager 2007 SP2.

#### Types de tâche que vous pouvez utiliser pour migrer chaque objet

- **Publications** (disponibles pour une migration à partir des sites sources Configuration Manager 2007 pris en charge)
  - Migration du regroupement
- **Catalogue Asset Intelligence**
  - Migration d'objet
  - Migration d'objets migrés précédemment
- **Configuration matérielle requise pour Asset Intelligence**
  - Migration d'objet
  - Migration d'objets migrés précédemment
- **Liste de logiciels Asset Intelligence**
  - Migration d'objet
  - Migration d'objets migrés précédemment
- **Limites**
  - Migration d'objet
  - Migration d'objets migrés précédemment
- **Bases de référence de configuration**
  - Migration du regroupement
  - Migration d'objet
  - Migration d'objets migrés précédemment
- **Éléments de configuration**
  - Migration du regroupement

- Migration d'objet
- Migration d'objets migrés précédemment

- **Fenêtres de maintenance**
  - Migration du regroupement
- **Images de démarrage de déploiement du système d’exploitation**
  - Migration du regroupement
  - Migration d'objet
  - Migration d'objets migrés précédemment
- **Packages de pilotes de déploiement du système d’exploitation**
  - Migration du regroupement
  - Migration d'objet
  - Migration d'objets migrés précédemment
- **Pilotes de déploiement du système d’exploitation**
  - Migration du regroupement
  - Migration d'objet
  - Migration d'objets migrés précédemment
- **Images de déploiement du système d’exploitation**
  - Migration du regroupement
  - Migration d'objet
  - Migration d'objets migrés précédemment
- **Packages de déploiement du système d’exploitation**
  - Migration du regroupement
  - Migration d'objet
  - Migration d'objets migrés précédemment
- **Packages de distribution de logiciels**
  - Migration du regroupement
  - Migration d'objet
  - Migration d'objets migrés précédemment
- **Règles de contrôle de logiciel**
  - Migration d'objet
  - Migration d'objets migrés précédemment
- **Packages de déploiement de mises à jour logicielles**
  - Migration du regroupement
  - Migration d'objet

    - Migration d'objets migrés précédemment
- **Modèles de déploiement de mises à jour logicielles**
    - Migration du regroupement
    - Migration d'objet
    - Migration d'objets migrés précédemment
- **Déploiements de mises à jour logicielles**
    - Migration du regroupement
- **Listes de mises à jour logicielles**
    - Migration d'objet
    - Migration d'objets migrés précédemment
- **Séquences de tâches**
    - Migration du regroupement
    - Migration d'objet
    - Migration d'objets migrés précédemment
- **Packages d'applications virtuelles**
    - Migration du regroupement
    - Migration d'objet

> **IMPORTANT**
> Bien que vous puissiez migrer un package d'application virtuelle en utilisant la migration d'objet, vous ne pouvez pas le migrer en utilisant le type de tâche de migration **Migration d'objets migrés précédemment**. Vous devez plutôt supprimer le package d'application virtuelle migré du site de destination, puis créer une tâche de migration pour migrer l'application virtuelle.

## Planification générale de toutes les tâches de migration

Utilisez l'Assistant Création de tâche de migration pour créer une tâche de migration pour migrer des objets vers votre hiérarchie de destination. Le type de tâche de migration que vous créez détermine les objets pouvant être migrés. Vous pouvez créer et utiliser plusieurs tâches de migration pour migrer des données à partir du même site source ou de plusieurs sites source. L'utilisation d'un type de tâche de migration n'empêche pas l'utilisation d'un autre type de tâche de migration.

Une fois la tâche de migration exécutée, son état devient **Terminé** , et vous ne pouvez plus la réexécuter. Toutefois, vous pouvez créer une tâche de migration pour migrer les objets migrés par la tâche d'origine, sans compter que la nouvelle tâche de migration peut inclure des objets supplémentaires également. Quand vous créez des tâches de migration supplémentaires, les objets déjà migrés s'affichent avec l'état **Migré**. Vous pouvez sélectionner ces objets pour les migrer à nouveau, mais si les objets n'ont pas été mis à jour dans la hiérarchie source, il est inutile de les migrer à nouveau. Si un objet a été mis à jour dans la hiérarchie source après sa migration, vous pouvez identifier l'objet lorsque vous utilisez le type de tâche de migration **Objets modifiés après la migration**.

Vous pouvez supprimer une tâche de migration avant son exécution. Cependant, une fois qu'une tâche de migration a été effectuée, elle reste visible dans la console Configuration Manager et ne peut pas être supprimée. Chaque tâche de migration terminée ou qui n'a pas encore été exécutée reste visible dans la console

Configuration Manager jusqu'à ce que le processus de migration soit fini et que vous ayez nettoyé les données de migration.

> **NOTE**
> Après avoir terminé la migration en utilisant l'action **Nettoyer les données de migration**, vous pouvez reconfigurer la même hiérarchie comme hiérarchie source active pour restaurer la visibilité des objets précédemment migrés.

Pour afficher les objets contenus dans une tâche de migration au sein de la console Configuration Manager, sélectionnez la tâche de migration, puis choisissez l'onglet **Objets dans la tâche**.

Utilisez les informations dans les sections suivantes pour planifier toutes les tâches de migration.

### Sélection de données

Lorsque vous créez une tâche de migration de regroupement, vous devez sélectionner au moins un regroupement. Une fois les regroupements sélectionnés, l'Assistant Création de tâche de migration affiche les objets associés aux regroupements. Par défaut, tous les objets associés aux regroupements sélectionnés sont migrés, mais vous pouvez désélectionner les objets à ne pas migrer avec cette tâche. Quand vous désélectionnez un objet qui a des objets dépendants, ces derniers sont également désélectionnés. Tous les objets désélectionnés sont ajoutés à une liste d'exclusion. Les objets dans une liste d'exclusion sont éliminés de la sélection automatique pour les prochaines tâches de migration. Vous devez modifier manuellement la liste d'exclusion pour supprimer les objets qui doivent être sélectionnés automatiquement pour les tâches de migration suivantes.

### Propriétaire de site pour le contenu migré

Lorsque vous migrez du contenu pour des déploiements, vous devez attribuer l'objet de contenu à un site dans la hiérarchie de destination. Ce site devient alors le propriétaire de ce contenu dans la hiérarchie de destination. Bien que le site de niveau supérieur de votre hiérarchie de destination soit le site qui migre les métadonnées du contenu, c'est le site attribué qui accède aux fichiers source d'origine du contenu dans le réseau.

Pour réduire la bande passante réseau utilisée lors de la migration, transférez la propriété du contenu au site disponible le plus proche. Dans la mesure où les informations sur le contenu sont partagées globalement dans System Center Configuration Manager, elles sont disponibles sur tous les sites.

Les informations sur le contenu sont partagées avec tous les sites de la hiérarchie de destination en utilisant la réplication de base de données. Cependant, le contenu que vous affectez à un site principal puis que vous déployez sur des points de distribution sur d'autres sites principaux est transféré via la réplication basée sur les fichiers. Ce transfert est routé via le site administration centrale, puis vers chaque site principal supplémentaire. En centralisant les packages que vous prévoyez de distribuer sur plusieurs sites principaux avant la migration ou au cours de la migration quand vous définissez un site comme propriétaire du contenu, vous pouvez réduire les transferts de données sur les réseaux à faible bande passante.

### Étendues de sécurité de l'administration basée sur des rôles pour les données migrées

Lorsque vous migrez des données vers une hiérarchie de destination, vous devez affecter une ou plusieurs étendues de sécurité d'administration basée sur des rôles aux objets dont les données sont migrées. Ainsi, seuls les utilisateurs administratifs appropriés peuvent accéder à ces données après la migration. Les étendues de sécurité que vous spécifiez sont définies par la tâche de migration et sont appliquées à chaque objet migré par cette tâche. Si vous voulez appliquer des étendues de sécurité différentes à différents ensembles d'objets et affecter ces étendues au cours de la migration, vous devez migrer les différents ensembles d'objets en utilisant différentes tâches de migration.

Avant de configurer une tâche de migration, vérifiez comment l'administration basée sur des rôles fonctionne dans System Center Configuration Manager. Si nécessaire, configurez une ou plusieurs étendues de sécurité pour les données à migrer pour définir les utilisateurs autorisés à accéder aux objets migrés dans la hiérarchie de destination.

Pour plus d'informations sur les étendues de sécurité et l'administration basée sur des rôles, consultez Principes de base de l'administration basée sur des rôles pour System Center Configuration Manager.

**Vérification des actions de migration**

Quand vous configurez une tâche de migration, l'Assistant Création de tâche de migration affiche une liste des actions à effectuer pour garantir la réussite de la migration, ainsi qu'une liste des actions entreprises par Configuration Manager pendant la migration des données sélectionnées. Lisez attentivement ces informations pour vérifier le résultat attendu.

**Planifier des tâches de migration**

Par défaut, une tâche de migration s'exécute immédiatement après sa création. Vous pouvez cependant spécifier le moment d'exécution de la tâche de migration quand vous créez la tâche ou en modifiant les propriétés de la tâche. Vous pouvez planifier l'exécution de la tâche de migration comme suit :

- Exécuter la tâche maintenant
- Exécuter la tâche à une heure de début spécifique
- Ne pas exécuter la tâche

**Spécifier la résolution des conflits de données migrées**

Par défaut, les tâches de migration ne remplacent pas les données dans la base de données de destination, sauf si vous configurez la tâche de migration pour qu'elle ignore ou remplace les données déjà migrées vers la base de données de destination.

## Planifier des tâches de migration de regroupements

Les tâches de migration de regroupements sont disponibles uniquement quand vous migrez des données à partir d'une hiérarchie source qui exécute une version prise en charge de Configuration Manager 2007. Vous devez spécifier un ou plusieurs regroupements à migrer lorsque vous utilisez la migration basée sur le regroupement. Pour chaque regroupement que vous spécifiez, la tâche de migration sélectionne automatiquement tous les objets associés pour les migrer. Par exemple, si vous sélectionnez un regroupement d'utilisateurs, les membres du regroupement sont identifiés et vous pouvez migrer les déploiements associés au regroupement. Vous pouvez également sélectionner d'autres objets de déploiement à migrer associés à ces membres. Tous ces éléments sélectionnés sont ajoutés à la liste des objets qui peuvent être migrés.

Quand vous migrez un regroupement, System Center Configuration Manager migre également les paramètres du regroupement, notamment les fenêtres de maintenance et les variables du regroupement. Il ne peut cependant pas migrer les paramètres du regroupement pour l'approvisionnement du client AMT.

Utilisez les informations des sections suivantes pour découvrir les configurations supplémentaires qui peuvent s'appliquer aux tâches de migration basées sur le regroupement.

**Exclure des objets d'une tâche de migration de regroupement**

Vous pouvez exclure des objets d'une tâche de migration de regroupement. Quand vous excluez un objet d'une tâche de migration de regroupement, l'objet est ajouté à une liste d'exclusion globale qui contient tous les objets que vous avez exclus des tâches de migration créées pour un site source dans la hiérarchie source actuelle. Les objets dans la liste d'exclusion peuvent toujours être migrés dans les tâches suivantes, mais ils ne sont pas inclus automatiquement lorsque vous créez une tâche de migration basée sur le regroupement.

Vous pouvez modifier la liste d'exclusion pour supprimer des objets que vous avez exclus. Lorsque vous supprimez un objet de la liste d'exclusion, il est automatiquement sélectionné lorsqu'un regroupement associé est défini lors de la création d'une tâche de migration.

**Regroupements non pris en charge**

Configuration Manager peut migrer les regroupements d'utilisateurs par défaut, les regroupements d'appareils et

la plupart des regroupements personnalisés à partir d'une hiérarchie source Configuration Manager 2007. Toutefois, Configuration Manager ne peut pas migrer les regroupements qui contiennent des utilisateurs et des appareils dans le même regroupement.

Vous ne pouvez pas migrer les regroupements suivants :

- Un regroupement qui contient des utilisateurs et des appareils.
- Un regroupement qui contient une référence à un regroupement correspondant à un type de ressource différent. tel qu'un regroupement de périphériques ayant un sous-regroupement ou un lien à un regroupement d'utilisateurs. Dans cet exemple, seul le regroupement de plus haut niveau migre.
- Un regroupement qui contient une règle pour inclure des ordinateurs inconnus. Le regroupement est migré, mais la règle d'inclusion d'ordinateurs inconnus n'est pas migrée.

**Regroupements vides**

Un regroupement vide est un regroupement qui n'a aucune ressource associée. Quand Configuration Manager migre un regroupement vide, il convertit le regroupement en un dossier d'organisation qui ne contient aucun utilisateur ou appareil. Ce dossier est créé avec le nom du regroupement vide sous le nœud **Regroupements d'utilisateurs** ou **Regroupements de périphériques** dans l'espace de travail **Ressources et Conformité** de la console Configuration Manager.

**Regroupements liés et sous-regroupements**

Quand vous migrez des regroupements liés à d'autres regroupements ou ayant des sous-regroupements, Configuration Manager crée un dossier sous le nœud **Regroupements d'utilisateurs** ou **Regroupements d'appareils** en plus des regroupements et sous-regroupements liés.

**Dépendances de regroupements et inclusion d'objets**

Quand vous spécifiez un regroupement à migrer dans l'Assistant Création de tâche de migration, tous les regroupements qui en dépendent sont automatiquement sélectionnés pour être inclus dans la tâche. Ce comportement garantit que toutes les ressources nécessaires sont disponibles après la migration.

Par exemple, vous sélectionnez un regroupement pour les appareils qui exécutent Windows 7 et qui est nommé **Win_7**. Ce regroupement est limité à un regroupement contenant tous vos systèmes d'exploitation clients, nommé **All_Clients**. Le regroupement **All_Clients** sera automatiquement sélectionné pour la migration.

**Limitation au regroupement**

Avec System Center Configuration Manager, les regroupements sont des données globales et sont évalués au niveau de chaque site de la hiérarchie. Par conséquent, pensez à limiter l'étendue d'un regroupement après sa migration. Pendant la migration, vous pouvez identifier un regroupement à partir de la hiérarchie de destination à utiliser pour limiter l'étendue du regroupement que vous migrez, de sorte que le regroupement migré n'inclut pas de membres imprévus.

Par exemple, dans Configuration Manager 2007, les regroupements sont évalués au niveau du site qui les crée et au niveau des sites enfants. Une publication peut être déployée vers un site enfant seulement, et cela limiterait l'étendue de cette publication à ce site enfant. En comparaison, avec System Center Configuration Manager, les regroupements sont évalués au niveau de chaque site, et les publications associées sont ensuite évaluées pour chaque site. La limitation au regroupement vous permet d'affiner les membres du regroupement à partir d'un autre regroupement afin d'éviter l'ajout de membres du regroupement imprévus.

**Remplacement du code de site**

Quand vous migrez un regroupement ayant des critères qui identifient un site Configuration Manager 2007, vous devez spécifier un site spécifique dans la hiérarchie de destination. Cela garantit que le regroupement migré reste fonctionnel dans votre environnement de destination et que son étendue n'augmente pas.

**Spécifier le comportement pour les publications migrées**

Par défaut, les tâches de migration basée sur des regroupements désactivent les publications qui migrent vers la hiérarchie de destination. Cela inclut tous les programmes qui sont associés à la publication. Quand vous créez une tâche de migration basée sur un regroupement qui a des publications, l'option **Activer les programmes à déployer dans Configuration Manager après la migration d'une publication** apparaît dans la page **Paramètres** de l'Assistant Création de tâche de migration. Si vous sélectionnez cette option, les programmes associés aux publications sont activés après qu'ils ont migré. Au titre des bonnes pratiques, ne sélectionnez pas cette option. Au lieu de cela, activez les programmes une fois qu'ils ont migré quand vous pouvez vérifier les clients qui les recevront.

> **NOTE**
> L'option **Activer les programmes à déployer dans Configuration Manager après la migration d'une publication** s'affiche uniquement quand vous créez une tâche de migration basée sur un regroupement et quand la tâche de migration contient des publications.

Pour activer un programme après la migration, décochez **Désactiver ce programme sur les ordinateurs qui le publient** sous l'onglet **Avancé** des propriétés du programme.

## Planifier des tâches de migration d'objets

Contrairement à la migration des regroupements, vous devez sélectionner chaque objet et instance d'objet que vous souhaitez migrer. Vous pouvez sélectionner des objets individuels (comme les publications d'une hiérarchie Configuration Manager 2007, ou une publication d'une hiérarchie System Center 2012 Configuration Manager ou System Center Configuration Manager) à ajouter à la liste d'objets à migrer pour une tâche de migration spécifique. Tous les objets que vous n'ajoutez pas à la liste de migration ne sont pas migrés vers le site de destination par la tâche de migration d'objet.

Les tâches de migration basées sur un objet ne sont associées à aucune autre configuration supplémentaire à planifier au-delà de celles applicables à toutes les tâches de migration.

## Planifier des tâches de migration d'objets déjà migrés

Si un objet que vous avez déjà migré vers la hiérarchie de destination est mis à jour dans la hiérarchie source, vous pouvez migrer de nouveau l'objet en utilisant le type de tâche **Objets modifiés après la migration** . Par exemple, quand vous renommez ou que vous mettez à jour les fichiers source d'un package dans la hiérarchie source, la version du package est incrémentée dans la hiérarchie source. Après l'incrémentation de version du package, le package peut être identifié pour la migration par ce type de tâche.

Ce type de tâche est similaire au type de migration d'objet, à l'exception du fait que lorsque vous sélectionnez des objets à migrer, vous pouvez choisir uniquement parmi des objets qui ont été mis à jour après avoir été migrés par une tâche de migration précédente.

Quand vous sélectionnez ce type de tâche, le comportement de résolution des conflits sur la page **Paramètres** de l'Assistant Création de tâche de migration est configuré pour remplacer les objets précédemment migrés. Ce paramètre ne peut pas être modifié.

> **NOTE**
> Cette tâche de migration peut identifier les objets qui sont automatiquement mis à jour par hiérarchie source, en plus des objets mis à jour par un utilisateur administratif.

# Planifier une stratégie de migration de clients dans System Center Configuration Manager

22/06/2018 • 12 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Pour migrer des clients de la hiérarchie source vers une hiérarchie de destination System Center Configuration Manager, vous devez effectuer deux tâches. Vous devez migrer les objets qui sont associés au client et vous devez réinstaller ou réaffecter les clients depuis la hiérarchie source à la hiérarchie de destination. Vous migrez tout d'abord les objets pour qu'ils soient disponibles lorsque les clients sont migrés. Les objets associés au client sont migrés à l'aide de tâches de migration. Pour plus d'informations sur la migration des objets associés au client, consultez Planification d'une stratégie pour les tâches de migration dans System Center Configuration Manager.

Utilisez les sections suivantes pour planifier la migration des clients vers la hiérarchie de destination.

- Planifier la migration des clients vers la hiérarchie de destination
- Planifier la gestion des données conservées sur les clients pendant la migration
- Planifier les données d'inventaire et de compatibilité pendant la migration

## Planifier la migration des clients vers la hiérarchie de destination

Quand vous migrez des clients d'une hiérarchie source, le logiciel client sur l'ordinateur client est mis à niveau avec la version du produit de la hiérarchie de destination.

- **Hiérarchie source Configuration Manager 2007** : quand vous migrez des clients à partir d'une hiérarchie source qui exécute une version prise en charge de Configuration Manager, le logiciel client est mis à niveau vers la version cliente de la hiérarchie de destination.
- **Hiérarchie source System Center 2012 Configuration Manager ou version ultérieure** : quand vous migrez des clients entre des hiérarchies avec la même version de produit, le logiciel client ne change pas ou ne se met pas à niveau. Le client est simplement réaffecté depuis la hiérarchie source vers un site de la hiérarchie de destination.

  > **NOTE**
  > Lorsque la version de produit d'une hiérarchie n'est pas prise en charge pour migration vers votre hiérarchie de destination, mettez à niveau tous les sites et les clients dans la hiérarchie source vers une version de produit compatible. Une fois la hiérarchie source mise à niveau vers une version de produit prise en charge, vous pouvez effectuer la migration entre hiérarchies. Pour plus d'informations, consultez Versions de Configuration Manager prises en charge pour la migration dans Prérequis de la migration dans System Center Configuration Manager.

Tenez compte des informations suivantes pour planifier la migration des clients :

- Pour mettre à niveau ou réaffecter des clients d'un site source vers un site de destination, vous pouvez utiliser une méthode de déploiement client prise en charge pour le déploiement de clients dans la hiérarchie de destination. Les méthodes de déploiement client classiques comprennent l'installation poussée du client, la distribution de logiciels, la stratégie de groupe et l'installation du logiciel client basé sur la mise à jour. Pour plus d'informations, consultez Méthodes d'installation du client dans System

Center Configuration Manager.

- Assurez-vous que l'appareil sur lequel s'exécute le logiciel client dans la hiérarchie source présente la configuration matérielle minimale requise et exécute un système d'exploitation pris en charge par la version de Configuration Manager utilisée dans la hiérarchie de destination.
- Avant de migrer un client, exécutez une tâche de migration pour migrer les informations que le client va utiliser dans la hiérarchie de destination.
- Les clients mis à niveau conservent leur historique d'exécution pour les déploiements. Cela évite d'avoir à réexécuter inutilement des déploiements dans la hiérarchie de destination.
  - Pour les clients Configuration Manager 2007, l'historique d'exécution de publication est conservé.
  - Pour les clients à partir de System Center 2012 Configuration Manager ou System Center Configuration Manager, l'historique d'exécution des déploiements est conservé.
- Vous pouvez migrer les clients à partir de sites de la hiérarchie source dans l'ordre de votre choix. Toutefois, migrez un nombre limité de clients en plusieurs étapes au lieu de migrer un grand nombre de clients simultanément. Une migration progressive réduit les besoins en bande passante et le traitement du serveur lorsque chaque client qui vient d'être mis à niveau envoie son inventaire complet initial et ses données de compatibilité au site qui lui est affecté.
- Quand vous migrez des clients Configuration Manager 2007, le logiciel client existant est désinstallé de l'ordinateur client et le nouveau logiciel client y est installé.
- Configuration Manager ne peut pas migrer un client Configuration Manager 2007 sur lequel est installé le client App-V, sauf si la version de ce dernier est la version 4.6 SP1 ou une version ultérieure.

Vous pouvez surveiller le processus de migration du client dans le nœud **Migration** de l'espace de travail **Administration** dans la console Configuration Manager.

Après la migration du client vers la hiérarchie de destination, vous ne pouvez plus gérer cet appareil dans votre hiérarchie source et vous devez supprimer le client de la hiérarchie source. Bien que cette action ne soit pas obligatoire dans le cadre du processus de migration des hiérarchies, elle peut empêcher l'identification d'un client migré dans un rapport de hiérarchie source ou un nombre incorrect de ressources entre les deux hiérarchies au cours de la migration. Par exemple, lorsqu'un client migré reste dans la base de données du site source, vous pourriez exécuter un rapport de mises à jour logicielles qui identifie incorrectement l'ordinateur comme ressource non gérée alors qu'il est géré par la hiérarchie de destination.

## Planifier la gestion des données conservées sur les clients pendant la migration

Lorsque vous migrez un client de sa hiérarchie source vers la hiérarchie de destination, certaines informations sont conservées sur le périphérique, alors que d'autres ne sont pas disponibles sur le périphérique après la migration.

Les informations suivantes sont conservées sur le périphérique client :

- L'identificateur unique (GUID) qui associe un client à ses informations dans la base de données Configuration Manager.
- L'historique de publication ou de déploiement qui empêche les clients de ré exécuter inutilement des publications ou des déploiements dans la hiérarchie de destination.

Les informations suivantes ne sont pas conservées sur le périphérique client :

- Fichiers dans le cache du client. Si le client requiert ces fichiers pour installer le logiciel, il les télécharge à

nouveau depuis la hiérarchie de destination.

- Informations de la hiérarchie source à propos de publications ou déploiements qui n'ont pas encore été exécutés. Si vous souhaitez que le client exécute des publications ou des déploiements après la migration, vous devez les redéployer vers le client dans la hiérarchie de destination.
- Informations sur l'inventaire. Le client renvoie ces informations à son site attribué dans la hiérarchie de destination après la migration du client et la génération des nouvelles données du client.
- Données de compatibilité. Le client renvoie ces informations à son site attribué dans la hiérarchie de destination après la migration du client et la génération des nouvelles données du client.

Quand un client migre, les informations stockées dans le chemin du Registre et des fichiers du client Configuration Manager ne sont pas conservées. Après la migration, réappliquez ces paramètres. Les paramètres types sont les suivants :

- Modes de gestion de l'alimentation
- Paramètres de journalisation
- Paramètres de stratégie locale

En outre, il peut être nécessaire de réinstaller certaines applications.

## Planifier les données d’inventaire et de compatibilité pendant la migration

Les données d'inventaire et de compatibilité client ne sont pas enregistrées lorsque vous migrez un client vers la hiérarchie de destination. En revanche, ces informations sont recréées dans la hiérarchie de destination lorsqu'un client envoie pour la première fois les informations à son site affecté. Pour réduire les besoins en bande passante et le traitement du serveur, ne migrez pas tous les clients en même temps, mais en plusieurs étapes.

En outre, vous ne pouvez pas migrer des personnalisations d'inventaire matériel à partir d'une hiérarchie source. Vous devez les introduire dans la hiérarchie de destination indépendamment de la migration. Pour plus d’informations sur la manière d’étendre l’inventaire matériel, consultez Guide pratique pour configurer l’inventaire matériel dans System Center Configuration Manager.

# Planifier une stratégie de migration de déploiement de contenu dans System Center Configuration Manager

22/06/2018 • 48 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Durant le processus de migration des données vers une hiérarchie de destination System Center Configuration Manager, les clients Configuration Manager des hiérarchies source et de destination peuvent conserver l'accès au contenu que vous avez déployé dans la hiérarchie source. Vous pouvez aussi utiliser la migration pour mettre à niveau ou réaffecter des points de distribution de la hiérarchie source afin qu'ils deviennent des points de distribution dans la hiérarchie de destination. Lorsque vous partagez et mettez à niveau ou réaffectez des points de distribution, cette stratégie permet d'éviter d'avoir à redéployer du contenu vers de nouveaux serveurs dans la hiérarchie de destination pour les clients dont vous effectuez la migration.

Bien que vous puissiez recréer et distribuer le contenu dans la hiérarchie de destination, vous pouvez également utiliser les options suivantes pour gérer ce contenu :

- Partagez des points de distribution dans la hiérarchie source avec des clients dans la hiérarchie de destination.
- Mettez à niveau les points de distribution Configuration Manager 2007 autonomes ou les sites secondaires Configuration Manager 2007 dans la hiérarchie source pour qu'ils deviennent des points de distribution dans la hiérarchie de destination.
- Réaffectez les points de distribution d'une hiérarchie source System Center Configuration Manager à un site de la hiérarchie de destination.

Utilisez les sections suivantes pour vous aider à planifier le déploiement de contenu pendant la migration :



## Partager des points de distribution entre une hiérarchie source et une hiérarchie de destination

Lors de la migration, vous pouvez partager les points de distribution d'une hiérarchie source avec la hiérarchie de destination. Vous pouvez utiliser des points de distribution partagés pour rendre le contenu migré à partir d'une hiérarchie source immédiatement accessible aux clients situés dans la hiérarchie de destination sans avoir à recréer ce contenu ni à le redistribuer vers de nouveaux points de distribution dans la hiérarchie de destination. Lorsque les clients situés dans la hiérarchie de destination demandent le contenu déployé sur les points de distribution que vous avez partagés, ces points de distribution partagés peuvent être proposés aux clients

comme emplacements de contenu valides.

En plus de constituer un emplacement de contenu valide pour les clients dans la hiérarchie de destination pendant que la migration à partir de la hiérarchie source est active, il est possible de mettre à niveau ou de réaffecter un point de distribution dans la hiérarchie de destination. Vous pouvez mettre à niveau des points de distribution partagés Configuration Manager 2007 et réaffecter des points de distribution partagés System Center 2012 Configuration Manager. Lorsque vous mettez à niveau ou réaffectez un point de distribution partagé, le point de distribution est supprimé de la hiérarchie source et il devient un point de distribution dans la hiérarchie de destination. Après avoir mis à niveau ou réaffecté un point de distribution partagé, vous pouvez continuer à utiliser le point de distribution dans la hiérarchie de destination une fois la migration à partir de la hiérarchie source terminée. Pour plus d'informations sur la mise à niveau d'un point de distribution partagé, consultez Planifier la mise à niveau des points de distribution partagés Configuration Manager 2007. Pour plus d'informations sur la façon de réaffecter un point de distribution partagé, consultez Planifier la réaffectation des points de distribution System Center Configuration Manager.

Vous pouvez choisir de partager des points de distribution de n'importe quel site source de votre hiérarchie source. Quand vous partagez des points de distribution pour un site source, les sites secondaires enfants sont partagés sur chaque point de distribution concerné sur ce site principal et sur chacun des sites principaux. Pour qu'un point de distribution puisse être partagé, le serveur de système de site qui héberge le point de distribution doit être configuré avec un nom de domaine complet (FQDN). Les points de distribution configurés avec un nom NetBIOS sont ignorés.

> **TIP**
> Avec Configuration Manager 2007, vous n'avez pas besoin de configurer un nom de domaine complet pour les serveurs de système de site.

Utilisez les informations suivantes pour planifier les points de distribution partagés :

- Les points de distribution que vous partagez doivent respecter les conditions préalables applicables aux points de distribution partagés. Pour plus d'informations sur ces prérequis, consultez Configurations requises pour la migration dans Prérequis de la migration dans System Center Configuration Manager.
- L'action de partage de point de distribution est un paramètre de site qui partage tous les points de distribution admissibles sur un site source et sur les sites secondaires enfants directs. Vous ne pouvez pas sélectionner des points de distribution individuels à partager lorsque vous activez le partage de point de distribution.
- Les clients dans la hiérarchie de destination peuvent recevoir des informations d'emplacement du contenu pour les packages distribués sur les points de distribution partagés à partir de la hiérarchie source. Pour les points de distribution d'une hiérarchie source Configuration Manager 2007, cela inclut les points de distribution de branche, les points de distribution sur des partages de serveur et les points de distribution standard.

  > **WARNING**
  > Si vous modifiez la hiérarchie source, les points de distribution partagés de la hiérarchie source d'origine ne sont plus disponibles et ne peuvent pas être proposés comme emplacements de contenu aux clients dans la hiérarchie de destination. Si vous reconfigurez la migration pour utiliser la hiérarchie source d'origine, les points de distribution partagés précédents sont restaurés en tant que serveurs valides d'emplacement du contenu.

- Lorsque vous faites migrer un package qui est hébergé sur un point de distribution partagé, la version du package doit rester la même dans les hiérarchies source et de destination. Lorsque la version du package n'est pas la même dans la hiérarchie source et la hiérarchie de destination, les clients dans la hiérarchie de

destination ne peuvent pas récupérer ce contenu à partir du point de distribution partagé. Par conséquent, si vous mettez à jour un package dans la hiérarchie source, vous devez à nouveau faire migrer les données du package pour que les clients dans la hiérarchie de destination puissent récupérer ce contenu à partir d'un point de distribution partagé.

> **NOTE**
> Quand vous affichez les détails d'un package hébergé sur un point de distribution partagé, le nombre de packages qui s'affichent comme **Packages migrés hébergés** sous l'onglet **Points de distribution partagés** des sites source n'est pas mis à jour avant la fin du cycle suivant de collecte des données.

- Vous pouvez afficher les points de distribution partagés et leurs propriétés dans le nœud **Hiérarchie source** de l'espace de travail **Administration** dans la console Configuration Manager connectée à la hiérarchie de destination.
- Vous ne pouvez pas utiliser un point de distribution partagé d'une hiérarchie source Configuration Manager 2007 pour héberger des packages pour Microsoft Application Virtualization (App-V). Les packages App-V doivent migrer et être convertis pour l'utilisation par les clients dans la hiérarchie de destination. Toutefois, vous pouvez utiliser un point de distribution partagé d'une hiérarchie source System Center 2012 Configuration Manager ou System Center Configuration Manager afin d'héberger des packages App-V pour des clients dans une hiérarchie de destination.
- Quand vous partagez un point de distribution protégé d'une hiérarchie source Configuration Manager 2007, la hiérarchie de destination crée un groupe de limites qui inclut les emplacements réseau protégés de ce point de distribution. Vous ne pouvez pas changer ce groupe de limites dans la hiérarchie de destination. Toutefois, si vous changez les informations des limites protégées pour le point de distribution dans la hiérarchie source Configuration Manager 2007, ce changement est reflété dans la hiérarchie de destination après le prochain cycle de collecte des données.

> **NOTE**
> Les sites System Center 2012 Configuration Manager et System Center Configuration Manager utilisent le concept de points de distribution préférés au lieu des points de distribution protégés. Cette condition s'applique uniquement aux points de distribution partagés à partir de sites source Configuration Manager 2007.

Les points de distribution éligibles ne sont pas visibles dans la console Configuration Manager tant que vous n'avez pas partagé de points de distribution d'un site source. Une fois que vous avez partagé des points de distribution, seuls les points de distribution effectivement partagés sont répertoriés.

Une fois que vous avez partagé des points de distribution, vous pouvez modifier la configuration de n'importe quel point de distribution partagé dans la hiérarchie source. Les modifications que vous apportez à la configuration d'un point de distribution sont répercutées dans la hiérarchie de destination à l'issue du cycle suivant de collecte des données. Les points de distribution que vous avez mis à jour pour qu'ils puissent être partagés le sont automatiquement, tandis que ceux qui ne peuvent plus l'être cessent de partager des points de distribution. Par exemple, vous pouvez avoir d'un point de distribution qui n'est pas configuré avec un nom de domaine complet d'intranet et qui n'était pas initialement partagé avec la hiérarchie de destination. Après avoir configuré le nom de domaine complet du point de distribution, le cycle suivant de collecte des données identifie cette configuration et le point de distribution est alors partagé avec la hiérarchie de destination.

## Planifier la mise à niveau des points de distribution partagés Configuration Manager 2007

Quand vous effectuez une migration à partir d'une hiérarchie source Configuration Manager 2007, vous pouvez

mettre à niveau un point de distribution partagé pour en faire un point de distribution System Center Configuration Manager. Vous pouvez mettre à niveau des points de distribution sur des sites principaux et sur des sites secondaires. Le processus de mise à niveau supprime le point de distribution de la hiérarchie Configuration Manager 2007, et le convertit en serveur de système de site dans la hiérarchie de destination. Ce processus copie également le contenu existant qui se trouve sur le point de distribution vers un nouvel emplacement sur l'ordinateur du point de distribution. Le processus de mise à niveau modifie alors la copie du contenu pour créer le magasin d'instances uniques à utiliser avec le déploiement de contenu dans la hiérarchie de destination. Ainsi, quand vous mettez à niveau un point de distribution, vous n'avez pas besoin de redistribuer le contenu migré qui était hébergé sur le point de distribution Configuration Manager 2007.

Une fois que Configuration Manager a converti le contenu en stockage SIS (Single-Instance-Store), Configuration Manager supprime le contenu source d'origine sur l'ordinateur du point de distribution pour libérer de l'espace disque. Configuration Manager n'utilise pas l'emplacement du contenu source d'origine.

Tous les points de distribution Configuration Manager 2007 que vous pouvez partager ne remplissent pas les conditions d'une mise à niveau vers System Center Configuration Manager. Pour être éligible à une mise à niveau, un point de distribution Configuration Manager 2007 doit remplir les conditions de la mise à niveau. Ces conditions incluent le serveur de système de site sur lequel le point de distribution est installé et le type de point de distribution Configuration Manager 2007 installé. Par exemple, vous ne pouvez pas mettre à niveau un type de point de distribution qui est installé sur l'ordinateur serveur de site au niveau d'un site principal, mais vous pouvez mettre à niveau un point de distribution standard qui est installé sur l'ordinateur serveur de site au niveau d'un site secondaire.

> **NOTE**
>
> Vous ne pouvez mettre à niveau que les points de distribution partagés Configuration Manager 2007 qui se trouvent sur un ordinateur exécutant une version de système d'exploitation prise en charge en tant que point de distribution dans la hiérarchie de destination. Par exemple, bien que vous puissiez partager un point de distribution Configuration Manager 2007 situé sur un ordinateur exécutant Windows Vista, vous ne pouvez pas le mettre à niveau, car System Center Configuration Manager ne prend pas en charge l'utilisation de ce système d'exploitation en tant que point de distribution.

Le tableau suivant répertorie les emplacements pris en charge pour chaque type de point de distribution Configuration Manager 2007 pouvant être mis à niveau.

| TYPE DE POINT DE DISTRIBUTION | POINT DE DISTRIBUTION SUR UN ORDINATEUR DU SYSTÈME DE SITE AUTRE QUE LE SERVEUR DE SITE | POINT DE DISTRIBUTION SUR UN ORDINATEUR DU SYSTÈME DE SITE AUTRE QUE LE SERVEUR DE SITE ET HÉBERGEANT D'AUTRES RÔLES DE SYSTÈME DE SITE | POINT DE DISTRIBUTION SUR UN SERVEUR DE SITE SECONDAIRE |
|---|---|---|---|
| Point de distribution standard | Oui | Non | Oui |
| Point de distribution sur des partages de serveur[1] | Oui | Non | Non |
| Point de distribution de branche | Oui | Non | Non |

[1] System Center Configuration Manager ne prend pas en charge les partages de serveur des systèmes de site, mais il prend en charge la mise à niveau d'un point de distribution Configuration Manager 2007 qui se trouve sur un partage de serveur. Quand vous mettez à niveau un point de distribution Configuration Manager 2007 situé sur un partage de serveur, le type de point de distribution est automatiquement converti en serveur. De plus, vous devez sélectionner le lecteur de l'ordinateur du point de distribution destiné à stocker le magasin de contenu d'instances uniques.

> **WARNING**
> Avant de mettre à niveau un point de distribution de branche, désinstallez le logiciel client Configuration Manager 2007. Quand vous mettez à niveau un point de distribution de branche sur lequel est installé le logiciel client Configuration Manager 2007, le contenu déployé est supprimé de l'ordinateur, ce qui entraîne l'échec de la mise à niveau du point de distribution.

Pour identifier les points de distribution qui peuvent être mis à niveau, dans la console Configuration Manager, dans le nœud **Hiérarchie source**, sélectionnez un site source, puis l'onglet **Points de distribution partagés**. Les points de distribution éligibles affichent **Oui** dans la colonne **Éligible à la mise à niveau** .

Quand vous mettez à niveau un point de distribution installé sur un serveur de site secondaire Configuration Manager 2007, le site secondaire est désinstallé de la hiérarchie source. Bien que ce scénario corresponde à une mise à niveau du site secondaire, cela s'applique uniquement au rôle de système de site de point de distribution. Le résultat est que le site secondaire n'est pas mis à niveau et qu'il est désinstallé. Ceci laisse un seul point de distribution de la hiérarchie de destination sur l'ordinateur qui était le serveur de site secondaire. Si vous envisagez de mettre à niveau le point de distribution sur un site secondaire, consultez Planifier la mise à niveau des sites secondaires Configuration Manager 2007 dans cette rubrique.

**Processus de mise à niveau des points de distribution**

Vous pouvez utiliser la console Configuration Manager pour mettre à niveau les points de distribution Configuration Manager 2007 que vous avez partagés avec la hiérarchie de destination. Quand vous mettez à niveau un point de distribution partagé, le point de distribution est désinstallé du site Configuration Manager 2007. Il est ensuite installé comme point de distribution qui est attaché à un site principal ou secondaire que vous spécifiez dans la hiérarchie de destination. Le processus de mise à niveau crée une copie du contenu migré qui est stocké sur le point de distribution, puis convertit cette copie en magasin de contenu d'instances uniques. Quand Configuration Manager convertit un package en magasin de contenu d'instances uniques, il supprime ce package du partage SMSPKG sur l'ordinateur du point de distribution, sauf si le package comporte une ou plusieurs publications configurées pour **Exécuter le programme à partir du point de distribution**.

Pour mettre à niveau le point de distribution, Configuration Manager utilise le **compte d'accès au site source** configuré pour collecter des données à partir du fournisseur SMS du site source. Bien que ce compte nécessite uniquement l'autorisation de **lecture** pour permettre aux objets de site de collecter des données du site source, il doit disposer également de l'autorisation de **suppression** et de **modification** dans la classe **Site** pour pouvoir supprimer correctement le point de distribution du site Configuration Manager 2007 durant la mise à niveau.

> **NOTE**
> Configuration Manager peut convertir le contenu en magasin d'instances uniques sur un seul point de distribution à la fois. Quand vous configurez des mises à niveau de plusieurs point de distribution, les points de distribution sont placés en file d'attente pour la mise à niveau et traités un par un.

Avant la mise à niveau d'un point de distribution partagé, vérifiez que tout le contenu déployé sur le point de distribution a migré. Le contenu que vous ne faites pas migrer avant de mettre à niveau le point de distribution n'est pas disponible dans la hiérarchie de destination après la mise à niveau. Lorsque vous mettez à niveau un point de distribution, le contenu dans les packages migrés est converti dans un format compatible avec le magasin d'instances uniques de la hiérarchie de destination.

Pour permettre la mise à niveau d'un point de distribution dans la console Configuration Manager, le serveur de système de site Configuration Manager 2007 doit remplir les conditions suivantes :

- La configuration de point de distribution et l'emplacement doivent être éligibles à la mise à niveau.
- L'ordinateur du point de distribution doit avoir un espace disque suffisant pour que le contenu puisse être

converti du format de stockage de contenu Configuration Manager 2007 vers le format de magasin d'instances uniques. Cette conversion nécessite que l'espace disque disponible soit égal à la taille du package le plus volumineux stocké sur le point de distribution.

- L'ordinateur de point de distribution doit exécuter une version de système d'exploitation prise en charge comme un point de distribution dans la hiérarchie de destination.

> **NOTE**
> Quand Configuration Manager vérifie si le point de distribution peut être mis à niveau, il ne valide pas la version du système d'exploitation de l'ordinateur du point de distribution.

Pour mettre à niveau un point de distribution, dans l'espace de travail **Administration**, développez **Migration**et le nœud **Hiérarchie source**, puis sélectionnez le site qui a le point de distribution à mettre à niveau. Ensuite, dans le volet des détails, sous l'onglet **Points de distribution partagés** , sélectionnez le point de distribution à mettre à niveau.

Vous pouvez vérifier si le point de distribution est prêt pour la mise à niveau en consultant l'état dans la colonne **Éligible à la réaffectation** . Ensuite, dans le ruban de la console Configuration Manager, sous l'onglet **Points de distribution**, dans le groupe **Point de distribution**, sélectionnez **Réaffecter**. Ceci ouvre un Assistant que vous utilisez pour terminer la mise à niveau du point de distribution.

Lorsque vous mettez à niveau un point de distribution partagé, vous devez affecter le point de distribution à un site principal ou secondaire de votre choix dans la hiérarchie de distribution. Une fois que le point de distribution est mis à niveau, gérez le point de distribution comme un point de distribution dans la hiérarchie de destination, comme tout autre point de distribution.

Vous pouvez surveiller la progression de la mise à niveau d'un point de distribution dans la console Configuration Manager en sélectionnant le nœud **Migration de point de distribution** sous le nœud **Migration** de l'espace de travail **Administration**. Vous pouvez également afficher des informations dans le journal **Migmctrl.log** sur le serveur de site d'administration centrale de la hiérarchie de destination ou dans le journal **distmgr.log** sur le serveur de site dans la hiérarchie de destination qui gère le point de distribution mis à niveau.

> **NOTE**
> Quand vous mettez à niveau un point de distribution sur la hiérarchie de destination, le rôle de système de site de point de distribution est supprimé du site source Configuration Manager 2007. Cependant, les packages qui ont été envoyés au point de distribution ne sont pas mis à jour dans la hiérarchie Configuration Manager 2007. Dans la console Configuration Manager 2007, les packages envoyés vers le point de distribution continuent de répertorier l'ordinateur du système de site en tant que point de distribution de **Type Inconnu**. Les mises à jour suivantes du package dans Configuration Manager 2007 génèrent des rapports d'erreurs du gestionnaire de distribution dans le journal distmgr.log relatif à ce site durant la tentative de mise à jour du package sur le système de site inconnu.

Si vous décidez de ne pas mettre à niveau un point de distribution partagé, vous pouvez toujours installer un point de distribution de la hiérarchie de destination sur un ancien point de distribution Configuration Manager 2007. Pour pouvoir installer le nouveau point de distribution, vous devez d'abord désinstaller tous les rôles de système de site Configuration Manager 2007 sur l'ordinateur du point de distribution. Cela inclut le site Configuration Manager 2007, s'il s'agit de l'ordinateur serveur de site. Quand vous désinstallez un point de distribution Configuration Manager 2007, le contenu qui a été déployé sur le point de distribution n'est pas supprimé de l'ordinateur.

**Planifier la mise à niveau des sites secondaires Configuration Manager 2007**

Quand vous utilisez la migration pour mettre à niveau un point de distribution partagé hébergé sur un serveur

de site secondaire Configuration Manager 2007, Configuration Manager met à niveau le rôle de système de site du point de distribution de façon à en faire un point de distribution dans la hiérarchie de destination. Il désinstalle également le site secondaire dans la hiérarchie source. Il en résulte un point de distribution System Center Configuration Manager, mais aucun site secondaire.

Pour qu'un point de distribution sur l'ordinateur serveur de site puisse être mis à niveau, Configuration Manager doit pouvoir désinstaller le site secondaire et chaque rôle de système de site présent sur cet ordinateur. En général, un point de distribution partagé sur un partage de serveur Configuration Manager 2007 peut être mis à niveau. Toutefois, lorsqu'il existe un partage de serveur sur le serveur de site secondaire, le site secondaire et tout point de distribution partagé sur cet ordinateur ne sont pas éligibles à la mise à niveau. La raison en est que le partage de serveur est traité comme un objet de système de site supplémentaire quand le processus tente de désinstaller le site secondaire, et que ce processus ne peut pas désinstaller cet objet. Dans ce scénario, vous pouvez activer un point de distribution standard sur le serveur de site secondaire, puis redistribuer le contenu vers ce point de distribution standard. Ce processus n'utilise pas la bande passante du réseau et, une fois le processus terminé, vous pouvez désinstaller le point de distribution sur le partage de serveur, puis mettre à niveau le point de distribution et le site secondaire.

Avant de mettre à niveau un point de distribution partagé, vérifiez la configuration du point de distribution dans Configuration Manager 2007 pour éviter de mettre à niveau un point de distribution sur site secondaire que vous souhaitez toujours utiliser avec Configuration Manager 2007. Il s'agit d'une pratique recommandée car après la mise à niveau d'un point de distribution partagé du serveur de site secondaire, le serveur de système de site est supprimé de la hiérarchie Configuration Manager 2007 et il ne peut plus être utilisé avec cette hiérarchie. Lorsque le site secondaire est supprimé, les points de distribution restants sur le site secondaire sont orphelins. Cela signifie qu'ils deviennent non gérés à partir de Configuration Manager 2007, et qu'ils ne sont plus partagés ou éligibles pour une mise à niveau.

> **WARNING**
> Quand vous affichez des points de distribution partagés dans la console Configuration Manager, aucune indication ne montre qu'un point de distribution partagé se trouve sur un serveur de système de site distant ou sur le serveur de site secondaire.

Quand un site secondaire se trouve à un emplacement réseau distant principalement utilisé pour contrôler le déploiement de contenu vers cet emplacement distant, vous pouvez envisager de mettre à niveau les sites secondaires qui ont un point de distribution partagé. Pour pouvoir configurer le contrôle de la bande passante quand vous distribuez du contenu à un point de distribution System Center Configuration Manager, vous pouvez souvent mettre à niveau un site secondaire pour en faire un point de distribution, configurer le point de distribution pour les contrôles de bande passante et éviter d'installer un site secondaire à cet emplacement réseau dans la hiérarchie de destination.

Le processus de mise à niveau d'un point de distribution partagé sur un serveur de site secondaire est identique à n'importe quelle autre mise à niveau d'un point de distribution partagé. Le contenu est copié et converti dans le stockage SIS (Single-Instance-Store) utilisé par la hiérarchie de destination. Cependant, quand vous mettez à niveau un point de distribution partagé sur un serveur de site secondaire, le processus de mise à niveau désinstalle également le point de gestion (s'il est présent), puis désinstalle le site secondaire du serveur. Ainsi, le site secondaire est supprimé de la hiérarchie Configuration Manager 2007. Pour désinstaller le site secondaire, Configuration Manager utilise le compte configuré pour recueillir des données à partir du site source.

Durant la mise à niveau, il existe un retard entre le moment où le site secondaire Configuration Manager 2007 est désinstallé et le moment où l'installation du point de distribution dans la hiérarchie de destination commence. Le cycle de collecte de données détermine ce décalage pouvant aller jusqu'à quatre heures. Le décalage est destiné à laisser le temps au site secondaire d'être désinstallé avant que l'installation du nouveau point de distribution commence.

Pour plus d'informations sur la mise à niveau d'un point de distribution partagé, consultez Planifier la mise à niveau des points de distribution partagés Configuration Manager 2007.

## Planifier la réaffectation des points de distribution System Center Configuration Manager

Durant la migration d'une version prise en charge de System Center 2012 Configuration Manager vers une hiérarchie de la même version, vous pouvez réaffecter un point de distribution partagé de la hiérarchie source à un site de la hiérarchie de destination. Cela est similaire au concept de mise à niveau d'un point de distribution Configuration Manager 2007 pour en faire un point de distribution dans la hiérarchie de destination. Vous pouvez réaffecter des points de distribution de sites principaux et de sites secondaires. Cette action de réaffectation d'un point de distribution supprime le point de distribution de la hiérarchie source et convertit l'ordinateur et son point de distribution en serveur de système de site pour un site que vous sélectionnez dans la hiérarchie de destination.

Lorsque vous réaffectez un point de distribution, il est inutile de redistribuer le contenu migré qui était hébergé sur le point de distribution du site source. De plus, à l'inverse de la mise à niveau d'un point de distribution Configuration Manager 2007, la réaffectation d'un point de distribution ne nécessite aucun espace disque supplémentaire sur l'ordinateur du point de distribution. La raison en est que, à partir de System Center 2012 Configuration Manager, les points de distribution utilisent le format SIS (Single-Instance-Store) pour le contenu. Le contenu sur l'ordinateur du point de distribution n'a pas besoin d'être converti quand le point de distribution est réaffecté entre les hiérarchies.

Pour qu'un point de distribution System Center 2012 Configuration Manager puisse être réaffecté, il doit répondre aux critères suivants :

- Le point de distribution partagé doit être installé sur un ordinateur autre que le serveur de site.
- Le point de distribution partagé ne peut pas être hébergé avec des rôles de système de site supplémentaires.

Pour identifier les points de distribution qui peuvent être réaffectés, dans la console Configuration Manager, dans le nœud **Hiérarchie source**, sélectionnez un site source, puis l'onglet **Points de distribution partagés**. Les points de distribution éligibles indiquent **Oui** dans la colonne **Éligible à la réaffectation** (avant System Center 2012 R2 Configuration Manager, cette colonne était nommée **Éligible à la mise à niveau**).

**Processus de réattribution des points de distribution**

Vous pouvez utiliser la console Configuration Manager pour réaffecter les points de distribution que vous avez partagés à partir d'une hiérarchie source active. Quand vous réaffectez un point de distribution partagé, le point de distribution est désinstallé du site source, puis installé comme point de distribution attaché à un site principal ou secondaire que vous spécifiez dans la hiérarchie de destination.

Pour réaffecter le point de distribution, la hiérarchie de destination utilise le compte d'accès au site source configuré pour collecter des données à partir du fournisseur SMS du site source. Pour plus d'informations sur les autorisations nécessaires et les prérequis supplémentaires, consultez Prérequis de la migration dans System Center Configuration Manager.

## Migrer plusieurs points de distribution partagés en même temps

Depuis la version 1610, vous pouvez utiliser l'option **Réaffecter le point de distribution** pour que Configuration Manager traite en parallèle la réaffectation d'un maximum de 50 points de distribution partagés en même temps. Cela inclut les points de distribution partagés des sites sources pris en charge qui exécutent :

- Configuration Manager 2007
- System Center 2012 Configuration Manager

- System Center 2012 R2 Configuration Manager
- System Center Configuration Manager (branche actuelle)

Quand vous réaffectez les points de distribution, chaque point de distribution doit pouvoir être mis à niveau ou réaffecté. Le nom de l'action et du processus impliqués, mise à niveau ou réaffectation, dépend de la version de Configuration Manager exécutée par le site source. Les résultats finaux des deux actions sont identiques : le point de distribution est affecté à un des sites Current Branch avec son contenu en place.

Avant la version 1610, Configuration Manager ne pouvait traiter qu'un seul point de distribution à la fois. Vous pouvez désormais réaffecter autant de points de distribution que vous le souhaitez avec les remarques suivantes :

- Même si vous ne pouvez pas effectuer une sélection multiple des points de distribution à réaffecter, quand vous en avez mis plusieurs en file d'attente, Configuration Manager les traite en parallèle au lieu d'attendre d'en terminer un avant de commencer le suivant.
- Par défaut, jusqu'à 50 points de distribution sont traités en parallèle à la fois. Une fois la réaffectation du premier point de distribution terminée, Configuration Manager commence à traiter le 51ème, et ainsi de suite.
- Quand vous utilisez le SDK Configuration Manager, vous pouvez modifier **SharedDPImportThreadLimit** pour ajuster le nombre de points de distribution réaffectés que Configuration Manager peut traiter en parallèle.

## Affecter la propriété du contenu lors de la migration de contenu

Lorsque vous migrez du contenu pour des déploiements, vous devez attribuer l'objet de contenu à un site dans la hiérarchie de destination. Ce site devient alors le propriétaire de ce contenu dans la hiérarchie de destination. Bien que le site de plus haut niveau de votre hiérarchie de destination soit le site qui migre les métadonnées du contenu, c'est le site affecté qui utilise les fichiers sources d'origine du contenu sur le réseau.

Pour réduire la bande passante réseau utilisée lors de la migration de contenu, transférez la propriété du contenu à un site proche dans la hiérarchie de destination sur le réseau vers l'emplacement de contenu dans la hiérarchie de destination. Comme les informations sur le contenu dans la hiérarchie de destination sont partagées globalement, elles seront disponibles sur chaque site.

Bien que les informations sur le contenu soient partagées sur tous les sites en utilisant la réplication de base de données, le contenu que vous affectez à un site principal et que vous déployez ensuite sur des points de distribution sur d'autres sites principaux est transféré en utilisant la réplication basée sur les fichiers. Ce transfert est routé via le site administration centrale, puis vers le site principal supplémentaire. Vous pouvez réduire les transferts de données sur les réseaux à faible bande passante en centralisant les packages que vous prévoyez de distribuer sur plusieurs sites principaux avant ou pendant la migration, quand vous définissez un site comme propriétaire du contenu.

# Planifier la migration d'objets Configuration Manager vers System Center Configuration Manager

22/06/2018 • 26 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Avec System Center Configuration Manager, vous pouvez migrer de nombreux objets différents associés à différentes fonctionnalités trouvées sur un site source. Utilisez les sections suivantes pour planifier la migration d'objets entre des hiérarchies.

- Planifier la migration des mises à jour logicielles
- Planifier la migration du contenu
- Planifier la migration des regroupements
- Planifier la migration de déploiements de systèmes d'exploitation
- Planifier la migration de la gestion de configuration souhaitée
- Planifier la migration des limites
- Planifier la migration des rapports
- Planifier la migration des dossiers d'organisation et de recherche
- Planifier la migration des personnalisations Asset Intelligence
- Planifier la migration des personnalisations des règles de contrôle de logiciel

## Planifier la migration des mises à jour logicielles

Vous pouvez migrer des objets de mise à jour logicielle, comme des packages de mise à jour logicielle et les déploiements de mise à jour logicielle.

Pour migrer des objets de mise à jour logicielle, vous devez d'abord configurer votre hiérarchie de destination avec des configurations qui correspondent à l'environnement de votre hiérarchie source. Pour cela, vous devez exécuter les actions suivantes :

- Déployer un point de mise à jour logicielle actif dans la hiérarchie de destination
- Configurer le catalogue de produits et de langues de sorte qu'il corresponde à la configuration de votre hiérarchie source
- Synchroniser le point de mise à jour logicielle de la hiérarchie de destination avec WSUS (Windows Server Update Services)

Lorsque vous migrez des mises à jour logicielles, tenez compte des éléments suivants :

- La migration d'objets de mise à jour logicielle peut échouer si vous n'avez pas synchronisé les informations de votre hiérarchie de destination de sorte qu'elles correspondent à la configuration de votre hiérarchie source.

> **WARNING**
> Configuration Manager ne prend pas en charge l'outil WSUSutil pour synchroniser les données entre une hiérarchie source et une hiérarchie de destination.

- Vous ne pouvez pas migrer des mises à jour personnalisées publiées à l'aide de l'éditeur de mise à jour System Center. Vous devez republier les mises à jour personnalisées dans la hiérarchie de destination.

Quand vous migrez depuis une hiérarchie source Configuration Manager 2007, le processus de migration modifie certains objets de mise à jour logicielle en fonction du format utilisé par la hiérarchie de destination. Utilisez le tableau suivant pour planifier la migration des objets de mise à jour logicielle depuis Configuration Manager 2007.

| OBJET CONFIGURATION MANAGER 2007 | NOM DE L'OBJET APRÈS LA MIGRATION |
|---|---|
| Listes des mises à jour logicielles | Les listes de mises à jour logicielles sont converties en groupes de mises à jour. |
| Déploiements de mises à jour logicielles | Les déploiements de mise à jour logicielle sont convertis en déploiements et groupes de mises à jour.<br><br>Une fois que vous avez effectué la migration d'un déploiement de mise à jour logicielle à partir de Configuration Manager 2007, vous devez l'activer dans la hiérarchie de destination avant de pouvoir le déployer. |
| Packages de mises à jour logicielles | Les packages de mises à jour logicielles restent des packages de mises à jour logicielles. |
| Modèles de mise à jour logicielle | Les modèles de mise à jour logicielle restent des modèles de mise à jour logicielle.<br><br>La valeur **Durée** dans les modèles de déploiement Configuration Manager 2007 n'est pas migrée. |

Quand vous migrez des objets à partir d'une hiérarchie source System Center 2012 Configuration Manager ou System Center Configuration Manager, les objets de mise à jour logicielle ne sont pas modifiés.

## Planifier la migration du contenu

Vous pouvez migrer du contenu d'une hiérarchie source prise en charge vers votre hiérarchie de destination. Pour une hiérarchie source Configuration Manager 2007, ce contenu comprend des programmes et des packages de distribution de logiciels, ainsi que des applications virtuelles, comme Microsoft Application Virtualization (App-V). Pour les hiérarchies sources System Center 2012 Configuration Manager et System Center Configuration Manager, ce contenu inclut des applications et des applications virtuelles App-V. Quand vous migrez du contenu entre des hiérarchies, les fichiers sources compressés sont migrés vers la hiérarchie de destination.

**Packages et programmes**

Lorsque vous migrez des packages et des programmes, ils ne sont pas modifiés par la migration. Cependant, avant de les migrer, vous devez configurer chaque package pour qu'il utilise un chemin d'accès UNC (Universal Naming Convention) pour son emplacement de fichier source. Dans le cadre de la configuration de la migration de packages et de programmes, vous devez affecter à un site de la hiérarchie de destination la gestion de ce contenu. Le contenu n'est pas migré à partir du site affecté, mais après la migration, le site affecté accède à l'emplacement du fichier source d'origine en utilisant le mappage UNC.

Après avoir migré un package et un programme vers la hiérarchie de destination et tant que la migration de la

hiérarchie source est active, vous pouvez mettre le contenu à la disposition des clients de cette hiérarchie en utilisant un point de distribution partagé. Pour utiliser un point de distribution partagé, le contenu doit rester accessible sur le point de distribution au niveau du site source. Pour plus d'informations sur les points de distribution partagés, consultez Partager les points de distribution entre les hiérarchies sources et de destination dans Planifier une stratégie de migration de déploiement de contenu dans System Center Configuration Manager.

Si la version du contenu migré a changé dans la hiérarchie source ou la hiérarchie de destination, les clients ne peuvent plus accéder au contenu à partir du point de distribution partagé dans la hiérarchie de destination. Dans ce cas, vous devez migrer à nouveau le contenu pour restaurer une version cohérente du package entre la hiérarchie source et la hiérarchie de destination. Ces informations sont synchronisées pendant le cycle de collecte des données.

> **TIP**
> Pour chaque package que vous migrez, mettez-le à jour dans la hiérarchie de destination. Cette action peut éviter les problèmes liés au déploiement du package sur les points de distribution de la hiérarchie de destination. Cependant, quand vous mettez à jour un package sur le point de distribution de la hiérarchie de destination, les clients de cette hiérarchie ne peuvent plus obtenir ce package à partir d'un point de distribution partagé. Pour mettre à jour un package dans la hiérarchie de destination, dans la console Configuration Manager, accédez à la bibliothèque de logiciels, cliquez avec le bouton droit sur le package, puis sélectionnez **Mettre à jour les points de distribution**. Effectuez cette action pour chaque package que vous migrez.

> **TIP**
> Vous pouvez utiliser Microsoft System Center Configuration Manager Package Conversion Manager pour convertir les packages et les programmes en applications System Center Configuration Manager. Téléchargez le gestionnaire de conversion des packages à partir du site Centre de téléchargement Microsoft . Pour plus d'informations, consultez Gestionnaire de conversion des packages Configuration Manager.

**Applications virtuelles**

Quand vous migrez des packages App-V à partir d'un site Configuration Manager 2007 pris en charge, le processus de migration les convertit en applications dans la hiérarchie de destination. En outre, selon les publications existantes du package App-V, les types de déploiements suivants sont créés dans la hiérarchie de destination :

- S'il n'existe pas de publications, un type de déploiement est créé qui utilise les paramètres du type de déploiement par défaut.
- S'il existe une publication, un type de déploiement utilisant les mêmes paramètres que la publication Configuration Manager 2007 est créé.
- S'il existe plusieurs publications, un type de déploiement est créé pour chaque publication Configuration Manager 2007 en utilisant les paramètres pour cette publication.

> **IMPORTANT**
> Si vous migrez un package App-V Configuration Manager 2007 précédemment migré, la migration échoue car les packages d'applications virtuelles ne prennent pas en charge le comportement de remplacement d'une migration. Dans ce cas, vous devez supprimer le package d'application virtuelle migré à partir de la hiérarchie de destination, puis créer une tâche de migration pour migrer l'application virtuelle.

> **NOTE**
> Après avoir migré un package App-V, vous pouvez utiliser l'Assistant Mise à jour du contenu pour changer le chemin d'accès source pour les types de déploiement App-V. Pour plus d'informations sur la mise à jour de contenu pour un type de déploiement, consultez « Comment gérer les types de déploiement » dans Tâches de gestion pour les applications System Center Configuration Manager.

Quand vous migrez depuis une hiérarchie source System Center 2012 Configuration Manager ou System Center Configuration Manager, vous pouvez migrer des objets pour l'environnement virtuel App-V, en plus des types de déploiement et des applications App-V. Pour plus d'informations sur les environnements App-V, consultez Déploiement d'applications virtuelles App-V avec System Center Configuration Manager.

**Publications**

Vous pouvez migrer des publications d'un site source Configuration Manager 2007 pris en charge vers la hiérarchie de destination en utilisant la migration basée sur les regroupements. Si vous mettez à niveau un client, il conserve l'historique des publications déjà exécutées pour empêcher le client de réexécuter les publications migrées.

> **NOTE**
> Vous ne pouvez pas migrer de publications pour les packages virtuels. Il s'agit d'une exception à la migration des publications.

**Applications**

Vous pouvez migrer des applications depuis une hiérarchie source System Center 2012 Configuration Manager ou System Center Configuration Manager prise en charge vers une hiérarchie de destination. Si vous réattribuez un client de la hiérarchie source à la hiérarchie de destination, le client conserve l'historique des applications installée précédemment pour éviter qu'il réexécute une application migrée.

## Planifier la migration des regroupements

Vous pouvez migrer les critères des regroupements d'une hiérarchie source System Center 2012 Configuration Manager ou System Center Configuration Manager prise en charge. Pour ce faire, vous utilisez une tâche de migration basée sur un objet. Lorsque vous migrez un regroupement, vous migrez les règles du regroupement et non les informations sur les membres du regroupement ni les informations ou les objets associés aux membres du regroupement.

La migration de l'objet de regroupement n'est pas prise en charge quand vous effectuez une migration à partir d'une hiérarchie source Configuration Manager 2007.

## Planifier la migration de déploiements de systèmes d'exploitation

Vous pouvez migrer les objets de déploiement de système d'exploitation suivants à partir d'une hiérarchie source pris en charge :

- Images et packages de système d'exploitation Le chemin source des images de démarrage est remplacé par l'emplacement de l'image par défaut pour le kit Windows AIK (Windows Administrative Installation Kit) sur le site de destination. Vous trouverez ci-dessous les exigences et les restrictions liées à la migration d'images et de packages de système d'exploitation :
    - Pour migrer des fichiers image, le compte d'ordinateur du serveur Fournisseur SMS du site de plus haut niveau de la hiérarchie de destination doit disposer de l'autorisation de **lecture** et d'**écriture** sur les fichiers image sources de l'emplacement Windows AIK du site source.

- Quand vous migrez un package d'installation de système d'exploitation, vérifiez que la configuration du package sur le site source pointe vers le dossier qui contient le fichier WIM et non pas vers le fichier WIM lui-même. Si le package d'installation pointe vers le fichier WIM, la migration du package d'installation échoue.
- Quand vous migrez un package d'images de démarrage à partir d'un site source Configuration Manager 2007, l'ID du package n'est pas conservé dans le site de destination. La conséquence de cela est que les clients de la hiérarchie de destination ne peuvent pas utiliser les packages d'images de démarrage disponibles sur les points de distribution partagés.

- Séquences de tâches Quand vous migrez une séquence de tâches qui a une référence à un package d'installation de client, cette référence est remplacée par une référence au package d'installation de client de la hiérarchie de destination.

  > **NOTE**
  > Quand vous migrez une séquence de tâches, Configuration Manager peut migrer des objets qui ne sont pas nécessaires dans la hiérarchie de destination. Ces objets incluent les images de démarrage et les packages d'installation du client Configuration Manager 2007.

- Pilotes et packages de pilotes Lorsque vous migrez des packages de pilotes, le compte d'ordinateur du fournisseur SMS dans la hiérarchie de destination doit avoir un contrôle total sur la source du package.

## Planifier la migration de la gestion de configuration souhaitée

Vous pouvez migrer des éléments de configuration et des lignes de base de configuration.

> **NOTE**
> Les éléments de configuration non interprétés des hiérarchies sources Configuration Manager 2007 ne sont pas pris en charge pour la migration. Vous ne pouvez pas migrer ou importer ces éléments de configuration dans la hiérarchie de destination. Pour plus d'informations sur les éléments de configuration non interprétés, consultez « Éléments de configuration non interprétés » dans la rubrique À propos des éléments de configuration dans la gestion de la configuration souhaitée, dans la bibliothèque de documentation Configuration Manager 2007.

Vous pouvez importer les packs de configuration Configuration Manager 2007. Le processus d'importation convertit automatiquement les packs de configuration pour qu'ils soient compatibles avec System Center Configuration Manager.

## Planifier la migration des limites

Vous pouvez migrer des limites entre les hiérarchies. Quand vous migrez des limites à partir de Configuration Manager 2007, chaque limite du site source migre simultanément et est ajoutée à un nouveau groupe de limites créé dans la hiérarchie de destination. Quand vous migrez les limites d'une hiérarchie System Center Configuration Manager 2012 ou System Center Configuration Manager, chaque limite sélectionnée est ajoutée à un nouveau groupe de limites dans la hiérarchie de destination.

Chaque groupe de limites créé automatiquement est activé pour l'emplacement de contenu, mais pas pour l'attribution de site. Cela empêche les limites de se chevaucher pour l'attribution de site entre les hiérarchies source et de destination. Quand vous migrez depuis un site source Configuration Manager 2007, ceci permet d'empêcher que les nouveaux clients Configuration Manager 2007 installés soient affectés de manière incorrecte à la hiérarchie de destination. Par défaut, les clients System Center Configuration Manager ne sont pas affectés automatiquement aux sites Configuration Manager 2007.

Lors de la migration, si vous partagez un point de distribution avec la hiérarchie de destination, les limites associées à cette distribution migrent automatiquement vers la hiérarchie de destination. Dans la hiérarchie de destination, la migration crée un groupe de limites en lecture seule pour chaque point de distribution partagé. Si vous modifiez les limites du point de distribution de la hiérarchie source, le groupe de limites de la hiérarchie de destination est mis à jour par rapport à ces modifications lors du prochain cycle de collecte de données.

## Planifier la migration des rapports

Configuration Manager ne prend pas en charge la migration des rapports. Utilisez plutôt le Générateur de rapports Microsoft SQL Server Reporting Services pour exporter des rapports à partir de la hiérarchie source, puis importez-les dans la hiérarchie de destination.

> **NOTE**
> Le schéma des rapports ayant changé entre Configuration Manager 2007 et System Center Configuration Manager, testez chaque rapport importé à partir d'une hiérarchie Configuration Manager 2007 pour vérifier qu'il fonctionne comme prévu.

Pour plus d'informations sur la création de rapports, consultez Génération de rapports dans System Center Configuration Manager.

## Planifier la migration des dossiers d'organisation et de recherche

Vous pouvez migrer des dossiers organisationnels et des dossiers de recherche d'une hiérarchie source prise en charge vers une hiérarchie de destination. De plus, à partir d'une hiérarchie source System Center 2012 Configuration Manager ou System Center Configuration Manager, vous pouvez migrer les critères d'une recherche enregistrée vers une hiérarchie de destination.

Par défaut, le processus de migration conserve les structures de dossiers de recherche et de dossiers d'administration pour les objets et les regroupements. Cependant, dans l'Assistant Création de tâche de migration, sur la page **Paramètres** , vous pouvez configurer une tâche de migration de sorte que la structure organisationnelle des objets ne soit pas migrée en décochant la case correspondant à cette option. Les structures organisationnelles des regroupements sont toujours gérées.

Ceci ne s'applique pas à un dossier de recherche qui contient des applications virtuelles. Quand un package App-V est migré, le package est converti en application dans System Center Configuration Manager. Après la migration du dossier de recherche, seuls les packages restants sont trouvés et le dossier de recherche ne peut pas trouver le package App-V du fait de la conversion en application lorsque le package App-V migre.

Quand vous migrez une recherche enregistrée à partir d'une hiérarchie source System Center 2012 Configuration Manager ou System Center Configuration Manager, vous migrez les critères de la recherche et non les informations relatives aux résultats de la recherche. La migration d'une recherche enregistrée est non applicable à partir d'un site source Configuration Manager 2007.

## Planifier la migration des personnalisations Asset Intelligence

Vous pouvez migrer des personnalisations pour Asset Intelligence d'une hiérarchie source prise en charge vers une hiérarchie de destination. La structure des personnalisations Asset Intelligence n'a pas changé de manière significative entre Configuration Manager 2007 et System Center Configuration Manager.

> **NOTE**
> System Center Configuration Manager ne prend pas en charge la migration d'objets Asset Intelligence depuis un site Configuration Manager 2007 utilisant Asset Intelligence Service 2.0 (AIS 2.0).

# Planifier la migration des personnalisations des règles de contrôle de logiciel

Le contrôle de logiciel n’a pas changé de manière significative entre Configuration Manager 2007 et System Center Configuration Manager. Vous pouvez migrer vos règles de contrôle de logiciel d'une hiérarchie source prise en charge vers une hiérarchie de destination.

Par défaut, les règles de contrôle de logiciel que vous migrez vers une hiérarchie de destination ne sont associées à aucun site spécifique de la hiérarchie de destination et s'appliquent à tous les clients de la hiérarchie. Pour appliquer une règle de contrôle de logiciel aux clients d'un site spécifique, vous devez modifier la règle de mesure après l'avoir migrée.

# Planification de la surveillance de la migration dans System Center Configuration Manager

22/06/2018 • 3 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

System Center Configuration Manager vous permet de surveiller la migration dans la console Configuration Manager qui se connecte à la hiérarchie de destination. Dans la console Configuration Manager, dans l'espace de travail **Administration**, vous pouvez utiliser le nœud **Migration** pour surveiller l'avancement et la réussite des tâches de migration. Vous pouvez consulter les informations récapitulatives de chaque tâche de migration qui identifie les objets qui ont été migrés, ceux qui n'ont pas encore été migrés et le nombre d'objets qui ont été exclus de la migration. Elles contiennent également des informations sur les problèmes éventuels de migration.

## Afficher l'avancement de la migration

Pour afficher l'avancement d'une tâche de migration, optez pour l'une des actions suivantes :

- Dans l'espace de travail **Administration** de la console Configuration Manager, développez le nœud **Tâches de migration**, sélectionnez une tâche de migration, puis sélectionnez l'onglet **Objets dans la tâche**.
- Utilisez les fichiers journaux Configuration Manager pour vérifier l'avancement de la migration ou pour identifier les problèmes. Le gestionnaire de migration est le processus de Configuration Manager qui suit les actions de migration et les enregistre dans le fichier migmctrl.log dans le dossier **<Chemin_Installation>\LOGS** sur le serveur de site.

  > **NOTE**
  > Si une tâche de migration échoue, examinez les informations dans ce fichier dès que possible. Les entrées du journal de migration sont continuellement ajoutées au fichier et remplacent les anciennes. Si les entrées sont remplacées, vous risquez de ne pas pouvoir déterminer si les problèmes qui peuvent apparaître avec les objets migrés sont liés à la migration. L'activité de migration est consignée sur le site de niveau supérieur de la hiérarchie, quel que soit le site auquel la console Configuration Manager se connecte au moment où vous configurez la migration.

- Utilisez les rapports Configuration Manager. Configuration Manager propose plusieurs rapports intégrés pour la migration, que vous pouvez aussi modifier en fonction de vos besoins. Pour plus d'informations sur les rapports Configuration Manager, consultez Génération de rapports dans System Center Configuration Manager.

# Planifier la fin de la migration dans System Center Configuration Manager

22/06/2018 • 7 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Avec System Center Configuration Manager, vous pouvez terminer le processus de migration quand une hiérarchie source ne contient plus de données à migrer vers votre hiérarchie de destination. Pour cela, suivez les étapes ci-dessous :

- Vérifiez que les données dont vous avez besoin ont été migrées. Avant de terminer la migration à partir d'une hiérarchie source, vérifiez que vous avez bien migré toutes les ressources de la hiérarchie source dont vous pouvez avoir besoin dans la hiérarchie de destination. Pensez notamment aux données et aux clients.
- Arrêtez la collecte des données des sites source. Pour pouvoir terminer la migration à partir d'une hiérarchie source, vous devez au préalable arrêter la collecte des données des sites source.
- Nettoyez les données de migration. Après avoir arrêté la collecte des données des sites source d'une hiérarchie source, vous pouvez supprimer de la base de données de la hiérarchie de destination les données relatives au processus de migration et à la hiérarchie source.
- Retirez la hiérarchie source. Une fois que la migration à partir d'une hiérarchie source est terminée et que cette hiérarchie ne contient plus de ressources que vous gérez, vous pouvez retirer les sites de la hiérarchie source et supprimer l'infrastructure associée de votre environnement. Pour plus d'informations sur le retrait de sites et de hiérarchies sources, consultez la documentation de cette version de Configuration Manager.

Pour planifier la fin d'une migration à partir d'une hiérarchie source en arrêtant la collecte de données et le nettoyage des données de migration, consultez les sections ci-dessous :

- Planifier l'arrêt de la collecte de données
- Planifier le nettoyage des données de migration

## Planifier l'arrêt de la collecte de données

Avant de terminer la migration et de nettoyer les données de migration, vous devez arrêter la collecte des données de chaque site source dans la hiérarchie source. Pour arrêter la collecte de données de chaque site source, vous devez exécuter la commande **Arrêter la collecte de données** sur les sites source de niveau inférieur, puis répéter le processus au niveau de chaque site parent. Le site de niveau supérieur de la hiérarchie source doit être le dernier site sur lequel vous arrêtez la collecte des données. Vous devez arrêter la collecte de données sur chaque site enfant avant d'exécuter cette commande sur un site parent. En règle générale, vous arrêtez la collecte de données uniquement quand vous êtes prêt à terminer le processus de migration.

Lorsque vous arrêtez la collecte des données d'un site source, les points de distribution partagés de ce site ne sont plus disponibles en tant qu'emplacements de contenu pour les clients de la hiérarchie de destination. Par conséquent, vérifiez que le contenu migré dont les clients ont besoin dans la hiérarchie de destination reste bien disponible. Pour cela, utilisez l'une des méthodes suivantes :

- Dans la hiérarchie de destination, distribuez le contenu à un point de distribution au moins.
- Avant d'arrêter la collecte de données à partir d'un site source, mettez à niveau ou réaffectez les points de

distribution partagés ayant le contenu requis. Pour plus d'informations sur la mise à niveau ou la réattribution de points de distribution partagés, consultez les sections correspondantes dans la rubrique Planification d'une stratégie de migration de déploiement de contenu dans System Center Configuration Manager.

Après avoir arrêté la collecte de données à partir de chaque site source de la hiérarchie source, vous pouvez nettoyer les données de migration. Dans la console Configuration Manager, vous pouvez accéder à chaque tâche de migration qui a été exécutée ou qui est planifiée pour être exécutée, tant que vous n'avez pas nettoyé les données de migration.

Pour plus d'informations sur les sites sources et la collecte de données, consultez Planification d'une stratégie de hiérarchie source dans System Center Configuration Manager.

## Planifier le nettoyage des données de migration

La dernière étape nécessaire pour terminer la migration consiste à nettoyer les données de migration. Vous pouvez utiliser la commande **Nettoyer les données de migration** après avoir arrêté la collecte des données pour chaque site source de la hiérarchie source. Cette action facultative supprime de la base de données de la hiérarchie de destination l'ensemble des données relatives à la hiérarchie source actuelle.

Lors du nettoyage des données de migration, la plupart des données relatives à la migration sont supprimées de la base de données de la hiérarchie de destination. Cependant, les détails sur les objets migrés sont conservés. Grâce à ces détails, vous pouvez utiliser l'espace de travail **Migration** pour reconfigurer la hiérarchie source contenant les données migrées afin de reprendre la migration à partir de cette hiérarchie source, ou de passer en revue les objets et la propriété de site des objets précédemment migrés.

# Configurer des hiérarchies sources et des sites sources pour la migration vers System Center Configuration Manager

22/06/2018 • 12 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Pour permettre la migration de données vers votre environnement System Center Configuration Manager, vous devez configurer une hiérarchie source Configuration Manager prise en charge et, dans cette hiérarchie, configurer un ou plusieurs sites sources contenant les données à migrer.

> **NOTE**
> Les opérations de migration sont exécutées sur le site de niveau supérieur de la hiérarchie de destination. Si vous configurez la migration à partir d'une console Configuration Manager connectée à un site enfant principal, vous devez donner le temps à la configuration de se répliquer vers le site d'administration centrale, de démarrer, puis de répliquer l'état vers le site principal auquel vous êtes connecté.

Pour spécifier la hiérarchie source et ajouter d'autres sites sources, aidez-vous des informations et des procédures figurant dans les sections suivantes. Au terme de ces procédures, vous pouvez créer des tâches de migration et commencer à migrer les données de la hiérarchie source vers la hiérarchie de destination.

- Spécifier une hiérarchie source pour la migration
- Identifier des sites sources supplémentaires dans la hiérarchie source

## Spécifier une hiérarchie source pour la migration

Pour migrer les données vers votre hiérarchie de destination, vous devez spécifier une hiérarchie source prise en charge qui présente les données à migrer. Par défaut, le site de niveau supérieur de cette hiérarchie devient un site source de la hiérarchie source. Si vous effectuez la migration à partir d'une hiérarchie Configuration Manager 2007, vous pouvez configurer des sites sources supplémentaires pour la migration après avoir collecté les données du site source initial. Si vous effectuez la migration à partir d'une hiérarchie System Center 2012 Configuration Manager ou System Center Configuration Manager, vous n'avez pas besoin de configurer des sites sources supplémentaires pour migrer les données de la hiérarchie source. Ceci est dû au fait que ces versions de Configuration Manager utilisent une base de données partagée qui est disponible sur le site de niveau supérieur dans la hiérarchie source. La base de données partagée présente toutes les informations que vous pouvez migrer.

Utilisez les procédures suivantes pour spécifier une hiérarchie source pour la migration et pour identifier des sites sources supplémentaires dans une hiérarchie Configuration Manager 2007.

Exécutez cette procédure dans une console Configuration Manager qui est connectée à la hiérarchie de destination :

**Pour configurer une hiérarchie source**

1. Dans la console Configuration Manager, cliquez sur **Administration**.
2. Dans l'espace de travail **Administration** , développez **Migration**, puis cliquez sur **Hiérarchie source**.
3. Sous l'onglet **Accueil** , dans le groupe **Migration** , cliquez sur **Spécifier la hiérarchie source**.

4. Dans la boîte de dialogue **Spécifier une hiérarchie source** , pour **Hiérarchie source**, sélectionnez **Nouvelle hiérarchie source**.

5. Dans **Serveur de site Configuration Manager de niveau supérieur**, entrez le nom ou l'adresse IP du site de niveau supérieur d'une hiérarchie source prise en charge.

6. Spécifiez les comptes d'accès au site source qui disposent des autorisations suivantes :

   - Compte du site source : Autorisation **Lecture** pour le fournisseur SMS du site de niveau supérieur spécifié dans la hiérarchie source. Les mises à niveau et le partage des points de distribution nécessitent les autorisations **Modifier** et **Supprimer** sur le site dans la hiérarchie source.

   - Compte de base de données du site source : Autorisation **Lecture** et **Exécution** sur la base de données SQL Server du site de niveau supérieur spécifié dans la hiérarchie source.

     Si vous spécifiez l'utilisation du compte d'ordinateur, Configuration Manager utilise le compte d'ordinateur du site de niveau supérieur de la hiérarchie de destination. Pour cette option, assurez-vous que ce compte est membre du groupe de sécurité **Utilisateurs du modèle COM distribué** dans le domaine où réside le site de niveau supérieur de la hiérarchie source.

7. Pour partager des points de distribution entre des hiérarchies source et de destination, activez la case à cocher **Activer le partage du point de distribution pour ce serveur de site source** . Si vous n'activez pas le partage des points de distribution maintenant, vous pouvez le faire en modifiant les informations d'identification du site source à la fin de la collecte des données.

8. Cliquez sur **OK** pour enregistrer la configuration. La boîte de dialogue **État de la collecte de données** s'ouvre, et la collecte de données démarre automatiquement.

9. À la fin de la collecte des données, cliquez sur **Fermer** pour fermer la boîte de dialogue **État de la collecte de données** et terminer la configuration.

## Identifier des sites sources supplémentaires dans la hiérarchie source

Lorsque vous configurez une hiérarchie source prise en charge, le site de niveau supérieur de cette hiérarchie est automatiquement configuré comme un site source, et les données sont collectées à partir de celui-ci. L'action suivante à effectuer dépend de la version de Configuration Manager qui est exécutée par la hiérarchie source :

- S'il s'agit d'une hiérarchie source Configuration Manager 2007, vous pouvez commencer la migration à partir de ce site source initial ou configurer des sites sources supplémentaires dans la hiérarchie source à la fin de la collecte des données du site source initial. Pour migrer des données qui sont disponibles uniquement sur un site enfant, configurez des sites sources supplémentaires dans une hiérarchie Configuration Manager 2007. Par exemple, vous pouvez configurer des sites sources supplémentaires pour collecter des données relatives au contenu que vous souhaitez migrer quand il est créé sur un site enfant de la hiérarchie source et qu'il n'est pas disponible sur le site de niveau supérieur dans la hiérarchie source.

- Dans le cas d'une hiérarchie source System Center 2012 Configuration Manager ou System Center Configuration Manager, vous n'avez pas besoin de configurer de sites sources supplémentaires. Ceci est dû au fait que ces versions de Configuration Manager utilisent une base de données partagée qui est disponible sur le site de niveau supérieur dans la hiérarchie source. La base de données partagée présente toutes les informations que vous pouvez migrer à partir de tous les sites dans cette hiérarchie source. Les données que vous pouvez migrer sont donc disponibles à partir du site de niveau supérieur de la hiérarchie source.

Quand vous configurez des sites sources supplémentaires dans une hiérarchie source Configuration Manager 2007, vous devez les configurer du haut de la hiérarchie source vers le bas. Vous devez configurer un site parent comme site source pour pouvoir configurer ses sites enfant comme sites source.

Effectuez la procédure suivante pour configurer des sites sources supplémentaires dans une hiérarchie source Configuration Manager 2007 :

**Pour identifier des sites sources supplémentaires dans la hiérarchie source**

1. Dans la console Configuration Manager, cliquez sur **Administration**.
2. Dans l'espace de travail **Administration** , développez **Migration**, puis cliquez sur **Hiérarchie source**.
3. Choisissez le site à configurer comme site source.
4. Dans l' onglet **Accueil** , dans le groupe **Site source** , cliquez sur **Configurer**.
5. Dans la boîte de dialogue **Informations d'identification du site source** , pour des comptes d'accès de site source, définissez les comptes qui disposent des autorisations suivantes :

   - Compte du site source : Autorisation **Lecture** pour le fournisseur SMS du site de niveau supérieur spécifié dans la hiérarchie source. Les mises à niveau et le partage des points de distribution nécessitent les autorisations **Modifier** et **Supprimer** sur le site dans la hiérarchie source.
   - Compte de base de données du site source : Autorisation **Lecture** et **Exécution** sur la base de données SQL Server du site de niveau supérieur spécifié dans la hiérarchie source.

   Si vous spécifiez l'utilisation du compte d'ordinateur, Configuration Manager utilise le compte d'ordinateur du site de niveau supérieur de la hiérarchie de destination. Pour cette option, assurez-vous que ce compte est membre du groupe de sécurité **Utilisateurs du modèle COM distribué** dans le domaine où réside le site de niveau supérieur de la hiérarchie source.
6. Pour partager des points de distribution entre des hiérarchies source et de destination, activez la case à cocher **Activer le partage du point de distribution pour ce serveur de site source** . Si vous n'activez pas le partage des points de distribution maintenant, vous pouvez le faire en modifiant les informations d'identification du site source à la fin de la collecte des données.
7. Cliquez sur **OK** pour enregistrer la configuration. La boîte de dialogue **État de la collecte de données** s'ouvre, et la collecte de données démarre automatiquement.
8. À la fin de la collecte des données, cliquez sur **Fermer** pour terminer la configuration.

# Opérations de migration vers System Center Configuration Manager

22/06/2018 • 20 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Pour la migration dans System Center Configuration Manager, vous pouvez migrer des données et des clients une fois que vous avez collecté des données à partir d'un site source dans une hiérarchie source prise en charge. Utilisez les informations des sections suivantes pour créer et exécuter des tâches de migration pour migrer des données et des clients, puis terminer le processus de migration.

- Créer et modifier des tâches de migration
- Exécuter des tâches de migration
- Mettre à niveau ou réattribuer un point de distribution partagé
- Surveiller l'activité de migration dans l'espace de travail Migration
- Migrer des clients
- Terminer la migration

## Créer et modifier des tâches de migration

Procédez comme suit pour créer des tâches de migration de données, modifier la liste d'exclusions pour les tâches de migration basée sur des regroupements, configurer des points de distribution partagés et modifier des planifications de tâches de migration.

> **NOTE**
> La procédure ci-dessous permet de créer une tâche de migration basée sur des regroupements. Elle s'applique uniquement aux hiérarchies sources qui exécutent une version prise en charge de Configuration Manager 2007. Le type de tâche de migration basée sur les regroupements n'est pas disponible lorsque vous migrez à partir d'une hiérarchie source System Center 2012 Configuration Manager ou System Center Configuration Manager.

#### Créer une tâche de migration par regroupements

1. Dans la console Configuration Manager, choisissez **Administration**.
2. Dans l'espace de travail **Administration**, développez **Migration**, puis choisissez **Tâches de migration**.
3. Sous l'onglet **Accueil**, dans le groupe **Créer**, choisissez **Créer une tâche de migration**.
4. Dans la page **Général** de l'Assistant Création de tâche de migration, configurez les éléments suivants, puis choisissez **OK** :
   - Spécifiez un nom pour la tâche de migration.
   - Dans la liste déroulante **Type de tâche** , sélectionnez **Migration du regroupement**.
5. Dans la page **Sélectionner des regroupements**, configurez les éléments suivants, puis choisissez **Suivant** :
   - Sélectionnez les regroupements que vous souhaitez migrer.

- Si vous souhaitez migrer uniquement les regroupements, sans les objets qui leur sont associés, décochez **Migrer les objets qui sont associés aux regroupements spécifiés**. Si vous décochez cette option, aucun objet associé n'est migré au cours de cette tâche. Vous pouvez alors ignorer les étapes 6 et 7.

6. Dans la page **Sélectionner des objets**, décochez tous les types d'objet ou les objets disponibles spécifiques que vous ne souhaitez pas migrer. Par défaut, tous les types d'objet associés et les objets disponibles sont sélectionnés. Choisissez **Suivant**.
7. Dans la page **Propriété du contenu**, attribuez la propriété du contenu de chaque site source de la liste à un site de la hiérarchie de destination, puis choisissez **Suivant**.
8. Dans la page **Étendue de sécurité**, sélectionnez la ou les étendues de sécurité d'administration basée sur un rôle que vous voulez affecter aux objets à migrer dans cette tâche de migration, puis choisissez **Suivant**.
9. Dans la page **Limitation au regroupement**, configurez un regroupement de la hiérarchie de destination pour limiter l'étendue de chaque regroupement de la liste, puis choisissez **Suivant**. Si aucun regroupement n'est répertorié, choisissez **Suivant**.
10. Dans la page **Remplacement d'un code de site**, affectez un code de site de la hiérarchie de destination pour remplacer le code de site Configuration Manager 2007 de chaque regroupement répertorié, puis choisissez **Suivant**. Si aucun regroupement n'est répertorié, choisissez **Suivant**.
11. Dans la page **Consulter les informations**, choisissez **Enregistrer dans un fichier** pour enregistrer les informations affichées en vue de les consulter ultérieurement. Quand vous êtes prêt à continuer, choisissez **Suivant**.
12. Dans la page **Paramètres**, définissez la période d'exécution de la tâche de migration et tous les autres paramètres nécessaires à cette tâche, puis choisissez **Suivant**.
13. Confirmez les paramètres et mettez fin à l'Assistant.

#### Créer une tâche de migration par objets

1. Dans la console Configuration Manager, choisissez **Administration**.
2. Dans l'espace de travail **Administration**, développez **Migration**, puis choisissez **Tâches de migration**.
3. Sous l'onglet **Accueil**, dans le groupe **Créer**, choisissez **Créer une tâche de migration**.
4. Dans la page **Général** de l'Assistant Création de tâche de migration, configurez les éléments suivants, puis choisissez **Suivant** :
   - Spécifiez un nom pour la tâche de migration.
   - Dans la liste déroulante **Type de tâche** , sélectionnez **Migration d'objet**.
5. Sur la page **Sélectionner des objets** , sélectionnez les types d'objet que vous souhaitez migrer. Par défaut, tous les objets disponibles sont sélectionnés pour chaque type d'objet que vous sélectionnez.
6. Dans la page **Propriété du contenu**, attribuez la propriété du contenu de chaque site source de la liste à un site de la hiérarchie de destination, puis choisissez **Suivant**. Si aucun site source n'est répertorié, choisissez **Suivant**.
7. Dans la page **Étendue de sécurité**, sélectionnez la ou les étendues de sécurité d'administration basée sur un rôle que vous voulez affecter aux objets de cette tâche de migration, puis choisissez **Suivant**.
8. Dans la page **Consulter les informations**, choisissez **Enregistrer dans un fichier** pour enregistrer les informations affichées en vue de les consulter ultérieurement. Quand vous êtes prêt à continuer, choisissez **Suivant**.

9. Dans la page **Paramètres**, définissez la période d'exécution de la tâche de migration et tous les autres paramètres nécessaires à cette tâche. Ensuite, choisissez **Suivant**.

10. Confirmez les paramètres et mettez fin à l'Assistant.

#### Créer une tâche de migration pour migrer des objets modifiés

1. Dans la console Configuration Manager, choisissez **Administration**.

2. Dans l'espace de travail **Administration**, développez **Migration**, puis choisissez **Tâches de migration**.

3. Sous l'onglet **Accueil**, dans le groupe **Créer**, choisissez **Créer une tâche de migration**.

4. Dans la page **Général** de l'Assistant Création de tâche de migration, configurez les éléments suivants, puis choisissez **Suivant** :

   - Spécifiez un nom pour la tâche de migration.
   - Dans la liste déroulante **Type de tâche**, sélectionnez **Objets modifiés après la migration**.

5. Sur la page **Sélectionner des objets** , sélectionnez les types d'objet que vous souhaitez migrer. Par défaut, tous les objets disponibles sont sélectionnés pour chaque type d'objet que vous sélectionnez.

6. Dans la page **Propriété du contenu**, attribuez la propriété du contenu de chaque site source de la liste à un site de la hiérarchie de destination, puis choisissez **Suivant**. Si aucun site source n'est répertorié, choisissez **Suivant**.

7. Dans la page **Étendue de sécurité**, sélectionnez la ou les étendues de sécurité d'administration basée sur un rôle que vous voulez affecter aux objets de cette tâche de migration, puis choisissez **Suivant**.

8. Dans la page **Consulter les informations**, choisissez **Enregistrer dans un fichier** pour enregistrer les informations affichées en vue de les consulter ultérieurement. Quand vous êtes prêt à continuer, choisissez **Suivant**.

9. Dans la page **Paramètres**, définissez la période d'exécution de la tâche de migration et tous les autres paramètres nécessaires à cette tâche. À la différence des autres types de tâches de migration, cette tâche de migration doit remplacer les objets migrés précédemment dans la base de données System Center Configuration Manager. Choisissez **Suivant**.

10. Confirmez les paramètres, puis terminez l'Assistant.

### Modifier la liste d'exclusions pour la migration

1. Dans la console Configuration Manager, choisissez **Administration**.

2. Dans l'espace de travail **Administration**, choisissez **Migration** pour accéder à la liste d'exclusions. Vous pouvez également accéder à la liste des exclusions à partir du nœud **Hiérarchie source** ou **Tâches de migration** .

3. Sous l'onglet **Accueil**, dans le groupe **Migration**, choisissez **Modifier la liste d'exclusion**.

4. Dans la boîte de dialogue **Modifier la liste d'exclusion**, sélectionnez l'objet exclu que vous souhaitez retirer de la liste d'exclusions, puis choisissez **Supprimer**.

5. Choisissez **OK** pour enregistrer les modifications et terminer l'opération. Pour annuler les modifications en cours et restaurer tous les objets que vous avez supprimés, choisissez **Annuler**, puis choisissez **Non**. La suppression des objets est annulée et la boîte de dialogue **Modifier la liste d'exclusion** se ferme.

#### Partager des points de distribution à partir de la hiérarchie source

1. Dans la console Configuration Manager, choisissez **Administration**.

2. Dans l'espace de travail **Administration**, développez **Migration**, choisissez **Hiérarchie source**, puis sélectionnez le site source que vous souhaitez configurer.

3. Sous l'onglet **Accueil**, dans le groupe **Site source**, choisissez **Configurer**.
4. Dans la boîte de dialogue **Informations d'identification du site source**, sélectionnez **Activer le partage du point de distribution pour ce serveur de site source**, puis choisissez **OK**.
5. Une fois la collecte des données terminée, choisissez **Fermer**.

#### Modifier la planification d'une tâche de migration

1. Dans la console Configuration Manager, choisissez **Administration**.
2. Dans l'espace de travail **Administration**, développez **Migration**, puis choisissez **Tâches de migration**.
3. Choisissez la tâche de migration que vous souhaitez modifier. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
4. Dans les propriétés de la tâche de migration, sélectionnez l'onglet **Paramètres**, modifiez l'heure d'exécution de la tâche de migration, puis choisissez **OK**.

## Exécuter des tâches de migration

Pour exécuter une tâche de migration n'a pas encore commencé, suivez la procédure ci-dessous.

1. Dans la console Configuration Manager, choisissez **Administration**.
2. Dans l'espace de travail **Administration**, développez **Migration**, puis choisissez **Tâches de migration**.
3. Choisissez la tâche de migration que vous souhaitez exécuter. Sous l'onglet **Accueil**, dans le groupe **Tâche de migration**, choisissez **Démarrer**.
4. Choisissez **Oui** pour démarrer la tâche de migration.

## Mettre à niveau ou réattribuer un point de distribution partagé

Vous pouvez mettre à niveau un point de distribution pris en charge qui est partagé à partir d'un site source Configuration Manager 2007 (ou réaffecter un point de distribution pris en charge qui est partagé à partir d'un site source System Center Configuration Manager) pour qu'il devienne un point de distribution dans la hiérarchie de destination.

> **IMPORTANT**
> Avant de mettre à niveau un point de distribution de branche Configuration Manager 2007, vous devez désinstaller le logiciel client Configuration Manager 2007 de l'ordinateur du point de distribution de branche. Si le logiciel client Configuration Manager 2007 est installé lorsque vous essayez de mettre à niveau le point de distribution, la mise à niveau échoue et le contenu précédemment déployé sur le point de distribution de branche est supprimé de l'ordinateur.

Caution

Quand vous mettez à niveau ou réaffectez un point de distribution partagé, le rôle de système de site et l'ordinateur du système de site du point de distribution sont supprimés du site source et ajoutés comme point de distribution au site sélectionné dans la hiérarchie de destination.

#### Mettre à niveau ou réattribuer un point de distribution partagé

1. Dans la console Configuration Manager, choisissez **Administration**.
2. Dans l'espace de travail **Administration**, développez **Migration**, puis choisissez **Hiérarchie source**.
3. Sélectionnez le site propriétaire du point de distribution à mettre à niveau, choisissez l'onglet **Points de distribution partagés**, puis sélectionnez le point de distribution éligible que vous souhaitez mettre à niveau ou réaffecter.

4. Sous l'onglet **Point de distribution**, dans le groupe **Point de distribution**, choisissez **Réaffecter**.
5. Dans l'Assistant Réaffectation du point de distribution partagé, spécifiez les paramètres comme si vous installiez un nouveau point de distribution pour la hiérarchie de destination, en ajoutant les configurations suivantes :
   - Dans la page **Conversion du contenu**, prenez connaissance des conseils relatifs à l'espace nécessaire pour convertir le contenu existant. Puis, dans la page **Paramètres du lecteur** de l'Assistant, vérifiez que le lecteur de l'ordinateur du point de distribution sélectionné a la quantité nécessaire d'espace disque disponible.
6. Confirmez les paramètres, puis terminez l'Assistant.

## Surveiller l'activité de migration dans l'espace de travail Migration

Utilisez la console Configuration Manager pour surveiller la migration.

1. Dans la console Configuration Manager, choisissez **Administration**.
2. Dans l'espace de travail **Administration**, développez **Migration**, puis choisissez **Tâches de migration**.
3. Choisissez la tâche de migration que vous souhaitez surveiller.
4. Affichez les détails et l'état de la tâche de migration sélectionnée sur les onglets **Synthèse** et **Objets de la tâche**.

## Migrer des clients

Effectuez la migration des clients vers la hiérarchie de destination après avoir migré les données des clients entre les hiérarchies, mais avant de terminer le processus de migration. La migration de clients entre les hiérarchies implique la désinstallation du logiciel client Configuration Manager des ordinateurs qui sont affectés à la hiérarchie source, puis l'installation du logiciel client Configuration Manager à partir de la hiérarchie de destination. Lorsque vous installez le client à partir de la hiérarchie de destination, vous affectez également le client à un site principal de cette hiérarchie. Pour en savoir plus sur la migration de clients, consultez Planification d'une stratégie de migration de clients dans System Center Configuration Manager.

## Terminer la migration

Procédez comme suit pour terminer la migration à partir de la hiérarchie source.

1. Dans la console Configuration Manager, choisissez **Administration**.
2. Dans l'espace de travail **Administration**, développez **Migration**, puis choisissez **Hiérarchie source**.
3. Dans le cas d'une hiérarchie source Configuration Manager 2007, sélectionnez un site source qui se trouve au niveau inférieur de la hiérarchie source. Dans le cas d'une hiérarchie source System Center 2012 Configuration Manager ou System Center Configuration Manager, sélectionnez le site source disponible.
4. Sous l'onglet **Accueil**, dans le groupe **Nettoyer**, choisissez **Arrêter la collecte de données**.
5. Choisissez **Oui** pour confirmer l'action.
6. Pour une hiérarchie source Configuration Manager 2007, avant de passer à l'étape suivante, répétez les étapes 3, 4 et 5. Effectuez ces étapes au niveau de chaque site de la hiérarchie, du bas vers le haut. Dans le cas d'une hiérarchie source System Center 2012 Configuration Manager ou System Center Configuration Manager, passez à l'étape suivante.
7. Sous l'onglet **Accueil**, dans le groupe **Nettoyer**, choisissez **Nettoyer les données de migration**.
8. Dans la boîte de dialogue **Nettoyer les données de migration**, dans la liste déroulante **Hiérarchie**

**source**, sélectionnez le code de site et le serveur de site du site de niveau supérieur de la hiérarchie source, puis choisissez **OK**.

9. Choisissez **Oui** pour terminer le processus de migration pour la hiérarchie source.

# Sécurité et confidentialité pour la migration vers System Center Configuration Manager

22/06/2018 • 5 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cette rubrique contient les bonnes pratiques en matière de sécurité et les informations de confidentialité pour la migration vers votre environnement System Center Configuration Manager.

## Meilleures pratiques de sécurité pour la migration

Utilisez les meilleures pratiques de sécurité suivantes pour la migration.

| BONNES PRATIQUES DE SÉCURITÉ | PLUS D'INFORMATIONS |
|---|---|
| Utilisez le compte d'ordinateur pour le compte du fournisseur SMS du site source et le compte SQL Server du site source plutôt qu'un compte d'utilisateur. | Si vous devez utiliser un compte d'utilisateur pour la migration, supprimez les détails du compte une fois la migration terminée. |
| Lorsque vous migrez le contenu d'un point de distribution d'un site source vers un point de distribution d'un site de destination, utilisez IPsec. | Bien que le contenu migré soit haché pour détecter la falsification, si les données sont modifiées pendant leur transfert, la migration échoue. |
| Veillez à restreindre et surveiller les utilisateurs administratifs qui peuvent créer des tâches de migration. | L'intégrité de la base de données de la hiérarchie de destination dépend de l'intégrité des données que l'utilisateur administratif décide d'importer à partir de la hiérarchie source. En outre, cet utilisateur administratif peut lire toutes les données de la hiérarchie source. |

**Problèmes de sécurité pour la migration**

La migration présente les problèmes de sécurité suivants :

- Les clients dont l'accès à un site source a été bloqué peuvent être attribués correctement à la hiérarchie de destination, avant que leur enregistrement de client n'ait été migré.

  Bien que Configuration Manager conserve l'état de blocage des clients que vous migrez, ces derniers peuvent être correctement affectés à la hiérarchie de destination si cette affectation a lieu avant la fin de la migration de l'enregistrement de client.

- Les messages d'audit ne sont pas migrés.

Lorsque vous migrez les données d'un site source vers un site de destination, vous perdez toutes les informations d'audit de la hiérarchie source.

## Informations de confidentialité pour la migration

La migration découvre des informations à partir des bases de données de site que vous identifiez dans une infrastructure source et stocke ces données dans la base de données de la hiérarchie de destination. Les informations que System Center Configuration Manager peut découvrir à partir d'un site ou d'une hiérarchie source dépendent des fonctionnalités qui ont été activées dans l'environnement source, ainsi que des opérations de gestion réalisées dans cet environnement.

Pour plus d'informations sur la sécurité et la confidentialité, consultez l'une des rubriques suivantes :

- Pour plus d'informations sur les informations de confidentialité pour Configuration Manager 2007, voir Sécurité et confidentialité pour Configuration Manager 2007 dans la bibliothèque de documentation de Configuration Manager 2007.
- Pour plus d'informations sur les informations de confidentialité pour System Center 2012 Configuration Manager, voir Sécurité et confidentialité pour System Center 2012 Configuration Manager dans la bibliothèque de documentation de System Center 2012 Configuration Manager.
- Pour plus d'informations sur les informations de confidentialité pour System Center Configuration Manager, voir Sécurité et confidentialité pour System Center Configuration Manager.

Vous pouvez migrer l'intégralité des données prises en charge d'un site source vers une hiérarchie de destination ou uniquement une partie de ces données.

La migration n'est pas activée par défaut et nécessite plusieurs étapes de configuration. Les informations relatives à la migration ne sont pas envoyées à Microsoft.

Avant de migrer les données d'une hiérarchie source, analysez vos besoins en matière de confidentialité.

# Commencer à utiliser System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Une fois que vous avez planifié votre topologie de site et de hiérarchie System Center Configuration Manager et que vous êtes prêt à installer ou à mettre à niveau des sites, utilisez les informations fournies dans les rubriques suivantes :

- Installer des sites System Center Configuration Manager
- Mettre à niveau vers System Center Configuration Manager
- Scénarios pour simplifier votre installation de System Center Configuration Manager
- Configurer des sites et des hiérarchies pour System Center Configuration Manager
- Migrer des données entre hiérarchies dans System Center Configuration Manager

# Où trouver le support d'installation pour System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Si vous disposez de licences en volume pour System Center Configuration Manager avec Software Assurance, ou si vous avez acheté des licences pour des licences en volume pour System Center Configuration Manager, vous pouvez télécharger le support source de base pour installer System Center Configuration Manager à partir du Centre de gestion des licences en volume.

Si vous souhaitez acheter des licences en volume pour System Center Configuration Manager, contactez votre revendeur Microsoft ou consultez la page How to purchase through Volume Licensing (Procédure d'achat via des licences en volume). Vous pouvez également télécharger le support nécessaire pour installer une version d'évaluation de System Center Configuration Manager à partir du site web Centre d'évaluation TechNet.

Pour en savoir plus sur le support de base pour Configuration Manager, consultez Versions de base et de mise à jour.

# Informations de référence sur le programme d'installation de System Center Configuration Manager

22/06/2018 • 5 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Le programme d'installation de System Center Configuration Manager fournit des liens vers plusieurs rubriques détaillées dans les sections suivantes. Les informations présentées ici peuvent vous aider à préparer l'installation d'un site ou d'une hiérarchie Configuration Manager, et à prendre certaines décisions relatives à l'installation.

## Avant de commencer

Avant d'installer de nouveaux sites Configuration Manager, veillez à passer en revue les informations suivantes. Celles-ci peuvent vous aider à mettre en œuvre une conception de déploiement réussie :

- Principes de base de System Center Configuration Manager
- Planifier l'infrastructure System Center Configuration Manager
- Préparer l'installation de sites System Center Configuration Manager

## Évaluer la préparation du serveur

Avant de commencer l'installation d'un nouveau site, vérifiez que le serveur de site et les serveurs de système de site distant que vous envisagez d'utiliser pour le site (par exemple, le serveur qui héberge la base de données) respectent tous les prérequis. Les rubriques suivantes de la bibliothèque de documentation peuvent vous aider :

- Configurations prises en charge pour System Center Configuration Manager
- Outil de vérification de la configuration requise

## Clients pour d'autres systèmes d'exploitation

Vous pouvez télécharger le logiciel client pour Configuration Manager à partir du Centre de téléchargement Microsoft pour les systèmes d'exploitation suivants :

- Mac (Apple)
- UNIX
- Linux

Utilisez les liens suivants pour télécharger des clients pour la version de Configuration Manager que vous utilisez :

- Consultez Microsoft System Center Configuration Manager - Clients pour systèmes d'exploitation supplémentaires

## Paramètres et niveaux de données d'utilisation

Quand vous installez votre premier site System Center Configuration Manager, Configuration Manager installe et configure automatiquement un nouveau rôle de système de site, appelé **point de connexion de service**, sur le serveur de site. Les paramètres par défaut du point de connexion de service sont les suivants :

- Mode **En ligne** (un mode hors connexion est également disponible)

- Niveau **Étendu** de collecte de données (deux autres niveaux de collecte de données, De base et Total, sont disponibles)

Quand le rôle de système de site du point de connexion de service est en ligne, Microsoft peut collecter automatiquement des informations d'utilisation et de diagnostic sur Internet. Les informations collectées nous aident à effectuer les tâches suivantes :

- Identifier et résoudre les problèmes
- améliorer nos produits et services ;
- identifier les mises à jour pour Configuration Manager applicables à la version de Configuration Manager que vous utilisez.

**Niveaux de collecte de données**

La collecte de données comprend les trois niveaux suivants :

- **De base** : comprend des données sur l'installation et la mise à niveau, comme le nombre de sites et les fonctionnalités de Configuration Manager qui sont activées. Aucune information personnelle n'est transmise.
- **Étendu** : comprend les données du paramètre de niveau De base et transmet des données relatives à la hiérarchie, à la façon dont chaque fonctionnalité est utilisée (fréquence et durée), ainsi que des informations de diagnostics améliorées telles que l'état de la mémoire de votre serveur quand un blocage du système ou d'une application se produit. Aucune information personnelle n'est transmise.
- **Total** : comprend les données des paramètres De base et Étendu, et envoie également des informations de diagnostics avancées telles que des fichiers système et des instantanés de la mémoire. Cette option peut inclure des informations personnelles, mais nous n'utilisons pas ces informations pour vous identifier, vous contacter ou vous envoyer du contenu publicitaire.

Pour plus d'informations, notamment sur la divulgation des informations collectées par chaque niveau, consultez Données d'utilisation et de diagnostic pour System Center Configuration Manager.

Pour voir la déclaration de confidentialité de System Center Configuration Manager en ligne, accédez à http://go.microsoft.com/fwlink/?LinkID=626527.

# Téléchargeur d'installation pour System Center Configuration Manager

22/06/2018 • 7 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Avant d'exécuter le programme d'installation pour installer ou mettre à niveau un site System Center Configuration Manager, vous pouvez utiliser l'application autonome Téléchargeur d'installation correspondant à la version de Configuration Manager que vous souhaitez installer pour télécharger les fichiers d'installation mis à jour.

L'utilisation des fichiers d'installation mis à jour garantit que votre installation de site utilise les dernières versions des fichiers d'installation clés. En résumé :

- Quand vous utilisez le téléchargeur d'installation pour télécharger des fichiers avant de démarrer le programme d'installation, vous devez spécifier le dossier qui contiendra les fichiers.
- Le compte que vous utilisez pour exécuter le téléchargeur d'installation doit avoir des autorisations **Contrôle intégral** sur le dossier de téléchargement.
- Quand vous exécutez le programme d'installation pour installer ou mettre à niveau un site, vous pouvez lui demander d'utiliser cette copie locale des fichiers téléchargés précédemment. Cela évite au programme d'installation de devoir se connecter à Microsoft au démarrage de l'installation ou de la mise à niveau du site.
- Vous pouvez utiliser la même copie locale des fichiers d'installation pour des installations ou mises à niveau de sites ultérieures.

Le téléchargeur d'installation télécharge les types de fichiers suivants :

- Fichiers redistribuables requis
- Modules linguistiques
- Dernières mises à jour de produit pour le programme d'installation

Vous avez deux options pour exécuter le téléchargeur d'installation :

- Exécuter l'application avec l'interface utilisateur
- Pour les options de ligne de commande, exécuter l'application à l'invite de commandes

## Exécuter le téléchargeur d'installation avec l'interface utilisateur

1. Sur un ordinateur disposant d'un accès Internet, ouvrez l'Explorateur Windows et accédez à **<support_installation_Configuration_Manager>\SMSSETUP\BIN\X64**.
2. Double cliquez sur **Setupdl.exe** pour ouvrir le téléchargeur d'installation.
3. Spécifiez le chemin du dossier où seront hébergés les fichiers d'installation mis à jour, puis cliquez sur **Télécharger**. Le téléchargeur d'installation vérifie les fichiers qui figurent dans le dossier de téléchargement. Il télécharge uniquement les fichiers manquants ou plus récents que les fichiers existants. Le téléchargeur d'installation crée des sous-dossiers pour les langues téléchargées et d'autres sous-dossiers requis.
4. Pour passer en revue les résultats du téléchargement, ouvrez le fichier **ConfigMgrSetup.log** situé dans le répertoire racine du lecteur C.

# Exécuter le téléchargeur d'installation à partir d'une invite de commandes

1. Dans une fenêtre d'invite de commandes, accédez à ***<Support d'installation de Configuration Manager>*\SMSSETUP\BIN\X64**.

2. Exécutez **Setupdl.exe** pour ouvrir le téléchargeur d'installation.

   Vous pouvez utiliser les options de ligne de commande suivantes avec **Setupdl.exe** :

   - **/VERIFY**: utilisez cette option pour vérifier les fichiers dans le dossier de téléchargement, notamment les fichiers de langues. Examinez la liste des fichiers obsolètes dans le fichier ConfigMgrSetup.log situé dans le répertoire racine du lecteur C. Aucun fichier n'est téléchargé lorsque vous utilisez cette option.

   - **/VERIFYLANG**: utilisez cette option pour vérifier les fichiers de langues dans le dossier de téléchargement. Examinez la liste des fichiers de langue obsolètes dans le fichier ConfigMgrSetup.log situé dans le répertoire racine du lecteur C.

   - **/LANG**: utilisez cette option pour télécharger uniquement les fichiers de langues dans le dossier de téléchargement.

   - **/NOUI**: utilisez cette option pour démarrer le téléchargeur d'installation sans afficher l'interface utilisateur. Quand vous utilisez cette option, vous devez spécifier le **chemin de téléchargement** dans le cadre de la commande, à l'invite de commandes.

   - **<chemin_téléchargement>**: vous pouvez spécifier le chemin du dossier de téléchargement pour démarrer automatiquement la vérification ou le processus de téléchargement. Vous devez spécifier le chemin de téléchargement quand vous utilisez l'option **/NOUI**. Si vous ne spécifiez pas un chemin de téléchargement, vous devez le faire à l'ouverture du téléchargeur d'installation. Le téléchargeur d'installation crée le dossier si celui-ci n'existe pas.

   Exemples de commandes :

   - **setupd <chemin_téléchargement>**
     - Le téléchargeur d'installation démarre, vérifie les fichiers dans le dossier de téléchargement spécifié, puis télécharge uniquement les fichiers manquants ou présentant des versions plus récentes que les fichiers existants.
   - **setupdl /VERIFY <chemin_téléchargement>**
     - Le téléchargeur d'installation démarre, puis vérifie les fichiers dans le dossier de téléchargement spécifié.
   - **setupdl /NOUI <chemin_téléchargement>**
     - Le téléchargeur d'installation démarre, vérifie les fichiers dans le dossier de téléchargement spécifié, puis télécharge uniquement les fichiers manquants ou plus récents que les fichiers existants.
   - **setupdl /LANG <chemin_téléchargement>**
     - Le téléchargeur d'installation démarre, vérifie les fichiers de langue dans le dossier de téléchargement spécifié, puis télécharge uniquement les fichiers de langue manquants ou plus récents que les fichiers existants.
   - **setupdl /VERIFY**
     - Le téléchargeur d'installation démarre, et vous devez alors spécifier le chemin d'accès vers le dossier de téléchargement. Ensuite, une fois que vous avez cliqué sur **Vérifier**, le téléchargeur

d'installation vérifie les fichiers dans le dossier de téléchargement.

3. Pour passer en revue les résultats du téléchargement, ouvrez le fichier **ConfigMgrSetup.log** situé dans le répertoire racine du lecteur C.

# Outil de vérification des prérequis pour System Center Configuration Manager

22/06/2018 • 12 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Avant d'exécuter le programme d'installation pour installer ou mettre à niveau un site System Center Configuration Manager, ou avant d'installer un rôle de système de site sur un nouveau serveur, vous pouvez utiliser cette application autonome (**Prereqchk.exe**) de la version de Configuration Manager que vous voulez utiliser pour vérifier l'état de préparation du serveur. Utilisez l'Outil de vérification des prérequis pour identifier et résoudre les problèmes susceptibles de bloquer l'installation d'un site ou d'un rôle de système de site.

> **NOTE**
> L'Outil de vérification des prérequis s'exécute toujours pendant l'installation.

Par défaut, quand l'Outil de vérification des prérequis s'exécute :

- Il valide le serveur sur lequel il s'exécute.
- Il recherche un serveur de site sur l'ordinateur local et exécute uniquement les vérifications applicables au site.
- Si aucun site existant n'est détecté, toutes les règles de vérification des prérequis sont exécutées.
- Il vérifie les règles pour s'assurer de la présence des logiciels et des paramètres nécessaires à l'installation. Il est possible qu'un logiciel requis nécessite des configurations ou des mises à jour logicielles supplémentaires qui ne sont pas vérifiées par l'Outil de vérification des prérequis.
- Il enregistre ses résultats dans le fichier journal **ConfigMgrPrereq.log** sur le lecteur système de l'ordinateur. Le fichier journal peut contenir des informations supplémentaires qui n'apparaissent pas dans l'interface de l'application.

Quand vous exécutez l'Outil de vérification des prérequis à l'invite de commandes et spécifiez des options de ligne de commande :

- L'Outil de vérification des prérequis effectue uniquement les vérifications associées au serveur de site ou aux systèmes de site que vous spécifiez sur la ligne de commande.
- Pour vérifier un ordinateur distant, votre compte d'utilisateur doit disposer des droits d'administrateur sur cet ordinateur.

Pour plus d'informations sur les vérifications effectuées par l'Outil de vérification des prérequis, consultez Liste des vérifications des prérequis pour System Center Configuration Manager.

## Copier les fichiers de l'Outil de vérification des prérequis sur un autre ordinateur

1. Dans l'Explorateur Windows, accédez à l'un des emplacements suivants :
   - ***<Support d'installation de Configuration Manager>*\SMSSETUP\BIN\X64**
   - ***<Répertoire d'installation de Configuration Manager>*\BIN\X64**
2. Copiez les fichiers suivants vers le dossier de destination sur l'autre ordinateur :
   - Prereqchk.exe

- Prereqcore.dll
- Basesql.dll
- Basesvr.dll
- Baseutil.dll

## Exécuter l'Outil de vérification des prérequis avec les vérifications par défaut

1. Dans l'Explorateur Windows, accédez à l'un des emplacements suivants :
   - **<*Support d'installation de Configuration Manager*>\SMSSETUP\BIN\X64**
   - **<*Répertoire d'installation de Configuration Manager*>\BIN\X64**
2. Exécutez **prereqchk.exe** pour démarrer l'Outil de vérification des prérequis.
   L'Outil de vérification des prérequis détecte les sites existants et, une fois identifiés, vérifie s'ils sont prêts pour une mise à niveau. Si aucun site n'est trouvé, toutes les vérifications sont effectuées. La colonne **Type de site** fournit des informations sur le serveur de site ou le système de site auquel la règle est associée.

## Exécuter l'Outil de vérification des prérequis à partir d'une invite de commandes pour toutes les vérifications par défaut

1. Ouvrez une fenêtre d'invite de commandes, puis accédez à l'un des répertoires suivants :
   - **<*Support d'installation de Configuration Manager*>\SMSSETUP\BIN\X64**
   - **<*Répertoire d'installation de Configuration Manager*>\BIN\X64**
2. Entrez **prereqchk.exe /LOCAL** pour démarrer l'Outil de vérification des prérequis et effectuer toutes les vérifications des prérequis sur le serveur.

## Exécuter l'Outil de vérification des prérequis à partir d'une invite de commandes pour utiliser des options

1. Ouvrez une fenêtre d'invite de commandes, puis accédez à l'un des répertoires suivants :
   - **<*Support d'installation de Configuration Manager*>\SMSSETUP\BIN\X64**
   - **<*Répertoire d'installation de Configuration Manager*>\BIN\X64**
2. Entrez **prereqchk.exe** en ajoutant une ou plusieurs des options de ligne de commande suivantes.

   Par exemple, pour vérifier un site principal, vous pouvez spécifier ce qui suit :

   **prereqchk.exe [/NOUI] /PRI /SQL <Nom de domaine complet de SQL Server> /SDK <Nom de domaine complet du fournisseur SMS> [/JOIN <Nom de domaine complet du site d'administration centrale>] [/MP <Nom de domaine complet du point de gestion>] [/DP <Nom de domaine complet du point de distribution>]**

   **Serveur de site d'administration centrale** :

   - **/NOUI**

     Non obligatoire. Démarre l'Outil de vérification des prérequis sans afficher l'interface utilisateur. Vous devez spécifier cette option avant toute autre option dans la ligne de commande.

   - **/CAS**

     Obligatoire. Vérifie que l'ordinateur local répond à la configuration requise pour le site d'administration centrale.

- **/SQL <*FQDN de SQL Server*>**

  Obligatoire. À l'aide du nom de domaine complet, vérifie que l'ordinateur spécifié présente la configuration requise pour que SQL Server puisse héberger la base de données du site Configuration Manager.

- **/SDK <*FQDN du fournisseur SMS*>**

  Obligatoire. Vérifie que l'ordinateur spécifié répond à la configuration requise pour le fournisseur SMS.

- **/Ssbport**

  Non obligatoire. Vérifie qu'une exception de pare-feu est en place pour autoriser la communication sur le port SQL Server Service Broker (SSB). Le port SSB par défaut est 4022.

- **InstallDir <*Chemin d'installation de Configuration Manager*>**

  Non obligatoire. Vérifie l'espace disque minimal nécessaire pour l'installation du site.

**Serveur de site principal** :

- **/NOUI**

  Non obligatoire. Démarre l'Outil de vérification des prérequis sans afficher l'interface utilisateur. Vous devez spécifier cette option avant toute autre option dans la ligne de commande.

- **/PRI**

  Obligatoire. Vérifie que l'ordinateur local répond à la configuration requise pour le site principal.

- **/SQL <*FQDN de SQL Server*>**

  Obligatoire. Vérifie que l'ordinateur spécifié présente la configuration requise pour que SQL Server puisse héberger la base de données du site Configuration Manager.

- **/SDK <*FQDN du fournisseur SMS*>**

  Obligatoire. Vérifie que l'ordinateur spécifié répond à la configuration requise pour le fournisseur SMS.

- **/JOIN <*FQDN du site d'administration centrale*>**

  Non obligatoire. Vérifie que l'ordinateur local est conforme à la configuration requise pour se connecter au serveur de site d'administration centrale.

- **/MP <*FQDN du point de gestion*>**

  Non obligatoire. Vérifie que l'ordinateur spécifié répond à la configuration requise pour le rôle de système de site du point de gestion. Cette option est prise en charge uniquement avec l'option **/PRI** .

- **/DP <*FQDN du point de distribution*>**

  Non obligatoire. Vérifie que l'ordinateur spécifié répond à la configuration requise pour le rôle de système de site du point de distribution. Cette option est prise en charge uniquement avec l'option **/PRI** .

- **/Ssbport**

  Non obligatoire. Vérifie qu'une exception de pare-feu est en place pour permettre la communication sur le port SSB. Le port SSB par défaut est 4022.

- **InstallDir <*Chemin d'installation de Configuration Manager*>**

Non obligatoire. Vérifie l'espace disque minimal nécessaire pour l'installation du site.

**Serveur de site secondaire** :

- **/NOUI**

  Non obligatoire. Démarre l'Outil de vérification des prérequis sans afficher l'interface utilisateur. Vous devez spécifier cette option avant toute autre option dans la ligne de commande.

- **/SEC <*FQDN du serveur de site secondaire*>**

  Obligatoire. Vérifie que l'ordinateur spécifié répond aux exigences pour le site secondaire.

- **/INSTALLSQLEXPRESS**

  Non obligatoire. Vérifie que SQL Server Express peut être installé sur l'ordinateur spécifié.

- **/Ssbport**

  Non obligatoire. Vérifie qu'une exception de pare-feu est en place pour permettre la communication sur le port SSB. Le port SSB par défaut est 4022.

- **/Sqlport**

  Non obligatoire. Vérifie qu'une exception de pare-feu est en place pour permettre la communication pour le port de service SQL Server, et que le port n'est pas utilisé par une autre instance nommée de SQL Server. Le port par défaut est 1433.

- **InstallDir <*Chemin d'installation de Configuration Manager*>**

  Non obligatoire. Vérifie l'espace disque minimal nécessaire pour l'installation du site.

- **/SourceDir**

  Non obligatoire. Vérifie que le compte d'ordinateur du site secondaire peut accéder au dossier qui héberge les fichiers sources d'installation.

**Console Configuration Manager** :

- **/Adminui**

  Obligatoire. Vérifie que l'ordinateur local présente la configuration requise pour l'installation de Configuration Manager.

3. L'interface utilisateur de l'Outil de vérification des prérequis affiche la liste des problèmes détectés dans la section **Résultat de la vérification de configuration requise** .
   - Cliquez sur un élément de la liste pour obtenir plus d'informations sur la façon de résoudre le problème.
   - Vous devez résoudre tous les éléments de la liste qui présentent un état **Erreur** avant d'installer le serveur de site, le système de site ou la console Configuration Manager.
   - Vous pouvez également ouvrir le fichier **ConfigMgrPrereq.log** à la racine du lecteur système pour examiner les résultats de l'Outil de vérification des prérequis. Le fichier journal peut contenir des informations supplémentaires qui ne sont pas affichées dans l'interface utilisateur de l'Outil de vérification des prérequis.

# Liste des vérifications des prérequis pour System Center Configuration Manager

22/06/2018 • 34 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les sections suivantes détaillent les vérifications des prérequis disponibles.

Pour obtenir des informations sur l'utilisation de l'Outil de vérification des prérequis, consultez Outil de vérification des prérequis.

## Vérifications des prérequis pour les droits de sécurité

Le tableau ci-dessous répertorie les vérifications qu'effectue l'Outil de vérification des prérequis en relation avec les droits de sécurité.

| VÉRIFICATION EFFECTUÉE | EXPLICATION | NIVEAU DE GRAVITÉ | SITE D'APPLICATION |
|---|---|---|---|
| **Droits d'administrateur sur le site d'administration centrale** | Vérifie que le compte d'utilisateur qui exécute le programme d'installation de Configuration Manager dispose de droits d'**administrateur** sur l'ordinateur du site d'administration centrale. | Erreur | Site principal |
| **Droits d'administration sur le site principal développé** | Vérifie que le compte d'utilisateur qui exécute le programme d'installation dispose de droits d'**administrateur** sur le site principal autonome qui sera développé. | Erreur | Site d'administration centrale |
| **Droits d'administration sur le système de site** | Vérifie que le compte d'utilisateur qui exécute le programme d'installation de Configuration Manager dispose de droits d'**administrateur** sur l'ordinateur du système de site. | Erreur | Site d'administration centrale,<br>Site principal,<br>Site secondaire |
| **Droits d'administration de l'ordinateur du site d'administration centrale sur le site principal développé** | Vérifie que le compte d'ordinateur du site d'administration centrale dispose de droits d'**administrateur** sur le site principal autonome qui sera développé. | Erreur | Site d'administration centrale |

| VÉRIFICATION EFFECTUÉE | EXPLICATION | NIVEAU DE GRAVITÉ | SITE D'APPLICATION |
|---|---|---|---|
| **Connexion à SQL Server sur le site d'administration centrale** | Vérifie que le compte d'utilisateur qui exécute le programme d'installation de Configuration Manager sur le site principal pour joindre une hiérarchie existante détient le rôle d'**administrateur système** sur l'instance SQL Server du site d'administration centrale. | Erreur | Site principal |
| **Droits d'administration du compte d'ordinateur serveur de site** | Vérifie que le compte d'ordinateur serveur de site dispose de droits d'**administrateur** sur les ordinateurs SQL Server et de point de gestion. | Erreur | Site principal, SQL Server |
| **Communication du système de site au serveur SQL Server** | Vérifie qu'un nom de principal du service (SPN) est enregistré dans les services de domaine Active Directory pour le compte destiné à exécuter le service SQL Server de l'instance SQL Server qui héberge la base de données du site Configuration Manager. Un SPN valide doit être enregistré dans les services de domaine Active Directory pour prendre en charge l'authentification Kerberos. | Avertissement | Site secondaire, Point de gestion |
| **Mode de sécurité SQL Server** | Vérifie que SQL Server est configuré pour la sécurité de l'authentification Windows. | Avertissement | SQL Server |
| **Droits d'administrateur système SQL Server** | Vérifie que le compte d'utilisateur exécutant le programme d'installation de Configuration Manager a le rôle **administrateur système** sur l'instance SQL Server sélectionnée pour l'installation de la base de données de site. Cette vérification échoue également lorsque le programme d'installation ne peut pas accéder à l'instance pour que SQL Server vérifie les autorisations. | Erreur | SQL Server |

| VÉRIFICATION EFFECTUÉE | EXPLICATION | NIVEAU DE GRAVITÉ | SITE D'APPLICATION |
|---|---|---|---|
| **Droits d'administrateur système SQL Server pour le site de référence** | Vérifie que le compte d'utilisateur exécutant le programme d'installation de Configuration Manager a le rôle **administrateur système** sur l'instance de rôle SQL Server sélectionnée comme base de données de site de référence. Les autorisations du rôle d'**administrateur système** SQL Server sont nécessaires pour modifier la base de données de site. | Erreur | SQL Server |

## Vérifications des prérequis pour les dépendances Configuration Manager

Le tableau ci-dessous répertorie les vérifications qu'effectue l'Outil de vérification des prérequis en rapport avec les dépendances Configuration Manager.

| VÉRIFICATION EFFECTUÉE | EXPLICATION | NIVEAU DE GRAVITÉ | SITE D'APPLICATION |
|---|---|---|---|
| **Mappages de migration actifs sur le site principal cible** | Vérifie qu'il n'existe pas de mappages de migration actifs aux sites principaux. | Erreur | Site d'administration centrale |
| **Réplica de point de gestion actif** | Vérifie s'il existe un réplica de point de gestion actif. | Erreur | Site principal |
| **Droits d'administration sur le point de distribution** | Vérifie que le compte d'utilisateur qui exécute le programme d'installation dispose de droits d'**administrateur** sur l'ordinateur du point de distribution. | Avertissement | Point de distribution |
| **Droits d'administration sur le point de gestion** | Vérifie que le compte d'ordinateur du serveur de site dispose de droits d'**administrateur** sur l'ordinateur du point de gestion et du point de distribution. | Avertissement | Point de gestion |
| **Partage administratif (système de site)** | Vérifie que les partages administratifs requis sont présents sur l'ordinateur du système de site. | Avertissement | Point de gestion |
| **Compatibilité des applications** | Vérifie que les applications actuelles sont compatibles avec le schéma d'application. | Avertissement | Site d'administration centrale,<br>Site principal |

| VÉRIFICATION EFFECTUÉE | EXPLICATION | NIVEAU DE GRAVITÉ | SITE D'APPLICATION |
|---|---|---|---|
| **Compatible BITS** | Vérifie que le service de transfert intelligent en arrière-plan (BITS) est installé sur l'ordinateur du système de site du point de gestion. L'échec de cette vérification signifie que le service BITS n'est pas installé, que le composant de compatibilité IIS (Internet Information Services) 6.0 WMI (Windows Management Instrumentation) pour IIS 7.0 n'est pas installé sur l'ordinateur ou sur l'hôte IIS distant, ou que le programme d'installation n'a pas pu vérifier les paramètres IIS distants, car les composants communs IIS n'étaient pas installés sur l'ordinateur serveur de site. | Erreur | Point de gestion |
| **Service BITS installé** | Vérifie que le service BITS est installé dans IIS. | Avertissement | Point de gestion |
| **Classement insensible à la casse sur SQL Server** | Vérifie que l'installation SQL Server utilise un classement qui ne respecte pas la casse, par exemple, SQL_Latin1_General_CP1_CI_AS. | Erreur | SQL Server |
| **Déterminer la version et le code du site principal autonome** | Vérifie que le site principal que vous prévoyez de développer est un site principal autonome et qu'il dispose de la même version de Configuration Manager, mais d'un code de site différent, que le site d'administration centrale à installer. | Erreur | Site d'administration centrale,<br>Site principal |
| **Rechercher des références de regroupement incompatibles** | Au cours d'une mise à niveau, cette vérification contrôle que les regroupements font uniquement référence à des regroupements du même type. | Erreur | Site d'administration centrale |
| **Version du client sur l'ordinateur du point de gestion** | Vérifie que vous installez le point de gestion sur un ordinateur dont la version du client Configuration Manager installé n'est pas différente. | Erreur | Point de gestion |

| VÉRIFICATION EFFECTUÉE | EXPLICATION | NIVEAU DE GRAVITÉ | SITE D'APPLICATION |
|---|---|---|---|
| **Configuration de l'utilisation de mémoire de SQL Server** | Vérifie si SQL Server est configuré pour une utilisation de mémoire illimitée. Vous devez configurer la mémoire de SQL Server avec une limite maximale. | Avertissement | SQL Server |
| **Instance SQL Server dédiée** | Vérifie si une instance dédiée du serveur SQL Server est configurée pour héberger la base de données de site Configuration Manager. Si un autre site utilise l'instance, vous devez sélectionner une autre instance pour le nouveau site à utiliser. Vous pouvez également désinstaller l'autre site ou déplacer sa base de données vers une autre instance du serveur SQL Server. | Erreur | Site d'administration centrale,<br>Site principal,<br>Site secondaire |
| **Composants serveur Configuration Manager existants sur le serveur** | Vérifie qu'un rôle de serveur de site ou de système de site n'est pas déjà installé sur l'ordinateur sélectionné pour l'installation du site. | Erreur | Site d'administration centrale,<br>Site principal,<br>Site secondaire |
| **Exception de pare-feu pour le serveur SQL Server** | Vérifie si le Pare-feu Windows est désactivé ou s'il existe une exception du Pare-feu Windows applicable à SQL Server. Vous devez autoriser l'accès à distance à Sqlservr.exe ou aux ports TCP obligatoires. Par défaut, SQL Server écoute le port TCP 1433 et SQL Server Service Broker (SSB) utilise le port TCP 4022. | Erreur | Site d'administration centrale,<br>Site principal,<br>Site secondaire,<br>Point de gestion |
| **Exception de pare-feu pour SQL Server (site principal autonome)** | Vérifie si le Pare-feu Windows est désactivé ou s'il existe une exception du Pare-feu Windows applicable à SQL Server. Vous devez autoriser l'accès à distance à Sqlservr.exe ou aux ports TCP obligatoires. Par défaut, SQL Server écoute le port TCP 1433 et SSB utilise le port TCP 4022. | Avertissement | Site principal (autonome uniquement) |

| VÉRIFICATION EFFECTUÉE | EXPLICATION | NIVEAU DE GRAVITÉ | SITE D'APPLICATION |
|---|---|---|---|
| **Exception de pare-feu pour SQL Server pour le point de gestion** | Vérifie si le Pare-feu Windows est désactivé ou s'il existe une exception du Pare-feu Windows applicable à SQL Server. | Avertissement | Point de gestion |
| **Configuration HTTPS IIS** | Vérifie les liaisons de site web IIS pour le protocole de communication HTTPS. Lorsque vous installez des rôles de site qui exigent HTTPS, vous devez configurer les liaisons de site IIS sur le serveur spécifié avec un certificat d'infrastructure à clé publique (PKI). | Avertissement | Point de gestion,<br>Point de distribution |
| **Service IIS en cours d'exécution** | Vérifie qu'IIS est installé et en cours d'exécution sur l'ordinateur pour installer le point de gestion ou le point de distribution. | Erreur | Point de gestion,<br>Point de distribution |
| **Reproduire le classement du site principal développé** | Vérifie que la base de données de site du site principal autonome que vous prévoyez de développer a le même classement que la base de données de site au niveau du site d'administration centrale. | Erreur | Site d'administration centrale |
| **La bibliothèque RDC (compression différentielle à distance) de Microsoft est enregistrée** | Vérifie que la bibliothèque RDC est enregistrée sur le serveur de site Configuration Manager. | Erreur | Site d'administration centrale,<br>Site principal,<br>Site secondaire |
| **Microsoft Windows Installer** | Vérifie la version de Windows Installer. L'échec de cette vérification signifie que le programme d'installation n'a pas pu vérifier la version ou que la version installée n'est pas conforme à la configuration minimale requise de Windows Installer 4.5. | Erreur | Site d'administration centrale,<br>Site principal,<br>Site secondaire |
| **Microsoft XML Core Services 6.0 (MSXML60)** | Vérifie que MSXML version 6.0 ou ultérieure est installé sur l'ordinateur. | Avertissement | Site d'administration centrale,<br>Site principal,<br>Site secondaire,<br>Console Configuration Manager,<br>Point de gestion,<br>Point de distribution |

| VÉRIFICATION EFFECTUÉE | EXPLICATION | NIVEAU DE GRAVITÉ | SITE D'APPLICATION |
|---|---|---|---|
| **Version minimale de .NET Framework pour la console Configuration Manager** | Vérifie si Microsoft .NET Framework 4.0 est installé sur l'ordinateur de la console Configuration Manager. Vous pouvez télécharger .NET Framework 4.0 depuis le Centre de téléchargement Microsoft. | Erreur | Console Configuration Manager |
| **Version minimale de .NET Framework pour le serveur de site Configuration Manager** | Vérifie si .NET Framework 3.5 est installé sur le serveur de site Configuration Manager. Pour Windows Server 2008, vous pouvez télécharger Microsoft .NET Framework 3.5 depuis le Centre de téléchargement Microsoft. Pour Windows Server 2008 R2, vous pouvez activer .NET Framework 3.5 en tant que fonctionnalité dans le Gestionnaire de serveur. | Erreur | Site d'administration centrale,<br>Site principal,<br>Site secondaire |
| **Version .NET Framework minimale pour l'installation de l'édition SQL Server Express pour un site secondaire Configuration Manager** | Vérifie que .NET Framework 4.0 est installé sur des ordinateurs de site secondaire Configuration Manager pour l'installation de SQL Server Express. | Erreur | Site secondaire |
| **Classement de base de données parent/enfant** | Vérifie que le classement de la base de données du site correspond au classement de la base de données du site parent. Tous les sites d'une même hiérarchie doivent utiliser le même classement de base de données. | Erreur | Site principal,<br>Site secondaire |
| **PowerShell 2.0 sur le serveur de site** | Vérifie que Windows PowerShell version 2.0 ou ultérieure est installé sur le serveur de site pour le connecteur Exchange de Configuration Manager. Pour plus d'informations sur PowerShell 2.0, consultez l'article 968930 de la Base de connaissances Microsoft. | Avertissement | Site principal |
| **Nom de domaine complet principal** | À l'aide d'un nom de domaine complet, vérifie que le nom NetBIOS de l'ordinateur correspond au nom d'hôte local (première étiquette du nom de domaine complet) de l'ordinateur. | Erreur | Site d'administration centrale,<br>Site principal,<br>Site secondaire,<br>SQL Server |

| VÉRIFICATION EFFECTUÉE | EXPLICATION | NIVEAU DE GRAVITÉ | SITE D'APPLICATION |
|---|---|---|---|
| **Connexion à distance avec WMI sur le site secondaire** | Vérifie si le programme d'installation est en mesure d'établir une connexion à distance avec WMI sur le serveur de site secondaire. | Avertissement | Site secondaire |
| **Classement SQL Server obligatoire** | Vérifie que l'instance pour SQL Server et la base de données du site Configuration Manager, si elle est installée, est configurée pour utiliser le classement SQL_Latin1_General_CP1_CI_AS, sauf si vous utilisez un système d'exploitation de langue chinoise qui nécessite la prise en charge de la norme GB18030.<br><br>Pour plus d'informations sur la modification des classements de votre instance SQL Server et des bases de données, consultez Définition et modification des classements dans la documentation en ligne de SQL Server 2008 R2. Pour plus d'informations sur l'activation de la prise en charge de la norme GB18030, consultez Prise en charge internationale dans System Center Configuration Manager. | Erreur | Site d'administration centrale,<br>Site principal,<br>Site secondaire |
| **Configurer le dossier source** | Vérifie que le compte d'ordinateur du site secondaire dispose d'autorisations de système de fichiers NFTS en **Lecture** et d'autorisations de partage en **Lecture** sur le dossier source d'installation et le partage.<br><br>**Remarque** : Le compte d'ordinateur de site secondaire doit être un **administrateur** sur l'ordinateur si vous utilisez des partages administratifs (par exemple, C$ et D$). | Erreur | Site secondaire |

| VÉRIFICATION EFFECTUÉE | EXPLICATION | NIVEAU DE GRAVITÉ | SITE D'APPLICATION |
|---|---|---|---|
| **Version de la source d'installation** | Vérifie que la version de Configuration Manager dans le dossier source que vous avez spécifié pour l'installation du site secondaire correspond à la version de Configuration Manager du site principal. | Erreur | Site secondaire |
| **Code de site en cours d'utilisation** | Vérifie que le code de site que vous avez spécifié n'est pas en cours d'utilisation dans la hiérarchie Configuration Manager. Vous devez spécifier un code de site unique pour ce site. | Erreur | Site principal |
| **L'ordinateur du fournisseur SMS a le même domaine que le serveur de site** | Vérifie si un ordinateur qui exécute une instance du fournisseur SMS a le même domaine que le serveur de site. | Erreur | Fournisseur SMS |
| **Édition SQL Server** | Vérifie que l'édition de SQL Server sur le site n'est pas SQL Server Express. | Erreur | SQL Server |
| **SQL Server Express sur un site secondaire** | Vérifie que SQL Server Express peut s'installer correctement sur l'ordinateur serveur de site pour un site secondaire. | Erreur | Site secondaire |
| **SQL Server sur l'ordinateur du site secondaire** | Vérifie que SQL Server est installé sur l'ordinateur du site secondaire. Vous ne pouvez pas installer SQL Server sur un système de site distant.<br><br>**Avertissement** : Cette vérification s'applique uniquement lorsque vous indiquez au programme d'installation d'utiliser une instance existante de SQL Server. | Erreur | Site secondaire |

| VÉRIFICATION EFFECTUÉE | EXPLICATION | NIVEAU DE GRAVITÉ | SITE D'APPLICATION |
|---|---|---|---|
| **Allocation de mémoire pour le processus SQL Server** | Vérifie que SQL Server réserve un minimum de 8 Go de mémoire pour le site d'administration centrale et le site principal, ainsi qu'un minimum de 4 Go de mémoire pour le site secondaire. Pour plus d'informations sur la définition d'une quantité fixe de mémoire à l'aide de SQL Server Management Studio, consultez Procédure : définir une quantité fixe de mémoire (SQL Server Management Studio).<br><br>**Remarque** : Cette vérification n'est pas applicable à SQL Server Express sur un site secondaire qui est limité à 1 Go de mémoire réservée. | Avertissement | SQL Server |
| **Compte en cours d'exécution du service SQL Server** | Vérifie que le compte d'ouverture de session pour le service SQL Server n'est pas un compte d'utilisateur local ou SERVICE LOCAL. Vous devez configurer le service SQL Server pour utiliser un compte de domaine valide, SERVICE RÉSEAU ou SYSTÈME LOCAL. | Erreur | Site d'administration centrale,<br>Site principal,<br>Site secondaire |
| **Port TCP SQL Server** | Vérifie que TCP est activé pour l'instance SQL Server et qu'il est configuré pour utiliser un port statique. | Erreur | SQL Server |
| **Version de SQL Server** | Vérifie qu'une version prise en charge de SQL Server est installée sur le serveur de base de données de site spécifié. Pour plus d'informations, consultez Prise en charge des versions de SQL Server pour System Center Configuration Manager. | Erreur | SQL Server |

| VÉRIFICATION EFFECTUÉE | EXPLICATION | NIVEAU DE GRAVITÉ | SITE D'APPLICATION |
|---|---|---|---|
| **Version du système d'exploitation du système de site non prise en charge pour la mise à niveau** | Pendant une mise à niveau, cette règle vérifie si des rôles de système de site autres que des points de distribution sont installés sur les ordinateurs exécutant Windows Server 2008 ou une version antérieure.<br><br>**Remarque** : Étant donné que cette vérification ne peut pas résoudre l'état des rôles de système de site installés dans Azure ou pour le stockage cloud utilisé par Microsoft Intune quand vous intégrez Intune avec Configuration Manager, vous pouvez ignorer les avertissements pour ces rôles et les considérer comme faux positifs. | Avertissement | Site principal,<br>Site secondaire |
| **Rôle de système de site « Point de synchronisation Asset Intelligence » non pris en charge sur le site principal développé** | Vérifie que le rôle de système site de point de synchronisation Asset Intelligence n'est pas installé sur le site principal autonome que vous développez. | Erreur | Site d'administration centrale |
| **Rôle de système de site « Point Endpoint Protection » non pris en charge sur le site principal développé** | Vérifie que le rôle de système site de point Endpoint Protection n'est pas installé sur le site principal autonome que vous développez. | Erreur | Site d'administration centrale |
| **Rôle de système de site « Connecteur Microsoft Intune » non pris en charge sur le site principal développé** | Vérifie que le rôle de système site Connecteur Microsoft Intune n'est pas installé sur le site principal autonome que vous développez. | Erreur | Site d'administration centrale |
| **Outil de migration de l'état utilisateur (USMT) installé** | Vérifie si le composant Outil de migration de l'état utilisateur (USMT) du Kit de déploiement et d'évaluation Windows (ADK) pour Windows 8.1 est installé. | Erreur | Site d'administration centrale,<br>Site principal (autonome uniquement) |
| **Valider le nom de domaine complet de l'ordinateur SQL Server** | Vérifie que le nom de domaine complet spécifié pour l'ordinateur SQL Server est valide. | Erreur | SQL Server |

| VÉRIFICATION EFFECTUÉE | EXPLICATION | NIVEAU DE GRAVITÉ | SITE D'APPLICATION |
|---|---|---|---|
| **Vérifier la version du site d'administration centrale** | Vérifie que le site d'administration centrale dispose de la même version de Configuration Manager. | Erreur | Site principal |
| **Vérifier que le serveur de site dispose des autorisations requises pour être publié dans Active Directory** | Vérifie que le compte d'ordinateur du serveur de site dispose des autorisations **Contrôle total** vers le conteneur **System Management** dans le domaine Active Directory. Pour plus d'informations sur les options de configuration des autorisations obligatoires, consultez Préparer Active Directory pour la publication de site.<br><br>**Remarque** : Vous pouvez ignorer cet avertissement si vous avez vérifié manuellement les autorisations. | Avertissement | Site d'administration centrale,<br>Site principal,<br>Site secondaire |
| **Outils de déploiement Windows installés** | Vérifie si le composant Outils de déploiement Windows de Windows ADK pour Windows 10 est installé. | Erreur | Fournisseur SMS |
| **Cluster de basculement Windows** | Vérifie que les ordinateurs avec un point de gestion ou un point de distribution ne font pas partie d'un cluster Windows. | Erreur | Point de gestion<br>Point de distribution |
| **Environnement de préinstallation Windows installé** | Vérifie si le composant Environnement de préinstallation Windows de Windows ADK pour Windows 10 est installé. | Erreur | Fournisseur SMS |
| **Windows Remote Management (WinRM) v1.1** | Vérifie que WinRM 1.1 est installé sur le serveur de site principal ou sur l'ordinateur de la console Configuration Manager pour exécuter la console de gestion hors bande. Pour plus d'informations sur le téléchargement de WinRM 1.1, consultez l'article 936059 de la Base de connaissances Microsoft. | Avertissement | Site principal,<br>Console Configuration Manager |

| VÉRIFICATION EFFECTUÉE | EXPLICATION | NIVEAU DE GRAVITÉ | SITE D'APPLICATION |
|---|---|---|---|
| **WSUS sur le serveur de site** | Vérifie que Windows Server Update Services (WSUS) 3.0 Service Pack 2 (SP2) est installé sur le serveur de site. Lorsque vous utilisez un point de mise à jour logicielle sur un ordinateur qui n'est pas le serveur de site, vous devez installer la console d'administration WSUS sur le serveur de site. Pour plus d'informations sur WSUS, consultez Windows Server Update Services . | Avertissement | Site d'administration centrale,<br>Site principal |

## Vérifications des prérequis en rapport avec la configuration système requise

Le tableau suivant présente la liste des vérifications qu'effectue l'Outil de vérification des prérequis en rapport avec la configuration système requise.

| VÉRIFICATION EFFECTUÉE | EXPLICATION | NIVEAU DE GRAVITÉ | SITE D'APPLICATION |
|---|---|---|---|
| **Vérification du niveau fonctionnel du domaine Active Directory** | Vérifie que le niveau fonctionnel du domaine Active Directory est au moins Windows Server 2008 R2. | Avertissement | Site d'administration centrale,<br>Site principal |
| **Vérifier que le service de serveur est en cours d'exécution** | Vérifie que le service de serveur est démarré. | Erreur | Site d'administration centrale,<br>Site principal,<br>Site secondaire |
| **Appartenance au domaine** | Vérifie que l'ordinateur Configuration Manager est membre d'un domaine Windows. | Erreur | Site d'administration centrale,<br>Site principal,<br>Site secondaire,<br>Fournisseur SMS,<br>SQL Server |
| **Appartenance au domaine** | Vérifie que l'ordinateur Configuration Manager est membre d'un domaine Windows. | Avertissement | Point de gestion,<br>Point de distribution |
| **Lecteur FAT sur le serveur de site** | Vérifie si le lecteur de disque est formaté avec le système de fichiers FAT. Pour une meilleure sécurité, installez les composants de serveur de site sur des disques formatés avec le système de fichiers NTFS. | Avertissement | Site principal |

| VÉRIFICATION EFFECTUÉE | EXPLICATION | NIVEAU DE GRAVITÉ | SITE D'APPLICATION |
|---|---|---|---|
| **Espace disque disponible sur le serveur de site** | Pour installer le serveur de site sur un ordinateur, ce dernier doit disposer d'au moins 15 Go d'espace disque disponible. Vous devez disposer de 1 Go d'espace disponible supplémentaire si vous installez le rôle de système de site de fournisseur SMS sur le même ordinateur. | Erreur | Site d'administration centrale,<br>Site principal,<br>Site secondaire |
| **Redémarrage du système en attente** | Vérifie si un autre programme requiert le redémarrage du serveur avant d'exécuter le programme d'installation. | Erreur | Site d'administration centrale,<br>Site principal,<br>Site secondaire,<br>Console Configuration Manager,<br>Fournisseur SMS,<br>SQL Server,<br>Point de gestion,<br>Point de distribution |
| **Contrôleur de domaine en lecture seule** | Les serveurs de base de données de site et les serveurs de site secondaire ne sont pas pris en charge sur un contrôleur de domaine en lecture seule (RODC). Pour plus d'informations, consultez Problèmes lors de l'installation de SQL Server sur un contrôleur de domaine dans la Base de connaissances Microsoft. | Erreur | Site d'administration centrale,<br>Site principal,<br>Site secondaire |
| **Extensions de schéma** | Détermine si le schéma des services de domaine Active Directory a été étendu et, le cas échéant, la version des extensions de schéma utilisées. Les extensions de schéma Active Directory de Configuration Manager ne sont pas requises pour installer le serveur de site, mais nous les recommandons pour utiliser pleinement toutes les fonctionnalités de Configuration Manager. Pour plus d'informations sur les avantages d'étendre le schéma, consultez Préparer Active Directory pour la publication de site. | Avertissement | Site d'administration centrale,<br>Site principal |

| VÉRIFICATION EFFECTUÉE | EXPLICATION | NIVEAU DE GRAVITÉ | SITE D'APPLICATION |
|---|---|---|---|
| **Longueur du nom de domaine complet du serveur de site** | Vérifie la longueur du nom de domaine complet de l'ordinateur du serveur de site. | Erreur | Site d'administration centrale,<br>Site principal,<br>Site secondaire |
| **Système d'exploitation de la console Configuration Manager non pris en charge** | Vérifie que la console Configuration Manager peut être installée sur les ordinateurs qui exécutent une version de système d'exploitation prise en charge. Pour plus d'informations, consultez Systèmes d'exploitation pris en charge pour la console System Center Configuration Manager. | Erreur | Console Configuration Manager |
| **Version du système d'exploitation du serveur de site non prise en charge pour l'installation** | Vérifie qu'un système d'exploitation pris en charge s'exécute sur le serveur. Pour plus d'informations, consultez Systèmes d'exploitation pris en charge pour les serveurs de système de site System Center Configuration Manager. | Erreur | Site d'administration centrale,<br>Site principal,<br>Site secondaire,<br>Console Configuration Manager,<br>Point de gestion,<br>Point de distribution |
| **Vérifier la cohérence de la base de données** | Depuis la version 1602, ce contrôle vérifie la cohérence de la base de données. | Erreur | Site d'administration centrale,<br>Site principal |

# Ressources d'installation de sites System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les rubriques suivantes peuvent vous aider à installer System Center Configuration Manager ou à ajouter des sites à votre hiérarchie Configuration Manager existante.

- Préparer l'installation des sites

  Cette rubrique contient des informations essentielles destinées à vous aider à installer un site dans une hiérarchie nouvelle ou existante. Elle indique notamment les cas où vous devez utiliser d'autres fichiers sources que ceux par défaut, les limitations qui s'appliquent à tous les sites, et les actions facultatives que vous pouvez effectuer pour simplifier l'installation de plusieurs sites.

- Conditions préalables à l'installation d'un site

  Découvrez quels sont les droits d'utilisateur et les autorisations que votre compte doit avoir pour installer un site, et quelles sont les conditions préalables à vérifier pour chaque type de site que vous pouvez installer.

- Installer des sites à l'aide de l'Assistant Installation

  Cette rubrique vous guide tout au long de l'Assistant Installation de site. Il fournit des détails sur des options qui peuvent ne pas être suffisamment claires dans l'interface utilisateur de l'Assistant.

- Installer des sites à l'aide d'une ligne de commande et d'un script

  Découvrez comment obtenir un script d'installation de site et comment l'utiliser pour installer un site sans assistance.

- Installer la console Configuration Manager

  Cette rubrique offre des conseils sur la façon d'installer la console Configuration Manager sur un ordinateur sur lequel vous n'installez pas de site.

- Mettre à niveau une installation d'évaluation vers une installation complète

  Lisez cette rubrique quand vous êtes prêt à mettre à niveau votre site d'évaluation vers un site Configuration Manager sous licence complète.

# Préparer l'installation de sites System Center Configuration Manager

22/06/2018 • 16 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Pour préparer dans les meilleures conditions le déploiement d'un ou plusieurs sites System Center Configuration Manager, prenez connaissance des informations contenues dans cet article. Ces étapes peuvent vous faire gagner du temps durant l'installation de plusieurs sites et vous éviter des faux pas qui pourraient vous contraindre à réinstaller un ou plusieurs sites.

> **TIP**
> Lors de la gestion de l'infrastructure de site et de hiérarchie de System Center Configuration Manager, les termes *mise à niveau*, *mise à jour* et *installation* sont utilisés pour décrire trois concepts distincts. Pour connaître la signification et l'usage de chaque terme, consultez À propos de la mise à niveau, de la mise à jour et de l'installation de l'infrastructure de site et de hiérarchie.

## Options d'installation de différents types de sites

Quand vous installez une nouvelle version de Configuration Manager, la version des fichiers sources que vous pouvez utiliser dépend de la version des sites qui se trouvent déjà dans la hiérarchie (le cas échéant). Les méthodes d'installation disponibles dépendent du type de site que vous souhaitez installer.

Avant d'installer un site, veillez à élaborer le plan de votre hiérarchie et à déterminer le type de site que vous voulez installer. Pour plus d'informations, consultez Concevoir une hiérarchie de sites.

### Premier site

Le premier site que vous installez dans une hiérarchie doit être un site principal autonome ou un site d'administration centrale.

**Support d'installation** : pour installer un site d'administration centrale ou un site principal autonome comme premier site d'une nouvelle hiérarchie, vous devez utiliser une version de base de référence de Configuration Manager. N'installez pas le premier site d'une nouvelle hiérarchie à l'aide de fichiers sources mis à jour extraits du dossier CD.Latest d'un site.

**Méthode d'installation** : vous pouvez installer l'un ou l'autre type de site en vous aidant de l'Assistant Installation de Configuration Manager. Vous pouvez aussi configurer un script à utiliser avec une installation scriptée en ligne de commande.

### Sites supplémentaires

Après avoir installé le site initial, vous pouvez à tout moment ajouter d'autres sites. Vous disposez des options suivantes pour ajouter des sites (jusqu'aux limites autorisées) :

| SITE EXISTANT | TYPE DE SITE SUPPLÉMENTAIRE QUE VOUS POUVEZ INSTALLER |
|---|---|
| Site d'administration centrale | Site principal enfant |
| Site principal enfant | Site secondaire |

| SITE EXISTANT | TYPE DE SITE SUPPLÉMENTAIRE QUE VOUS POUVEZ INSTALLER |
| --- | --- |
| Site principal autonome | Site secondaire (vous pouvez étendre le site principal, ce qui convertit le site principal autonome en site principal enfant) |

**Support d'installation** : quand vous installez un site d'administration centrale pour étendre un site principal autonome, ou que vous installez un nouveau site principal enfant dans une hiérarchie existante, vous devez utiliser le support d'installation (qui contient les fichiers sources) qui correspond à la version du ou des sites existants.

> **IMPORTANT**
> Si vous avez installé des mises à jour dans la console qui ont changé la version des sites installés précédemment, n'utilisez pas le support d'installation d'origine. Utilisez plutôt les fichiers sources du dossier CD.Latest d'un site mis à jour. Configuration Manager vous impose d'utiliser des fichiers sources qui correspondent à la version du site existant auquel votre nouveau site doit se connecter.

Un site secondaire doit être installé à partir de la console Configuration Manager. De cette façon, les sites secondaires sont toujours installés à l'aide des fichiers sources à partir du site principal parent.

**Méthode d'installation** : la méthode que vous utilisez pour installer des sites supplémentaires dépend du type de site que vous voulez installer.

- **Ajouter un site d'administration centrale** : vous pouvez utiliser l'Assistant Installation de Configuration Manager ou une ligne de commande scriptée pour installer le nouveau site d'administration centrale comme site parent de votre site principal autonome existant. Pour plus d'informations, consultez Extension d'un site principal autonome.
- **Ajouter un site principal enfant** : vous pouvez utiliser l'Assistant Installation de Configuration Manager ou une installation en ligne de commande pour ajouter un site principal enfant sous un site d'administration centrale.
- **Ajouter un site secondaire** : utilisez la console Configuration Manager pour installer un site secondaire comme site enfant sous un site principal. Les autres méthodes ne sont pas prises en charge pour l'ajout de sites secondaires.

## Tâches courantes à effectuer avant de commencer une installation

- **Déterminer la topologie de la hiérarchie que vous allez utiliser pour votre déploiement**
  Pour plus d'informations, consultez Concevoir une hiérarchie de sites pour System Center Configuration Manager.
- **Préparer et configurer des serveurs individuels pour respecter les prérequis et les configurations prises en charge en vue d'une utilisation avec Configuration Manager**
  Pour plus d'informations, consultez Prérequis des sites et systèmes de site.
- **Installer et configurer SQL Server pour héberger la base de données du site**
  Pour plus d'informations, consultez Prise en charge des versions de SQL Server pour System Center Configuration Manager.
- **Préparer votre environnement réseau pour prendre en charge Configuration Manager**
  Pour plus d'informations, consultez Configurer les pare-feu, les ports et les domaines pour préparer votre infrastructure pour Configuration Manager.
- **Si vous prévoyez d'utiliser une infrastructure à clé publique (PKI), préparer votre infrastructure et vos certificats**
  Pour plus d'informations, consultez Configuration requise des certificats PKI pour Configuration Manager.

- **Installer les dernières mises à jour de sécurité sur les ordinateurs que vous devez utiliser comme serveurs de site ou serveurs de système de site et les redémarrer si nécessaire**

## À propos des noms de site et des codes de site

Les codes de site et les noms de site permettent d'identifier et de gérer les sites dans une hiérarchie Configuration Manager. Dans la console Configuration Manager, le code de site et le nom de site s'affichent au format *<code_site> - <nom_site>*. Chaque code de site que vous utilisez dans votre hiérarchie doit être unique. Si le schéma Active Directory est étendu pour Configuration Manager et que vos sites publient des données, les codes de site utilisés dans une forêt Active Directory doivent être uniques, même s'ils sont utilisés dans une autre hiérarchie Configuration Manager ou s'ils ont été utilisés dans des installations précédentes de Configuration Manager. Veillez à planifier correctement vos codes et noms de site avant de déployer votre hiérarchie.

**Spécifier un code de site et un nom de site**

Quand vous exécutez le programme d'installation de Configuration Manager, vous êtes invité à fournir un code de site et un nom de site pour le site d'administration centrale, et pour l'installation de chaque site principal et secondaire. Un code de site doit identifier chaque site de façon unique dans la hiérarchie. Le code de site étant utilisé dans les noms de dossiers, n'utilisez jamais les noms suivants comme code de site, notamment les noms réservés à Configuration Manager et à Windows :

- AUX
- CON
- NUL
- PRN
- SMS

> **NOTE**
> Le programme d'installation de Configuration Manager ne vérifie pas si un code de site est déjà utilisé.

Pour entrer le code de site pour un site quand vous exécutez le programme d'installation de Configuration Manager, vous devez entrer trois caractères alphanumériques. Seules les lettres de *A* à *Z* et les nombres de *0* à *9*, dans n'importe quelle combinaison, sont autorisés dans les codes de site. La séquence de lettres ou de chiffres n'influe en rien sur la communication entre les sites. Par exemple, il n'est pas nécessaire de nommer un site principal *ABC* et un site secondaire *DEF*.

Le nom du site est un identificateur de nom convivial pour ce site. Vous pouvez utiliser uniquement les caractères de *A* à *Z*, de *a* à *z* et de *0* à *9*, ainsi que le tiret (-) dans les noms des sites.

> **IMPORTANT**
> La modification du code de site ou du nom de site après l'installation du site n'est pas prise en charge.

**Réutiliser un code de site**

Les codes de site ne peuvent pas être utilisés plusieurs fois dans une hiérarchie Configuration Manager pour un site d'administration centrale ou un site principal, même si le site et le code de site d'origine ont été désinstallés. Si vous réutilisez un code de site, vous risquez d'avoir des conflits d'ID d'objet dans votre hiérarchie. Vous pouvez réutiliser le code de site d'un site secondaire si ce site secondaire et le code de site ne sont plus utilisés dans votre hiérarchie Configuration Manager ou dans la forêt Active Directory.

## Limites et restrictions concernant les sites installés

Avant d'installer un site, vous devez connaître les limitations suivantes qui s'appliquent aux sites et aux hiérarchies :

- Après l'exécution du programme d'installation, vous ne pouvez modifier les propriétés suivantes du site qu'en désinstallant le site et en le réinstallant avec les nouvelles valeurs :
  - Répertoire d'installation des fichiers programmes
  - Code de site
  - Description du site
- Si votre hiérarchie comprend un site d'administration centrale :
  - Configuration Manager ne permet pas de retirer un site principal enfant d'une hiérarchie pour en faire un site principal autonome ou pour le rattacher à une autre hiérarchie. Au lieu de cela, vous devez désinstaller le site principal enfant et le réinstaller comme nouveau site principal autonome ou comme site enfant du site d'administration centrale d'une autre hiérarchie.

# Étapes facultatives avant d'exécuter le programme d'installation

**Exécuter manuellement le Téléchargeur d'installation**

Pour télécharger les fichiers d'installation mis à jour pour Configuration Manager, vous pouvez exécuter le Téléchargeur d'installation. Si l'ordinateur sur lequel vous voulez exécuter le programme d'installation n'est pas connecté à Internet, ou si vous prévoyez d'installer plusieurs serveurs de site, utilisez le Téléchargeur d'installation pour télécharger les mises à jour requises du programme d'installation. Voici des informations supplémentaires :

- Par défaut, le programme d'installation se connecte à Internet pour télécharger les fichiers du programme d'installation mis à jour.
- Par défaut, les fichiers sont stockés dans le dossier Redist.
- Vous pouvez diriger le programme d'installation vers un emplacement sur votre réseau où vous avez précédemment stocké une copie de ces fichiers.

**Exécuter manuellement l'Outil de vérification des conditions préalables**

Pour identifier et résoudre les problèmes avant d'exécuter le programme d'installation pour installer un site et avant d'installer un rôle de système de site sur un serveur, vous pouvez exécuter l'Outil de vérification des prérequis. Cet outil permet de vérifier que l'ordinateur remplit les conditions requises pour héberger le site ou le rôle de système de site. Voici des informations supplémentaires :

- Par défaut, le programme d'installation exécute l'Outil de vérification des prérequis.
- En cas d'erreur, le programme d'installation s'arrête jusqu'à ce que le problème soit résolu.

**Identifier des ports facultatifs**

Vous pouvez identifier des ports facultatifs pouvant être utilisés par les clients et les systèmes de site. Voici des informations supplémentaires :

- Par défaut, les systèmes de site et les clients utilisent des ports prédéfinis pour communiquer.
- Pendant l'installation, vous pouvez configurer d'autres ports.

  Pour plus d'informations, consultez Ports utilisés dans System Center Configuration Manager.

# Prérequis à l'installation de sites System Center Configuration Manager

22/06/2018 • 13 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Avant de commencer une installation de site, il est préférable d'en savoir plus sur les prérequis pour l'installation de différents types de sites System Center Configuration Manager.

## Sites principaux et site d'administration centrale

Les prérequis suivants s'appliquent à l'installation d'un site d'administration centrale en tant que premier site d'une hiérarchie, à l'installation d'un site principal autonome ou à l'installation d'un site principal enfant. Si vous installez un site d'administration centrale dans le cadre d'une extension de hiérarchie, consultez Extension d'un site principal autonome dans cette rubrique.

**Prérequis pour l'installation d'un site principal ou d'un site d'administration centrale**

- Le compte d'utilisateur qui installe le site doit disposer des droits suivants :
  - **Administrateur** sur l'ordinateur serveur de site
  - **Administrateur** sur chaque ordinateur devant héberger la **base de données du site** ou une instance du **Fournisseur SMS** pour le site
  - **Sysadmin** sur l'instance de SQL Server qui héberge la base de données du site

    > **IMPORTANT**
    > Une fois l'installation terminée, le compte d'utilisateur qui exécute le programme d'installation et le compte d'ordinateur du serveur de site doivent tous deux conserver des droits d'administrateur système sur SQL Server. Ne supprimez pas les droits d'administrateur système de ces comptes.

- Si vous installez un site principal, vous devez disposer des droits supplémentaires suivants :
  - **Administrateur** sur les autres ordinateurs où vous allez installer le point de gestion initial et le point de distribution (s'il n'est pas sur le serveur de site)
- Si vous installez un nouveau site principal enfant sous un site d'administration centrale, vous devez disposer des droits supplémentaires suivants :
  - **Administrateur** sur l'ordinateur hébergeant le site d'administration centrale
  - Droits d'administration basée sur des rôles dans Configuration Manager, qui équivalent au rôle de sécurité **Administrateur d'infrastructure** ou **Administrateur complet**
- Vous devez utiliser le support d'installation correct (fichiers sources) et exécuter le programme d'installation à partir de cet emplacement. Pour plus d'informations sur les fichiers sources adéquats à utiliser pour installer différents types de sites, consultez Options d'installation des différents types de sites dans la rubrique Préparer l'installation des sites.
- L'ordinateur serveur de site doit avoir accès aux fichiers d'installation mis à jour de Microsoft de l'une des manières suivantes :
  - Avant de commencer l'installation, vous pouvez télécharger et stocker une copie de ces fichiers sur votre

réseau local à l'aide du Téléchargeur d'installation.
    - Si une copie locale de ces fichiers n'est pas disponible, le serveur de site doit avoir accès à Internet pour pouvoir télécharger ces fichiers à partir de Microsoft lors de l'installation.
- Pour pouvoir étendre un site principal autonome ayant un rôle de système de site Point de connexion de service installé, vous devez désinstaller le point de connexion de service. Une seule instance de ce rôle est autorisée dans une hiérarchie, et uniquement sur le site de niveau supérieur de la hiérarchie. Vous avez la possibilité de réinstaller le rôle lors de l'installation du site d'administration centrale.
- Le serveur de site et les ordinateurs de base de données du site doivent présenter toutes les configurations prévues dans les conditions préalables. Avant de démarrer le programme d'installation, vous pouvez exécuter manuellement l'Outil de vérification des prérequis pour identifier et résoudre les problèmes.

**Configuration requise pour développer un site principal autonome**

Un site principal autonome doit remplir les conditions préalables suivantes pour pouvoir être étendu dans une hiérarchie constituée d'un site d'administration centrale :

- **Vous devez installer le nouveau site d'administration centrale à l'aide du support d'un dossier CD.Latest (qui contient les fichiers sources) qui correspond à la version du site principal autonome**

  Pour garantir la correspondance de la version, utilisez les fichiers sources figurant dans le dossier CD.Latest sur le site principal autonome.

  Pour plus d'informations sur les fichiers sources adéquats à utiliser pour installer différents sites, consultez Options d'installation des différents types de sites dans la rubrique Préparer l'installation des sites.

- **Le site principal autonome ne peut pas être configuré pour faire migrer les données d'une autre hiérarchie Configuration Manager**

  Vous devez arrêter la migration active vers le site principal autonome à partir d'autres hiérarchies Configuration Manager, puis supprimer toutes les configurations pour la migration. Sont incluses les tâches de migration qui ne sont pas terminées, la collecte des données et la configuration de la hiérarchie source active.

  En effet, les opérations de migration sont effectuées par le site de niveau supérieur de la hiérarchie et les configurations à faire migrer ne sont pas transférées au site d'administration centrale quand vous étendez un site principal autonome.

  Après avoir étendu le site principal autonome, si vous reconfigurez la migration sur le site principal, le site d'administration centrale assure les opérations liées à la migration. Pour plus d'informations sur la configuration de la migration, consultez Configurer des hiérarchies sources et des sites sources pour la migration vers System Center Configuration Manager.

- **Le compte de l'ordinateur appelé à héberger le nouveau site d'administration centrale doit être membre du groupe d'utilisateurs Administrateurs sur le site principal autonome**

  Pour étendre correctement le site principal autonome, le compte d'ordinateur du nouveau site d'administration centrale doit détenir des droits d'**Administrateur** sur le site principal autonome. Ceci est nécessaire uniquement durant l'extension de site. Vous pouvez supprimer le compte du groupe d'utilisateurs sur le site principal après l'extension du site.

- **Le compte d'utilisateur qui exécute le programme d'installation pour installer le nouveau site d'administration centrale doit avoir des droits d'administration basée sur les rôles au niveau du site principal autonome**

  Pour installer un site d'administration centrale dans le cadre d'une extension de site, le compte d'utilisateur qui exécute le programme d'installation pour installer le site d'administration centrale doit être défini dans

l'administration basée sur les rôles sur le site principal autonome en tant qu'**Administrateur complet** ou **Administrateur d'infrastructure**.

- **Pour pouvoir étendre le site, vous devez désinstaller les rôles système de site suivants du site principal autonome :**

  - Point de synchronisation Asset Intelligence
  - Point Endpoint Protection
  - point de connexion de service

  Ces rôles de système de site sont pris en charge uniquement sur le site de niveau supérieur de la hiérarchie. Par conséquent, vous devez désinstaller ces rôles système de site avant d'étendre le site principal autonome. Une fois le site étendu, vous pouvez réinstaller ces rôles de système de site sur le site d'administration centrale.

  Tous les autres rôles de système de site peuvent rester installés sur le site principal.

- **Le port pour SQL Server Service Broker (SSB) doit être ouvert entre le site principal autonome et l'ordinateur qui va installer le site d'administration centrale**

  Pour répliquer correctement des données entre un site d'administration centrale et un site principal, Configuration Manager exige un port ouvert entre les deux sites, qui sera utilisé par SSB. Quand vous installez un site d'administration centrale et que vous étendez un site principal autonome, la vérification des prérequis ne contrôle pas si le port que vous spécifiez pour SSB est ouvert sur le site principal.

**Problèmes connus quand vous configurez les services Azure :**
Lorsque vous utilisez l'un des services Azure suivants avec Configuration Manager et que vous prévoyez de développer un site, vous devez supprimer et recréer la connexion à ce service après avoir développé le site.

Services :

- Operations Manager Suite (OMS)
- Upgrade Readiness
- Microsoft Store pour Entreprises

Pour résoudre ce problème, procédez comme suit :

1. Dans la console Configuration Manager, supprimez le service Azure du nœud des services Azure.
2. Dans le portail Azure, supprimez du nœud Locataires Azure Active Directory le locataire qui est associé au service. Cette opération supprime l'application web Azure AD qui est associée au service.
3. Reconfigurez la connexion au service Azure pour l'utiliser avec Configuration Manager.

## Sites secondaires

Voici les prérequis à l'installation des sites secondaires :

- L'administrateur qui configure l'installation du site secondaire dans la console Configuration Manager doit avoir des droits d'administration basée sur des rôles qui équivalent au rôle de sécurité **Administrateur d'infrastructure** ou **Administrateur complet**.
- Le compte d'ordinateur du site principal parent doit être **Administrateur** sur l'ordinateur serveur du site secondaire.
- Lorsque le site secondaire utilise une instance précédemment installée de SQL Server pour héberger la base de données du site secondaire :

  - Le **compte d'ordinateur** du site principal parent doit disposer des droits d'administrateur système ( **sysadmin** ) sur l'instance de SQL Server exécutée sur l'ordinateur serveur de site secondaire.

  - Le compte **Système local** de l'ordinateur serveur de site secondaire doit disposer des droits

d'administrateur système ( **sysadmin** ) sur l'instance de SQL Server exécutée sur cet ordinateur.

> **IMPORTANT**
> Une fois l'installation terminée, les deux comptes doivent conserver les droits d'administrateur système (sysadmin) sur SQL Server. Ne supprimez pas les droits d'administrateur système de ces comptes.

- L'ordinateur serveur de site secondaire doit présenter toutes les configurations requises, ce qui inclut SQL Server et les rôles de système de site par défaut du point de gestion et du point de distribution.

# Utilisez l'Assistant Installation pour installer des sites System Center Configuration Manager.

22/06/2018 • 44 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Pour installer un nouveau site System Center Configuration Manager en utilisant une interface utilisateur guidée, vous utilisez l'Assistant Installation de Configuration Manager (setup.exe). Cet Assistant prend en charge l'installation d'un site principal ou d'un site d'administration centrale. Vous utilisez également cet Assistant pour mettre à niveau une installation d'évaluation de Configuration Manager vers une installation sous licence. Si vous ne voulez pas utiliser l'Assistant, vous pouvez utiliser à la place un script d'installation et exécuter une installation en ligne de commande sans assistance.

Pour installer un site secondaire, vous devez installer le site à partir de la console Configuration Manager. Les sites secondaires ne prennent pas en charge une installation en ligne de commande scriptée.

## Installer un site d'administration centrale ou un site principal

Utilisez la procédure suivante pour installer un site d'administration centrale ou un site principal, ou encore pour mettre à niveau un site d'évaluation vers un site Configuration Manager sous licence.

Avant de commencer l'installation du site, vous devez être familiarisé avec le contenu des articles suivants :

- Préparer l'installation des sites
- Prérequis à l'installation des sites

Si vous installez un site d'administration centrale dans le cadre d'un scénario de développement de site, lisez la section Développer un site principal autonome de cette rubrique avant d'utiliser la procédure suivante.

**Pour installer un site principal ou un site d'administration centrale**

1. Sur l'ordinateur sur lequel vous voulez installer le site, exécutez **<InstallationMedia>\SMSSETUP\BIN\X64\Setup.exe** pour démarrer l'**Assistant Installation de System Center Configuration Manager**.

   > **NOTE**
   > Quand vous installez un site d'administration centrale pour développer un site principal autonome, ou que vous installez un nouveau site principal enfant dans une hiérarchie existante, vous devez utiliser le média d'installation (fichiers sources) qui correspondent à la version du ou des sites existants. Si vous avez installé des mises à jour dans la console qui ont changé la version des sites installés précédemment, n'utilisez pas le support d'installation d'origine. Utilisez plutôt les fichiers sources du dossier CD.Latest d'un site mis à jour. Configuration Manager vous impose d'utiliser des fichiers sources qui correspondent à la version du site existant auquel votre nouveau site doit se connecter.

2. Dans la page **Avant de commencer**, choisissez **Suivant**.

3. Dans la page **Prise en main**, sélectionnez le type de site à installer :

   - **Site d'administration centrale** comme premier site d'une nouvelle hiérarchie, ou lors du développement d'un site principal autonome :

     Sélectionnez **Installer un site d'administration centrale Configuration Manager**.

À une étape ultérieure de cette procédure, vous aurez le choix entre installer un site d'administration centrale en tant que premier site d'une nouvelle hiérarchie ou installer un site d'administration centrale par extension d'un site principal autonome.

- **Site principal**, comme site principal autonome constituant le premier site d'une nouvelle hiérarchie, comme site principal enfant :

  Sélectionnez **Installer un site principal Configuration Manager**.

  > **TIP**
  > En règle générale, vous devez sélectionner l'option **Utiliser les options d'installation par défaut pour un site principal autonome** uniquement pour installer un site principal autonome dans un environnement de test. Quand vous sélectionnez cette option, le programme d'installation :
  >
  > - configure automatiquement le site comme site principal autonome ;
  > - utilise un chemin d'installation par défaut ;
  > - utilise une installation locale de l'instance par défaut de SQL Server pour la base de données du site ;
  > - installe un point de gestion et un point de distribution sur l'ordinateur serveur de site ;
  > - configure le site en anglais et dans la langue d'affichage du système d'exploitation sur le serveur de site principal si elle correspond à l'une des langues prises en charge par Configuration Manager.

4. Sur la page **Clé du produit** :

   - Choisissez d'installer Configuration Manager en tant que version d'évaluation ou version sous licence.

     - Si vous sélectionnez une version sous licence, entrez votre clé de produit, puis choisissez **Suivant**.
     - Si vous sélectionnez une édition d'évaluation, choisissez **Suivant**. (Vous pouvez mettre à niveau une installation d'évaluation vers une installation complète ultérieurement.)

   - À compter de la version Release d'octobre 2016 du support de base de référence de la version 1606 de System Center Configuration Manager, vous pouvez spécifier la date d'expiration de votre contrat Software Assurance. Dans cette page, vous avez la possibilité de spécifier la **date d'expiration de la Software Assurance** de votre contrat de licence en guise de rappel pratique pour vous. Si vous n'entrez pas cette date pendant l'installation, vous pouvez la spécifier ultérieurement dans la console Configuration Manager.

     > **NOTE**
     > Microsoft ne valide pas la date d'expiration que vous entrez et ne l'utilise pas pour la validation de la licence. Vous pouvez ainsi l'utiliser en guise de rappel de votre date d'expiration. Ce rappel est pratique, car Configuration Manager vérifie régulièrement les nouvelles mises à jour logicielles proposées en ligne, et l'état de votre licence Software Assurance doit être actualisé pour que vous soyez autorisé à utiliser ces mises à jour supplémentaires.

     Pour plus d'informations, consultez Licences et branches pour System Center Configuration Manager.

5. Dans la page **Termes du contrat de licence logiciel Microsoft** , lisez et acceptez les termes du contrat de licence.

6. Dans la page **Licences requises** , lisez et acceptez les termes du contrat de licence pour les logiciels requis. Le programme d'installation télécharge et installe automatiquement les logiciels sur les systèmes

ou les clients du site, si nécessaire. Vous devez cocher toutes les cases pour pouvoir passer à la page suivante.

7. Dans la page **Téléchargements requis** , spécifiez si le programme d'installation doit télécharger les tout derniers fichiers redistribuables requis à partir d'Internet ou utiliser des fichiers téléchargés précédemment :

   - Si vous souhaitez que le programme d'installation télécharge les fichiers à ce stade, sélectionnez **Télécharger les fichiers requis** , puis spécifiez l'emplacement où stocker les fichiers.
   - Si vous avez précédemment téléchargé les fichiers à l'aide du téléchargeur d'installation, sélectionnez **Utiliser des fichiers précédemment téléchargés**, puis spécifiez le dossier de téléchargement.

     > **TIP**
     > Si vous utilisez des fichiers téléchargés précédemment, vérifiez que le dossier de téléchargement indiqué contient la version la plus récente des fichiers.

8. Dans la page **Sélection de la langue du serveur**, sélectionnez les langues disponibles pour la console Configuration Manager et les rapports. (L'anglais est sélectionné par défaut et ne peut pas être supprimé.)

9. Dans la page **Sélection de la langue client**, sélectionnez les langues disponibles pour les ordinateurs clients, puis spécifiez si vous voulez activer toutes les langues du client pour les clients d'appareils mobiles. (L'anglais est sélectionné par défaut et ne peut pas être supprimé.)

   > **IMPORTANT**
   > Quand vous utilisez un site d'administration centrale, vérifiez que les langues du client que vous configurez sur ce site incluent toutes les langues du client que vous configurez au niveau de chaque site principal enfant. En effet, les clients qui effectuent l'installation à partir d'un point de distribution ont accès aux langues du client à partir du site de niveau supérieur, tandis que les clients qui effectuent l'installation à partir d'un point de gestion ont accès aux langues du client à partir de leur site principal attribué.

10. Dans la page **Paramètres d'installation et du site**, spécifiez les éléments suivants pour le nouveau site que vous installez :

    - **Code de site** : dans une hiérarchie, le code de chaque site doit être unique et constitué de trois caractères alphanumériques (A à Z et 0 à 9). Étant donné que le code de site est utilisé dans les noms de dossier, n'utilisez pas de noms réservés à Windows pour le site, à savoir :
      - AUX
      - CON
      - NUL
      - PRN
      - SMS

      > **NOTE**
      > Le programme d'installation ne vérifie pas si le code de site que vous spécifiez est déjà utilisé ou s'il s'agit d'un nom réservé.

    - **Nom du site** : chaque site doit posséder un nom convivial pour faciliter son identification.
    - **Dossier d'installation** : chemin du dossier de l'installation de Configuration Manager. Vous ne

pouvez pas modifier cet emplacement après l'installation du site. De plus, ce chemin ne doit pas contenir de caractères Unicode, ni d'espaces en fin de chaîne.

11. Dans la page **Installation de site**, utilisez l'option suivante correspondant à votre scénario :

    - **J'installe un site d'administration centrale :**

      Dans la page **Installation du site d'administration centrale**, sélectionnez **Installer en tant que premier site d'une nouvelle hiérarchie**, puis choisissez sur **Suivant** pour continuer.

    - **J'étends un site principal autonome en une hiérarchie comportant un site d'administration centrale :**

      Dans la page **Installation du site d'administration centrale**, sélectionnez **Étendre un site principal autonome existant dans une hiérarchie**, spécifiez le nom de domaine complet (FQDN) du serveur de site principal autonome, puis choisissez **Suivant** pour continuer.

      Le support que vous utilisez pour installer le nouveau site d'administration centrale doit correspondre à la version du site principal.

    - **J'installe un site principal autonome :**

      Dans la page **Installation du site principal**, sélectionnez**Installer le site principal en tant que site autonome**, puis choisissez **Suivant**.

    - **J'installe un site principal enfant :**

      Dans la page **Installation du site principal**, sélectionnez **Joindre le site principal à une hiérarchie existante**, spécifiez le nom de domaine complet (FQDN) pour le site d'administration centrale, puis choisissez **Suivant**.

12. Dans la page **Informations sur la base de données**, spécifiez les informations suivantes :

    - **Nom du SQL Server (FQDN)** : par défaut, il s'agit de l'ordinateur serveur de site.

      Si vous utilisez un port personnalisé, ajoutez ce port au nom FQDN du serveur SQL Server. Pour ce faire, faites suivre le nom FQDN du serveur d'une virgule, puis du numéro de port. Par exemple, pour le serveur *SQLServer1.fabrikam.com*, procédez ainsi pour spécifier le port *1551* : **SQLServer1.fabrikam.com,1551**

    - **Nom de l'instance** : par défaut, cette valeur est vide. L'instance par défaut de SQL est utilisée sur l'ordinateur serveur de site.

    - **Nom de base de données** : par défaut, la valeur définie est CM_<codeSite>. Vous êtes libre de spécifier un autre nom de votre choix.

    - **Port Service Broker** : la valeur prédéfinie indique d'utiliser le port SQL Server Service Broker (SSB) par défaut (4022). SQL l'utilise communiquer directement avec des bases de données d'autres sites.

13. Dans la deuxième page **Informations sur la base de données**, vous pouvez spécifier des emplacements autres que ceux par défaut pour le fichier de données SQL Server et le fichier journal SQL Server pour la base de données du site :

    - Les emplacements de fichier par défaut pour SQL Server sont indiqués.

    - Cette possibilité de spécifier des emplacements de fichiers autres que les emplacements par défaut n'est pas disponible quand vous utilisez un cluster SQL Server.

    - L'Outil de vérification des prérequis ne vérifie pas l'espace disque disponible aux emplacements de fichiers autres que les emplacements par défaut.

14. Dans la page **Paramètres du fournisseur SMS** , spécifiez le nom de domaine complet (FQDN) du serveur sur lequel vous souhaitez installer le fournisseur SMS.

    - Le serveur de site est spécifié par défaut.
    - Une fois le site installé, vous pouvez configurer d'autres fournisseurs SMS.

15. Dans la page **Paramètres de communication du client** , choisissez de configurer tous les systèmes de site pour accepter uniquement les communications HTTPS en provenance de clients ou de configurer la méthode de communication pour chaque rôle de système de site.

    Quand vous sélectionnez **Tous les rôles de système de site acceptent uniquement les communications HTTPS depuis les clients**, l'ordinateur client doit avoir un certificat PKI valide pour l'authentification du client. Pour plus d'informations sur la configuration requise des certificats PKI, consultez Configuration requise des certificats PKI pour Configuration Manager.

    > **NOTE**
    > Effectuez cette étape uniquement si vous installez un site principal. Si vous installez un site d'administration centrale, ignorez cette étape.

16. Sur la page **Rôles système de site** , choisissez d'installer un point de gestion ou un point de distribution. Pour chaque rôle de votre choisissez de faire installer par le programme d'installation :

    - Vous devez entrer le **nom de domaine complet (FQDN)** de l'ordinateur qui hébergera le rôle et choisir la méthode de connexion client que le serveur prendra en charge (HTTP ou HTTPS).
    - Si vous avez sélectionné **Tous les rôles de système de site acceptent uniquement les communications HTTPS depuis les clients** dans la page précédente, les paramètres de connexion client sont configurés automatiquement pour HTTPS et vous ne pouvez pas les modifier sans revenir en arrière et changer le paramètre.

    > **NOTE**
    > Effectuez cette étape uniquement si vous installez un site principal. Si vous installez un site d'administration centrale, ignorez cette étape.

    > **NOTE**
    > Pour installer des rôles de système de site, le programme d'installation utilise le **compte d'installation du système de site**. Par défaut, il utilise le compte d'ordinateur du site principal. Ce compte doit avoir des autorisations d'administrateur local sur un ordinateur distant pour installer le rôle de système de site. Si ce compte ne possède pas les autorisations requises, désélectionnez les rôles de système de site et installez-les ultérieurement à partir de la console Configuration Manager, après avoir configuré des comptes supplémentaires à utiliser en tant que comptes d'installation du système de site.

17. Dans la page **Données d'utilisation**, consultez les informations relatives aux données que Microsoft collecte, puis choisissez **Suivant**.

18. La page **Configuration du point de connexion de service** s'affiche pendant l'installation uniquement dans les cas suivants :

    - quand vous installez un site principal autonome ;
    - quand vous installez un site d'administration centrale.

> **NOTE**
> Si vous installez un site principal enfant, ignorez cette étape (cette page n'est pas disponible).

Si vous installez un site d'administration centrale dans le cadre d'un scénario de développement de site et que ce rôle est déjà installé sur le site principal autonome, vous devez désinstaller ce rôle du site principal autonome. Une seule instance de ce rôle est autorisée dans une hiérarchie, et uniquement sur le site de niveau supérieur de la hiérarchie.

Après avoir sélectionné une configuration pour le **point de connexion de service**, choisissez **Suivant**. (Une fois l'installation terminée, vous pouvez modifier cette configuration à partir de la console Configuration Manager.)

19. Dans la page **Résumé des paramètres**, vérifiez le paramètre que vous avez sélectionné. Quand vous êtes prêt, choisissez **Suivant** pour démarrer l'Outil de vérification des prérequis.
20. La page **Vérification de la configuration requise pour l'installation** répertorie tous les problèmes détectés.

    - Quand l'outil de vérification de la configuration requise détecte un problème, choisissez un élément affiché dans la liste pour obtenir des détails sur la façon de résoudre le problème.
    - Avant de poursuivre l'installation du site, vous devez résoudre chaque élément présentant l'état **Échec**. Les éléments présentant l'état **Avertissement** doivent être résolus, mais ils ne bloquent pas l'installation du site.
    - Après avoir résolu les problèmes, choisissez **Vérifier** pour réexécuter l'Outil de vérification des prérequis.

      Quand l'Outil de vérification des prérequis ne rencontre plus aucun état **Échec**, vous pouvez choisir **Commencer l'installation** pour démarrer l'installation du site.

> **TIP**
> Outre les commentaires formulés dans l'Assistant, vous pouvez trouver des informations supplémentaires sur les problèmes liés aux prérequis dans le fichier **ConfigMgrPrereq.log**, situé à la racine du lecteur système de l'ordinateur sur lequel vous effectuez l'installation. Pour obtenir une liste complète des règles et des descriptions des prérequis à l'installation, voir Liste des vérifications des prérequis pour System Center Configuration Manager.

21. Dans la page **Installation** , le programme d'installation affiche l'état de l'installation. Une fois l'installation du serveur de site principal terminée, vous avez la possibilité de **Fermer** l'Assistant Installation. Quand vous fermez l'Assistant, l'installation et les configurations de site initiales continuent en arrière-plan.

    - Vous pouvez connecter une console Configuration Manager au site avant la fin de l'installation. Dans ce cas, cette console est connectée en lecture seule, ce qui signifie qu'elle permet l'affichage des objets et des paramètres, mais pas leur modification.
    - Vous devez attendre la fin de l'installation pour pouvoir connecter une console permettant de modifier les objets et paramètres.

## Développer un site principal autonome

Après avoir installé un site principal autonome comme premier site, vous pouvez développer ce site ultérieurement dans une plus grande hiérarchie en installant un site d'administration centrale.

Quand vous développez un site principal autonome, vous installez un nouveau site d'administration centrale qui utilise la base de données du site principal autonome existant comme référence. Après l'installation du nouveau site d'administration centrale, le site principal autonome est utilisé comme site principal enfant.

- Seul un site principal autonome peut être étendu dans une nouvelle hiérarchie.
- Un seul site principal autonome peut être étendu dans une hiérarchie spécifique. Vous ne pouvez pas utiliser cette option pour joindre d'autres sites principaux autonomes dans la même hiérarchie. À la place, utilisez une migration pour migrer des données d'une hiérarchie vers une autre.
- Après avoir étendu un site autonome dans une hiérarchie comportant un site d'administration centrale, vous pouvez ajouter des sites principaux enfants.
- Pour supprimer un site principal d'une hiérarchie ayant un site d'administration centrale, vous devez le désinstaller.

Pour étendre le site, utilisez l'Assistant Installation de System Center Configuration Manager pour installer un nouveau site d'administration centrale, en prenant les précautions suivantes :

- Vous devez installer le site d'administration centrale en utilisant la même version de Configuration Manager que celle utilisée pour le site principal autonome.
- Dans la page **Prise en main** de l'Assistant Installation, sélectionnez l'option d'installation d'un site d'administration centrale. À un stade ultérieur, le programme d'installation vous permettra de choisir l'option de développement d'un site principal autonome existant.
- Quand vous configurez la page **Sélection de la langue client** pour le nouveau site d'administration centrale, sélectionnez les mêmes langues client que celles configurées pour le site principal autonome que vous développez.
- Dans la page **Installation de site**, sélectionnez l'option de développement du site principal autonome.

Pour développer un site principal autonome, consultez tout d'abord la configuration requise pour développer un site, puis utilisez la procédure *Pour installer un site principal ou un site d'administration centrale*, décrite précédemment dans cet article.

## Installer un site secondaire

Vous pouvez utiliser la console Configuration Manager pour installer un site secondaire.

- Si la console que vous utilisez n'est pas connectée au site principal qui sera le site parent du nouveau site secondaire, la commande d'installation du site sera répliquée sur le site principal approprié.
- Avant de commencer l'installation du site, vérifiez que votre compte d'utilisateur dispose des autorisations requises et que l'ordinateur qui va héberger le nouveau site secondaire remplit toutes les conditions préalables à une utilisation comme serveur de site secondaire.
- Quand vous installez le site secondaire, Configuration Manager configure le nouveau site pour utiliser les ports de communication client configurés sur le site principal parent.

**Pour installer un site secondaire**

1. Dans la console Configuration Manager, accédez à **Administration** > **Configuration du site** > **Sites**. Sélectionnez le site qui sera le site principal parent du nouveau site secondaire.
2. Choisissez **Créer un site secondaire** pour démarrer l'**Assistant Création de site secondaire**.
3. Dans la page **Avant de commencer**, vérifiez que le site principal répertorié est le site à utiliser comme parent du nouveau site secondaire. Ensuite, choisissez **Suivant**.

4. Dans la page **Général** , indiquez les informations suivantes :

   - **Code de site** : dans une hiérarchie, le code de chaque site doit être unique et constitué de trois caractères alphanumériques (A à Z et 0 à 9). Étant donné que le code de site est utilisé dans les noms de dossier, n'utilisez pas de noms réservés à Windows pour le site, à savoir :

     - AUX
     - CON
     - NUL
     - PRN
     - SMS

     > **NOTE**
     > Le programme d'installation ne vérifie pas si le code de site que vous spécifiez est déjà utilisé ou s'il s'agit d'un nom réservé.

   - **Nom du serveur de site** : nom de domaine complet du serveur sur lequel le nouveau site secondaire sera installé.
   - **Nom du site** : chaque site doit posséder un nom convivial pour faciliter son identification.
   - **Dossier d'installation** : chemin du dossier de l'installation de Configuration Manager. Vous ne pouvez pas modifier cet emplacement après l'installation du site. Ce chemin ne doit pas contenir de caractères Unicode, ni d'espaces en fin de chaîne.

   > **IMPORTANT**
   > Après avoir spécifié les détails dans cette page, vous pouvez choisir **Résumé** pour utiliser les paramètres par défaut pour le reste des options de site secondaire et accéder directement à la page **Résumé** de l'Assistant.
   >
   > - Utilisez cette option uniquement si vous êtes familiarisé avec les paramètres par défaut de cet Assistant et s'il s'agit des paramètres que vous souhaitez utiliser.
   > - Les groupes de limites ne sont pas associés au point de distribution quand vous utilisez les paramètres par défaut. Par conséquent, tant que vous n'avez pas configuré de groupes de limites incluant le serveur de site secondaire, les clients n'utilisent pas le point de distribution installé sur ce site secondaire comme emplacement source du contenu.

5. Dans la page **Fichiers sources d'installation** , choisissez la façon dont l'ordinateur du site secondaire obtient les fichiers sources pour l'installation du site.

   Si vous utilisez des fichiers sources stockés sur le réseau ou sur l'ordinateur du site secondaire :

   - L'emplacement des fichiers sources doit inclure un dossier nommé **Redist** contenant tous les fichiers précédemment téléchargés à l'aide du Téléchargeur d'installation.
   - Si des fichiers du dossier **Redist** ne sont pas disponibles, le programme d'installation ne peut pas installer le site secondaire.
   - Le compte de l'ordinateur du site secondaire doit disposer d'autorisations de **lecture** sur le dossier et le partage des fichiers sources.

6. Dans la page **Paramètres SQL Server** , spécifiez la version de SQL Server à utiliser, puis configurez les paramètres associés.

> **NOTE**
> Le programme d'installation ne valide pas les informations que vous entrez dans cette page avant de démarrer l'installation. Avant de continuer, vérifiez ces paramètres.

**Installer et configurer une copie locale de SQL Express sur l'ordinateur de site secondaire**

- **Port de service de SQL Server**: spécifiez le port de service de SQL Server que SQL Server Express doit utiliser. Le port de service est généralement configuré pour utiliser le port TCP 1433, mais vous pouvez configurer un autre port.
- **Port SQL Server Broker**: spécifiez le port SQL Server Service Broker (SSB) que SQL Server Express doit utiliser. Le Service Broker est généralement configuré pour utiliser le port TCP 4022, mais vous pouvez configurer un port différent. Vous devez spécifier un port valide qu'aucun autre site ou service n'utilise, et qu'aucune restriction de pare-feu ne bloque.

> **IMPORTANT**
> Quand Configuration Manager installe SQL Server Express, il installe SQL Server Express 2012 sans Service Pack :
>
> - Pour permettre la prise en charge du site secondaire, après son installation, vous devez mettre à niveau SQL Server Express 2012 avec une version prise en charge.
> - De plus, si l'installation du nouveau site secondaire échoue avant de se terminer, mais achève l'installation de SQL Server Express 2012, vous devez mettre à jour cette instance de SQL Server Express pour que Configuration Manager puisse réessayer d'installer correctement le site secondaire.

**Utiliser une instance SQL Server existante**

- **Nom de domaine complet de SQL Server** : vérifiez le nom de domaine complet de l'ordinateur exécutant SQL Server. Vous devez utiliser un serveur local exécutant SQL Server pour héberger la base de données de site secondaire, et vous ne pouvez pas modifier ce paramètre.
- **Instance SQL Server**: spécifiez l'instance SQL Server à utiliser en tant que base de données du site secondaire. Laissez cette option vide pour utiliser l'instance par défaut.
- **Nom de base de données de site ConfigMgr**: spécifiez le nom à utiliser pour la base de données du site secondaire.
- **Port SQL Server Broker**: spécifiez le port SQL Server Service Broker (SSB) que SQL Server doit utiliser. Vous devez spécifier un port valide qu'aucun autre site ou service n'utilise, et qu'aucune restriction de pare-feu ne bloque.

> **TIP**
> Pour obtenir la liste des versions de SQL Server prises en charge par System Center Configuration Manager, consultez Versions SQL Server prises en charge.

7. Dans la page **Point de distribution** , configurez les paramètres du point de distribution à installer sur le serveur de site secondaire.

   **Paramètres obligatoires :**

   - **Spécifiez la façon dont les appareils clients communiquent avec le point de distribution** : choisissez HTTP ou HTTPS.
   - **Créez un certificat auto-signé ou importez un certificat client PKI** : choisissez entre

l'utilisation d'un certificat auto-signé (qui permet également d'autoriser les connexions anonymes de clients Configuration Manager à la bibliothèque de contenu) et l'importation d'un certificat à partir de votre infrastructure à clé publique (PKI).

Ce certificat sert à authentifier le point de distribution auprès d'un point de gestion avant que ce point de distribution envoie des messages d'état.

Pour plus d'informations sur la configuration requise des certificats, consultez Configuration requise des certificats PKI pour Configuration Manager.

**Paramètres facultatifs :**

- **Installer et configurer IIS si requis par Configuration Manager** : sélectionnez ce paramètre pour permettre à Configuration Manager d'installer et de configurer Internet Information Services (IIS) sur le serveur si IIS n'est pas déjà installé. Les services Internet doivent être installés sur tous les points de distribution.

  > **NOTE**
  > Bien que ce paramètre soit facultatif, IIS doit être installé sur le serveur pour qu'un point de distribution puisse être correctement installé.

- **Activer et configurer BranchCache pour ce point de distribution**.
- **Description**. Description conviviale du point de distribution pour faciliter son identification.
- **Activer ce point de distribution pour le contenu préparé**.

8. Dans la page **Paramètres du lecteur** , spécifiez les paramètres du lecteur pour le point de distribution du site secondaire.

   Vous pouvez configurer jusqu'à deux lecteurs de disque pour la bibliothèque de contenu et deux lecteurs de disque pour le partage de package. Toutefois, Configuration Manager peut utiliser des lecteurs supplémentaires quand les deux premiers atteignent la réserve d'espace disque configurée. La page **Paramètres du lecteur** permet de configurer la priorité des lecteurs de disque et la quantité d'espace disque libre restant sur chaque lecteur de disque.

   - **Réserve d'espace libre sur le lecteur (Mo)** : la valeur que vous configurez pour ce paramètre détermine la quantité d'espace libre sur un lecteur avant que Configuration Manager choisisse un autre lecteur et poursuive le processus de copie sur ce lecteur. Les fichiers de contenu peuvent s'étendre sur plusieurs lecteurs.
   - **Emplacements du contenu**: Spécifiez les emplacements de contenu pour le partage de bibliothèque et de package de contenu. Configuration Manager copie le contenu à l'emplacement de contenu principal jusqu'à ce que la quantité d'espace libre atteigne la valeur spécifiée dans **Réserve d'espace libre sur le lecteur (Mo)**.

     Par défaut, les emplacements du contenu sont définis sur **Automatique**. L'emplacement de contenu principal est défini sur le lecteur de disque disposant le plus d'espace lors de l'installation. L'emplacement secondaire, quant à lui, est attribué au deuxième lecteur de disque disposant le plus d'espace. Quand le lecteur principal et le lecteur secondaire atteignent la réserve d'espace libre sur le lecteur, Configuration Manager sélectionne un autre lecteur disponible ayant le plus d'espace disque libre et poursuit le processus de copie.

9. Sur la page **Validation du contenu** , indiquez si vous souhaitez valider l'intégrité des fichiers de contenu sur le point de distribution.

   - Quand vous activez la validation de contenu selon un calendrier, Configuration Manager démarre

le processus à l'heure planifiée, et tout le contenu est vérifié sur le point de distribution.

- Vous pouvez également configurer le paramètre **Priorité de la validation du contenu**.
- Pour afficher les résultats du processus de validation du contenu, dans la console Configuration Manager, accédez à **Analyse** > **État de distribution** > **État du contenu**. Le contenu de chaque type de package (par exemple, application, package de mises à jour logicielles et image de démarrage) s'affiche.

10. Dans la page **Groupes de limites**, gérez les groupes de limites auxquels ce point de distribution est affecté :

    - Lors d'un déploiement de contenu, les clients doivent se trouver dans un groupe de limites associé au point de distribution pour l'utiliser comme emplacement source pour le contenu.
    - Vous pouvez sélectionner l'option **Autoriser l'emplacement source de secours pour le contenu** afin de permettre aux clients situés en-dehors de ces groupes de limites de revenir et d'utiliser le point de distribution comme emplacement source pour le contenu lorsque aucun point de distribution préféré n'est disponible.

      Pour plus d'informations sur les points de distribution préférés, consultez la rubrique Concepts fondamentaux de la gestion de contenu.

11. Dans la page **Résumé**, vérifiez les paramètres, puis choisissez **Suivant** pour installer le site secondaire. Quand l'Assistant affiche la page **Dernière étape**, vous pouvez fermer l'Assistant. L'installation du site secondaire se poursuit en arrière-plan.

**Pour vérifier l'état d'installation du site secondaire**

1. Dans la console Configuration Manager, accédez à **Administration** > **Configuration du site** > **Sites**.
2. Sélectionnez le serveur de site secondaire que vous installez, puis choisissez **Afficher l'état d'installation**.

> **TIP**
> Quand vous installez plusieurs sites secondaires à la fois, l'Outil de vérification des prérequis s'exécute sur un seul site à la fois ; il doit terminer de vérifier un site avant de pouvoir passer au site suivant.

# Utiliser la ligne de commande pour installer des sites System Center Configuration Manager

22/06/2018 • 10 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez exécuter le programme d'installation de System Center Configuration Manager à partir d'une invite de commandes pour installer divers types de site.

## Tâches prises en charge pour des installations via la ligne de commande

Cette méthode consistant à exécuter le programme d'installation prend en charge les tâches d'installation de site et de maintenance de site suivantes :

- **Installer un site d'administration centrale ou un site principal à partir de la ligne de commande**
  Consultez la rubrique Options de ligne de commande pour le programme d'installation.
- **Modifier les langues utilisées sur un site d'administration centrale ou un site principal**
  Pour modifier les langues installées sur un site à partir de la ligne de commande (y compris les langues des appareils mobiles), effectuez les opérations suivantes :
  - Exécutez le programme d'installation à partir de **<chemin_installation_Configuraton_Manager>\Bin\X64** sur le serveur de site.
  - Utilisez l'option de ligne de commande **/MANAGELANGS**.
  - Spécifiez un fichier de jeu de caractères qui définit les langues à ajouter ou supprimer.

    Par exemple, utilisez la syntaxe de commande suivante : **setupwpf.exe /MANAGELANGS <fichier de script de langue>**.

    Pour créer le fichier de script de langue, utilisez les informations fournies dans Options de ligne de commande pour gérer les langues.
- **Utiliser un fichier de script d'installation pour une installation sans assistance de site ou une récupération de site**
  Vous pouvez exécuter le programme d'installation à partir d'une invite de commandes en utilisant un script d'installation et en effectuant une installation sans assistance de site. Vous pouvez aussi utiliser cette option pour récupérer un site.

  Pour utiliser un script avec le programme d'installation :
  - Exécutez le programme d'installation avec l'option de ligne de commande **/SCRIPT** et spécifiez un fichier de script.
  - Le fichier de script doit être configuré avec les clés et les valeurs requises.

    Pour effectuer une installation sans assistance d'un site d'administration centrale ou d'un site principal, le fichier de script doit comporter les sections suivantes :
  - Identification
  - Options
  - SQLConfigOptions

    - HierarchyOptions
  - CloudConnectorOptions

  Pour récupérer un site, vous devez inclure également les sections suivantes du fichier de script :

  - Identification
  - Récupération

Pour plus d'informations, consultez Récupération de site sans assistance pour Configuration Manager.

Pour obtenir la liste des clés et des valeurs à utiliser dans un fichier de script d'installation sans assistance, consultez Clés du fichier de script d'installation sans assistance.

## À propos du fichier de script de ligne de commande

Pour réaliser une installation sans assistance de Configuration Manager, vous pouvez exécuter le programme d'installation avec l'option de ligne de commande **/SCRIPT** et spécifier un fichier de script contenant les options d'installation. Avec cette méthode, vous pouvez effectuer les tâches suivantes :

- Installer un site d'administration centrale
- Installer un site principal
- Installer une console Configuration Manager
- Récupérer un site

> **NOTE**
> Vous ne pouvez pas utiliser le fichier de script d'installation sans assistance pour mettre à niveau un site d'évaluation vers une installation sous licence de Configuration Manager.

**Le nom de la clé CDLatest**

Lorsque vous utilisez un média à partir du dossier CD.Latest pour exécuter une installation scriptée des quatre options d'installation suivantes, votre script doit inclure la clé **CDLatest** avec la valeur **1** :

- Installer un nouveau site d'administration centrale
- Installer un nouveau site principal
- Récupérer un site d'administration centrale
- Récupérer un site principal

Cette valeur n'est pas prise en charge pour l'utilisation avec le média d'installation que vous obtenez à partir du site de licence en volume de Microsoft. Consultez les options de ligne de commande pour plus d'informations sur l'utilisation de ce nom de clé dans le fichier de script.

**Créer le script**

Le script d'installation est automatiquement créé lorsque vous exécutez le programme d'installation pour installer un site à l'aide de l'interface utilisateur. Quand vous confirmez les paramètres dans la page **Résumé** de l'Assistant :

- Le programme d'installation crée le script **%TEMP%\ConfigMgrAutoSave.ini**. Vous pouvez renommer ce fichier avant de l'utiliser, en veillant à conserver l'extension de fichier .ini.
- Le script d'installation sans assistance contient les paramètres que vous avez sélectionnés dans l'Assistant.
- Une fois que le script est créé, vous pouvez le modifier pour installer d'autres sites dans votre hiérarchie.
- Vous pouvez ensuite utiliser ce script pour effectuer une installation sans assistance de Configuration Manager.

Le fichier de script fournit les mêmes informations que l'Assistant Installation demande, à l'exception des paramètres par défaut.
Vous devez spécifier toutes les valeurs pour les clés d'installation qui s'appliquent au type d'installation utilisé.

Lorsque le programme d'installation crée le script d'installation sans assistance, la valeur de clé de produit que vous entrez pendant l'installation est renseignée dans le script. Cette valeur peut être une clé de produit valide, ou **EVAL** lorsque vous installez une version d'évaluation de Configuration Manager. La valeur de clé de produit est renseignée dans le script pour permettre à la vérification des prérequis d'aboutir.

Lorsque le programme d'installation démarre l'installation effective du site, le script créé automatiquement fait l'objet d'une nouvelle écriture pour effacer la valeur de clé de produit dans le script créé. Avant d'utiliser le script pour une installation sans assistance d'un nouveau site, vous pouvez modifier le script pour fournir une clé de produit valide ou spécifier une installation d'évaluation de Configuration Manager.

**Noms des sections, noms des clés et valeurs**

Le script contient les noms de section, les noms de clé et les valeurs. Gardez à l'esprit les informations suivantes :

- Les noms des clés de section requis varient en fonction du type d'installation faisant l'objet du script.
- L'ordre des clés dans les sections et l'ordre des sections dans le fichier n'ont pas d'importance.
- Les clés ne tiennent pas compte de la casse.
- Lorsque vous attribuez des valeurs aux clés, le nom de la clé doit être suivi du signe égal (=) et de la valeur de la clé.

> **TIP**
> Pour connaître l'ensemble complet des options, consultez Options de ligne de commande pour le programme d'installation et les scripts.

## Utiliser l'option de ligne de commande /SCRIPT du programme d'installation

- Vous devez utiliser un fichier de script d'installation et spécifier le nom du fichier après l'option de ligne de commande **/SCRIPT** du programme d'installation. Gardez à l'esprit les informations suivantes :
  - Le nom du fichier doit avoir l'extension de nom de fichier **.ini**.
  - Quand vous faites référence au fichier de script du programme d'installation à l'invite de commandes, indiquez le chemin complet du fichier. Par exemple, si votre fichier d'initialisation du programme d'installation est nommé Setup.ini et se trouve dans le dossier C:\Setup, à l'invite de commandes, tapez : **setup /script c:\setup\setup.ini**.
- Le compte qui exécute le programme d'installation doit avoir des droits d'**administrateur** sur l'ordinateur. Si vous exécutez le programme d'installation avec le script sans assistance, ouvrez la fenêtre d'invite de commandes en utilisant l'option **Exécuter en tant qu'administrateur**.

# Options de ligne de commande pour le programme d'installation de System Center Configuration Manager

22/06/2018 • 64 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez les informations suivantes pour configurer des scripts ou installer System Center Configuration Manager à partir d'une ligne de commande.

## Options de ligne de commande pour le programme d'installation

**/DEINSTALL**
Désinstalle le site. Exécutez le programme d'installation à partir de l'ordinateur sur lequel est installé le serveur de site.

**/DONTSTARTSITECOMP**
Installe un site, mais empêche le démarrage du service Gestionnaire de composant de site. Tant que le service Gestionnaire de composant de site n'a pas démarré, le site n'est pas actif. Le Gestionnaire de composant de site est chargé d'installer et de démarrer le service SMS_Executive, ainsi que d'autres processus au niveau du site. Une fois l'installation du site terminée, quand vous démarrez le service Gestionnaire de composant de site, ce dernier installe le service SMS_Executive et d'autres processus nécessaires au fonctionnement du site.

**/HIDDEN**
Masque l'interface utilisateur pendant l'installation. Utilisez cette option uniquement avec l'option **/SCRIPT**. Le fichier de script sans assistance doit fournir toutes les options nécessaires pour éviter l'échec du programme d'installation.

**/NOUSERINPUT**
Désactive l'entrée utilisateur pendant l'installation, mais affiche l'Assistant Installation. Utilisez cette option uniquement avec l'option **/SCRIPT**. Le fichier de script sans assistance doit fournir toutes les options nécessaires pour éviter l'échec du programme d'installation.

**/RESETSITE**
Effectue une réinitialisation du site qui permet de réinitialiser la base de données et les comptes de service du site. Exécutez le programme d'installation à partir de ***<Chemin d'installation de Configuration Manager>*\BIN\X64** sur le serveur de site. Pour plus d'informations sur la réinitialisation du site, consultez la section Exécuter une réinitialisation de site de la rubrique Modifier votre infrastructure System Center Configuration Manager.

**/TESTDBUPGRADE *<Nom de l'instance>**<Nom de la base de données>***
Effectue un test sur une sauvegarde de la base de données du site pour vérifier qu'elle peut être mise à niveau. Indiquez le nom d'instance et le nom de base de données pour la base de données de site. Si vous spécifiez uniquement le nom de la base de données, le programme d'installation utilise le nom de l'instance par défaut.

> **IMPORTANT**
> N'exécutez pas cette option de ligne de commande sur la base de données de votre site de production. L'exécution de cette option de ligne de commande sur la base de données de votre site de production met à niveau la base de données du site et risque de rendre votre site inutilisable.

**/UPGRADE**
Exécute une mise à niveau sans assistance d'un site. Quand vous utilisez **/UPGRADE**, vous devez spécifier la clé du produit, en incluant les tirets (-). Par ailleurs, vous devez spécifier le chemin des fichiers nécessaires au programme d'installation que vous avez téléchargés précédemment.

Exemple : `setupwpf.exe /UPGRADE xxxxx-xxxxx-xxxxx-xxxxx-xxxxx <path to external component files>`

Pour plus d'informations sur les fichiers nécessaires au programme d'installation, consultez Téléchargeur d'installation.

**/SCRIPT <*Chemin du script d'installation*>**
Effectue des installations sans assistance. Un fichier d'initialisation de l'installation est requis quand vous utilisez l'option **/SCRIPT**. Pour plus d'informations sur l'exécution du programme d'installation sans assistance, consultez Installer des sites à l'aide d'une ligne de commande.

**/SDKINST <*Nom de domaine complet du fournisseur SMS*>**
Installe le fournisseur SMS sur l'ordinateur spécifié. Indiquez le nom de domaine complet de l'ordinateur du fournisseur SMS. Pour plus d'informations sur le fournisseur SMS, consultez Planifier le fournisseur SMS.

**/SDKDEINST <*Nom de domaine complet du fournisseur SMS*>**
Désinstalle le fournisseur SMS sur l'ordinateur spécifié. Indiquez le nom de domaine complet de l'ordinateur du fournisseur SMS.

**/MANAGELANGS <*Chemin du script de langue*>**
Gère les langues installées sur un site installé précédemment. Pour utiliser cette option, exécutez le programme d'installation à partir de **<*Chemin d'installation de Configuration Manager*>\BIN\X64** sur le serveur de site. Indiquez l'emplacement du fichier de script de langue qui contient les paramètres de langue. Pour plus d'informations sur les options de langue disponibles dans le fichier du script d'installation de langue, consultez la section Options de ligne de commande pour gérer les langues.

## Options de ligne de commande pour gérer les langues

**Identification**

- **Nom de clé :** Action
  - **Obligatoire :** oui
  - **Valeurs :** ManageLanguages
  - **Détails :** gère la prise en charge des langues de serveur, de client et de client mobile d'un site.

**Options**

- **Nom de clé :** AddServerLanguages
  - **Obligatoire :** non
  - **Valeurs :** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK ou ZHH
  - **Détails :** spécifie les langues de serveur qui seront disponibles pour la console Configuration

Manager, les rapports et les objets Configuration Manager. L'anglais est disponible par défaut.

- **Nom de clé :** AddClientLanguages
  - **Obligatoire :** non
  - **Valeurs :** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK ou ZHH
  - **Détails :** spécifie les langues qui seront disponibles sur les ordinateurs clients. L'anglais est disponible par défaut.
- **Nom de clé :** DeleteServerLanguages
  - **Obligatoire :** non
  - **Valeurs :** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK ou ZHH
  - **Détails :** Spécifie les langues à supprimer qui ne seront plus disponibles pour la console Configuration Manager, les rapports et les objets Configuration Manager. L'anglais est disponible par défaut et ne peut pas être supprimé.
- **Nom de clé :** DeleteClientLanguages
  - **Obligatoire :** non
  - **Valeurs :** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK ou ZHH
  - **Détails :** Spécifie les langues à supprimer qui ne seront plus disponibles sur les ordinateurs clients. L'anglais est disponible par défaut et ne peut pas être supprimé.
- **Nom de clé :** MobileDeviceLanguage
  - **Obligatoire :** oui
  - **Valeurs :** 0 ou 1

    0 = Ne pas installer

    1 = Installer
  - **Détails :** spécifie si les langues du client d'appareil mobile sont installées.
- **Nom de clé :** PrerequisiteComp
  - **Obligatoire :** oui
  - **Valeurs :** 0 ou 1

    0 = Télécharger

    1 = Déjà téléchargé
  - **Détails :** spécifie si les fichiers d'installation prérequis ont déjà été téléchargés. Par exemple, si vous utilisez la valeur **0**, le programme d'installation télécharge les fichiers.
- **Nom de clé :** PrerequisitePath
  - **Obligatoire :** oui
  - **Valeurs :** *<Chemin des fichiers nécessaires au programme d'installation>*

- **Détails :** spécifie le chemin des fichiers nécessaires au programme d'installation. Selon la valeur **PrerequisiteComp**, le programme d'installation utilise ce chemin pour stocker les fichiers téléchargés ou pour localiser des fichiers précédemment téléchargés.

## Clés du fichier de script d'installation sans assistance

Utilisez les sections suivantes pour vous aider à créer votre script d'installation sans assistance. Les listes affichent les clés de script d'installation disponibles ainsi que leurs valeurs correspondantes, indiquent si elles sont obligatoires ou non, le type d'installation pour lequel elles sont utilisées, ainsi qu'une brève description de la clé.

**Installation sans assistance d'un site d'administration centrale**

Utilisez les détails suivants pour installer un site d'administration centrale à l'aide d'un fichier de script d'installation sans assistance.

**Identification**

- **Nom de clé :** Action
  - **Obligatoire :** oui
  - **Valeurs :** InstallCAS
  - **Détails :** installe un site d'administration centrale.
- **Nom de la clé :** CDLatest
  - **Obligatoire :** Oui, uniquement en cas d'utilisation de médias du dossier CD.Latest.
  - **Valeurs :** 1. Toute autre valeur est considérée comme signifiant que CD.Latest ne doit pas être utilisé.
  - **Détails :** Le script doit inclure cette clé et cette valeur en cas d'exécution de l'installation à partir de médias du dossier CD.Latest dans le cadre de l'installation d'un site principal ou d'administration centrale, ou de la récupération d'un site principal ou d'administration centrale. Cette valeur indique au programme d'installation que des médias de CD.Latest sont utilisés.

**Options**

- **Nom de clé :** ProductID
  - **Obligatoire :** oui
  - **Valeurs :** <*xxxxx-xxxxx-xxxxx-xxxxx-xxxxx*> *ou* Eval
  - **Détails :** Spécifie la clé de produit de l'installation de Configuration Manager avec les tirets. Entrez **Eval** pour installer la version d'évaluation de Configuration Manager.
- **Nom de clé :** SiteCode
  - **Obligatoire :** oui
  - **Valeurs :** <*Code de site*>
  - **Détails :** spécifie les trois caractères alphanumériques qui identifient le site de manière unique dans votre hiérarchie.
- **Nom de clé :** Nom de site
  - **Obligatoire :** oui
  - **Valeurs :** <*Nom de site*>

- **Détails :** spécifie le nom de ce site.

- **Nom de clé :** SMSInstallDir
  - **Obligatoire :** oui
  - **Valeurs :** <*Chemin d'installation de Configuration Manager*>
  - **Détails :** spécifie le dossier d'installation des fichiers programmes de Configuration Manager.
- **Nom de clé :** SDKServer
  - **Obligatoire :** oui
  - **Valeurs :** <*Nom de domaine complet du fournisseur SMS*>
  - **Détails :** spécifie le FQDN du serveur qui héberge le fournisseur SMS. Vous pouvez configurer d'autres fournisseurs SMS pour le site après l'installation initiale.
- **Nom de clé :** PrerequisiteComp
  - **Obligatoire :** oui
  - **Valeurs :** 0 ou 1

    0 = Télécharger

    1 = Déjà téléchargé
  - **Détails :** spécifie si les fichiers d'installation prérequis ont déjà été téléchargés. Par exemple, si vous utilisez la valeur **0**, le programme d'installation télécharge les fichiers.
- **Nom de clé :** PrerequisitePath
  - **Obligatoire :** oui
  - **Valeurs :** <*Chemin des fichiers nécessaires au programme d'installation*>
  - **Détails :** spécifie le chemin des fichiers nécessaires au programme d'installation. Selon la valeur **PrerequisiteComp** , le programme d'installation utilise ce chemin pour stocker les fichiers téléchargés ou localiser des fichiers déjà téléchargés.
- **Nom de clé :** AdminConsole
  - **Obligatoire :** oui
  - **Valeurs :** 0 ou 1

    0 = Ne pas installer

    1 = Installer
  - **Détails :** spécifie si la console Configuration Manager doit ou non être installée.
- **Nom de clé :** JoinCEIP

  > **NOTE**
  > À compter de Configuration Manager version 1802, la fonctionnalité CEIP ne figure plus dans le produit.

  - **Obligatoire :** oui
  - **Valeurs :** 0 ou 1

0 = Ne pas participer

1 = Participer

- **Détails :** Spécifie si vous voulez participer au programme d'amélioration des services.

- **Nom de clé :** AddServerLanguages
  - **Obligatoire :** non
  - **Valeurs :** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK ou ZHH
  - **Détails :** spécifie les langues de serveur qui seront disponibles pour la console Configuration Manager, les rapports et les objets Configuration Manager. L'anglais est disponible par défaut.
- **Nom de clé :** AddClientLanguages
  - **Obligatoire :** non
  - **Valeurs :** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK ou ZHH
  - **Détails :** spécifie les langues qui seront disponibles sur les ordinateurs clients. L'anglais est disponible par défaut.
- **Nom de clé :** DeleteServerLanguages
  - **Obligatoire :** non
  - **Valeurs :** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK ou ZHH
  - **Détails :** modifie un site après son installation. Spécifie les langues à supprimer qui ne seront plus disponibles pour la console Configuration Manager, les rapports et les objets Configuration Manager. L'anglais est disponible par défaut et ne peut pas être supprimé.
- **Nom de clé :** DeleteClientLanguages
  - **Obligatoire :** non
  - **Valeurs :** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK ou ZHH
  - **Détails :** modifie un site après son installation. Spécifie les langues à supprimer qui ne seront plus disponibles sur les ordinateurs clients. L'anglais est disponible par défaut et ne peut pas être supprimé.
- **Nom de clé :** MobileDeviceLanguage
  - **Obligatoire :** oui
  - **Valeurs :** 0 ou 1

    0 = Ne pas installer

    1 = Installer
  - **Détails :** spécifie si les langues du client d'appareil mobile sont installées.

**SQLConfigOptions**

- **Nom de clé :** SQLServerName

- **Obligatoire :** oui
- **Valeurs :** <*Nom du serveur SQL*>
- **Détails :** Spécifie le nom du serveur ou de l'instance en cluster exécutant SQL Server qui hébergera la base de données du site.

- **Nom de clé :** DatabaseName
  - **Obligatoire :** oui
  - **Valeurs :** <*Nom de la base de données du site*> ou <*Nom de l'instance*>\<*Nom de la base de données du site*>
  - **Détails :** spécifie le nom de la base de données SQL Server à créer ou de la base de données SQL Server à utiliser quand le programme d'installation installe la base de données du site d'administration centrale.

    > **IMPORTANT**
    > Si vous n'utilisez pas l'instance par défaut, vous devez spécifier le nom d'instance et le nom de base de données de site.

- **Nom de clé :** SQLSSBPort
  - **Obligatoire :** non
  - **Valeurs :** <*Numéro du port SSB*>
  - **Détails :** spécifie le port SQL Server Service Broker (SSB) que SQL Server utilise. SSB est généralement configuré pour utiliser le port TCP 4022, mais vous pouvez configurer un autre port.
- **Nom de clé :** SQLDataFilePath
  - **Obligatoire :** non
  - **Valeurs :** <*Chemin du fichier .mdb de la base de données*>
  - **Détails :** Spécifie un autre emplacement pour créer le fichier .mdb de la base de données.
- **Nom de clé :** SQLLogFilePath
  - **Obligatoire :** non
  - **Valeurs :** <*Chemin du fichier .ldf de la base de données*>
  - **Détails :** Spécifie un autre emplacement pour créer le fichier .ldf de la base de données.

**CloudConnectorOptions**

- **Nom de clé :** CloudConnector
  - **Obligatoire :** oui
  - **Valeurs :** 0 ou 1

    0 = Ne pas installer

    1 = Installer
  - **Détails :** Spécifie s'il faut installer un point de connexion de service sur ce site. Comme le point de connexion de service peut uniquement être installé sur le site de niveau supérieur d'une hiérarchie,

cette valeur doit être **0** pour un site principal enfant.

- **Nom de clé :** CloudConnectorServer
  - **Obligatoire :** Obligatoire quand **CloudConnector** est égal à 1
  - **Valeurs :** <*Nom de domaine complet du serveur de point de connexion de service*>
  - **Détails :** spécifie le nom de domaine complet du serveur qui hébergera le rôle de système de site de point de connexion de service.
- **Nom de clé :** UseProxy
  - **Obligatoire :** Obligatoire quand **CloudConnector** est égal à 1
  - **Valeurs :** 0 ou 1

    0 = Ne pas installer

    1 = Installer
  - **Détails :** spécifie si le point de connexion de service utilise un serveur proxy.
- **Nom de clé :** ProxyName
  - **Obligatoire :** Obligatoire quand **UseProxy** est égal à 1
  - **Valeurs :** <*Nom de domaine complet du serveur proxy*>
  - **Détails :** spécifie le nom de domaine complet du serveur proxy utilisé par le point de connexion de service.
- **Nom de clé :** ProxyPort
  - **Obligatoire :** Obligatoire quand **UseProxy** est égal à 1
  - **Valeurs :** <*Numéro de port*>
  - **Détails :** Spécifie le numéro de port à utiliser pour le port proxy.

**Installation sans assistance d'un site principal**

Utilisez les détails suivants pour installer un site principal à l'aide d'un fichier de script d'installation sans assistance.

**Identification**

- **Nom de clé :** Action
  - **Obligatoire :** oui
  - **Valeurs :** InstallPrimarySite
  - **Détails :** installe un site principal.
- **Nom de la clé :** CDLatest
  - **Obligatoire :** Oui, uniquement en cas d'utilisation de médias du dossier CD.Latest.
  - **Valeurs :** 1. Toute autre valeur est considérée comme signifiant que CD.Latest ne doit pas être utilisé.
  - **Détails :** Le script doit inclure cette clé et cette valeur en cas d'exécution de l'installation à partir de médias du dossier CD.Latest dans le cadre de l'installation d'un site principal ou d'administration centrale, ou de la récupération d'un site principal ou d'administration centrale. Cette valeur indique

au programme d'installation que des médias de CD.Latest sont utilisés.

**Options**

- **Nom de clé :** ProductID
  - **Obligatoire :** oui
  - **Valeurs :** <*xxxxx-xxxxx-xxxxx-xxxxx-xxxxx*> *ou* Eval
  - **Détails :** Spécifie la clé de produit de l'installation de Configuration Manager avec les tirets. Entrez **Eval** pour installer la version d'évaluation de Configuration Manager.
- **Nom de clé :** SiteCode
  - **Obligatoire :** oui
  - **Valeurs :** <*Code de site*>
  - **Détails :** spécifie les trois caractères alphanumériques qui identifient le site de manière unique dans votre hiérarchie.
- **Nom de clé :** SiteName
  - **Obligatoire :** oui
  - **Valeurs :** <*Nom de site*>
  - **Détails :** spécifie le nom de ce site.
- **Nom de clé :** SMSInstallDir
  - **Obligatoire :** oui
  - **Valeurs :** <*Chemin d'installation de Configuration Manager*>
  - **Détails :** spécifie le dossier d'installation des fichiers programmes de Configuration Manager.
- **Nom de clé :** SDKServer
  - **Obligatoire :** oui
  - **Valeurs :** <*Nom de domaine complet du fournisseur SMS*>
  - **Détails :** spécifie le FQDN du serveur qui héberge le fournisseur SMS. Vous pouvez configurer d'autres fournisseurs SMS pour le site après l'installation initiale.
- **Nom de clé :** PrerequisiteComp
  - **Obligatoire :** oui
  - **Valeurs :** 0 ou 1

    0 = Télécharger

    1 = Déjà téléchargé
  - **Détails :** spécifie si les fichiers d'installation prérequis ont déjà été téléchargés. Par exemple, si vous utilisez la valeur **0**, le programme d'installation télécharge les fichiers.
- **Nom de clé :** PrerequisitePath
  - **Obligatoire :** oui
  - **Valeurs :** <*Chemin des fichiers nécessaires au programme d'installation*>

- **Détails :** spécifie le chemin des fichiers nécessaires au programme d'installation. Selon la valeur **PrerequisiteComp** , le programme d'installation utilise ce chemin pour stocker les fichiers téléchargés ou localiser des fichiers déjà téléchargés.

- **Nom de clé :** AdminConsole
  - **Obligatoire :** oui
  - **Valeurs :** 0 ou 1

    0 = Ne pas installer

    1 = Installer
  - **Détails :** spécifie si la console Configuration Manager doit ou non être installée.
- **Nom de clé :** JoinCEIP

  > **NOTE**
  > À compter de Configuration Manager version 1802, la fonctionnalité CEIP ne figure plus dans le produit.

  - **Obligatoire :** oui
  - **Valeurs :** 0 ou 1

    0 = Ne pas participer

    1 = Participer
  - **Détails :** Spécifie s'il faut participer au programme d'amélioration des services.
- **Nom de clé :** ManagementPoint
  - **Obligatoire :** non
  - **Valeurs :** <*Nom de domaine complet du serveur de site du point de gestion*>
  - **Détails :** spécifie le nom de domaine complet du serveur qui hébergera le rôle de système de site de point de gestion.
- **Nom de clé :** ManagementPointProtocol
  - **Obligatoire :** non
  - **Valeurs :** HTTPS *ou* HTTP
  - **Détails :** spécifie le protocole à utiliser pour le point de gestion.
- **Nom de clé :** DistributionPoint
  - **Obligatoire :** non
  - **Valeurs :** <*Nom de domaine complet du serveur de site du point de distribution*>
  - **Détails :** spécifie le protocole à utiliser pour le point de distribution.
- **Nom de clé :** DistributionPointProtocol
  - **Obligatoire :** non
  - **Valeurs :** HTTPS *ou* HTTP
  - **Détails :** spécifie le protocole à utiliser pour le point de distribution.

- **Nom de clé :** RoleCommunicationProtocol
  - **Obligatoire :** oui
  - **Valeurs :** EnforceHTTPS *ou* HTTPorHTTPS
  - **Détails :** Spécifie s'il faut configurer tous les systèmes de site pour n'accepter que les communications HTTPS des clients ou pour que la méthode de communication soit configurée pour chaque rôle de système de site. Quand vous sélectionnez **EnforceHTTPS**, l'ordinateur client doit disposer d'un certificat d'infrastructure à clé publique (PKI) valide pour l'authentification du client.
- **Nom de clé :** ClientsUsePKICertificate
  - **Obligatoire :** oui
  - **Valeurs :** 0 ou 1

    0 = Ne pas utiliser

    1 = Utiliser
  - **Détails :** spécifie si les clients utiliseront un certificat PKI de client pour communiquer avec les rôles de système de site.
- **Nom de clé :** AddServerLanguages
  - **Obligatoire :** non
  - **Valeurs :** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK ou ZHH
  - **Détails :** spécifie les langues de serveur qui seront disponibles pour la console Configuration Manager, les rapports et les objets Configuration Manager. L'anglais est disponible par défaut.
- **Nom de clé :** AddClientLanguages
  - **Obligatoire :** non
  - **Valeurs :** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK ou ZHH
  - **Détails :** spécifie les langues qui seront disponibles sur les ordinateurs clients. L'anglais est disponible par défaut.
- **Nom de clé :** DeleteServerLanguages
  - **Obligatoire :** non
  - **Valeurs :** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK ou ZHH
  - **Détails :** modifie un site après son installation. Spécifie les langues à supprimer qui ne seront plus disponibles pour la console Configuration Manager, les rapports et les objets Configuration Manager. L'anglais est disponible par défaut et ne peut pas être supprimé.
- **Nom de clé :** DeleteClientLanguages
  - **Obligatoire :** non
  - **Valeurs :** DEU, FRA, RUS, CHS, JPN, CHT, CSY, ESN, HUN, ITA, KOR, NLD, PLK, PTB, PTG, SVE, TRK ou ZHH

- **Détails :** modifie un site après son installation. Spécifie les langues à supprimer qui ne seront plus disponibles sur les ordinateurs clients. L'anglais est disponible par défaut et ne peut pas être supprimé.

- **Nom de clé :** MobileDeviceLanguage
  - **Obligatoire :** oui
  - **Valeurs :** 0 ou 1

    0 = Ne pas installer

    1 = Installer
  - **Détails :** spécifie si les langues du client d'appareil mobile sont installées.

**SQLConfigOptions**

- **Nom de clé :** SQLServerName
  - **Obligatoire :** oui
  - **Valeurs :** <*Nom du serveur SQL*>
  - **Détails :** Spécifie le nom du serveur ou de l'instance en cluster exécutant SQL Server qui hébergera la base de données du site.
- **Nom de clé :** DatabaseName
  - **Obligatoire :** oui
  - **Valeurs :** <*Nom de la base de données du site*> ou <*Nom de l'instance*>\<*Nom de la base de données du site*>
  - **Détails :** Spécifie le nom de la base de données SQL Server à créer ou de la base de données SQL Server à utiliser pour installer la base de données du site principal.

    > **IMPORTANT**
    > Si vous n'utilisez pas l'instance par défaut, vous devez spécifier le nom d'instance et le nom de base de données de site.

- **Nom de clé :** SQLSSBPort
  - **Obligatoire :** non
  - **Valeurs :** <*Numéro du port SSB*>
  - **Détails :** Spécifie le port SSB que SQL Server utilise. SSB est généralement configuré pour utiliser le port TCP 4022, mais vous pouvez configurer un autre port.
- **Nom de clé :** SQLDataFilePath
  - **Obligatoire :** non
  - **Valeurs :** <*Chemin du fichier .mdb de la base de données*>
  - **Détails :** Spécifie un autre emplacement pour créer le fichier .mdb de la base de données.
- **Nom de clé :** SQLLogFilePath
  - **Obligatoire :** non

- **Valeurs :** <*Chemin du fichier .ldf de la base de données*>
- **Détails :** Spécifie un autre emplacement pour créer le fichier .ldf de la base de données.

**HierarchyExpansionOption**

- **Nom de clé :** CCARSiteServer
  - **Obligatoire :** non
  - **Valeurs :** <*Nom de domaine complet du site d'administration centrale*>
  - **Détails :** spécifie le site d'administration centrale auquel un site principal s'attache quand il rejoint la hiérarchie Configuration Manager. Spécifiez le site d'administration centrale lors de l'installation.
- **Nom de clé :** CASRetryInterval
  - **Obligatoire :** non
  - **Valeurs :** <*intervalle*>
  - **Détails :** spécifie l'intervalle (en minutes) avant une nouvelle tentative de connexion au site d'administration centrale après un échec de connexion. Par exemple, en cas d'échec de la connexion au site d'administration centrale, le site principal attend le nombre de minutes que vous avez spécifié pour la valeur **CASRetryInterval** et réessaye d'établir la connexion.
- **Nom de clé :** WaitForCASTimeout
  - **Obligatoire :** non
  - **Valeurs :** <*délai_attente*>

    Valeur de **0** à **100**
  - **Détails :** spécifie la valeur maximale du délai d'attente (en minutes) pour qu'un site principal se connecte au site d'administration centrale. Par exemple, en cas d'échec de la connexion d'un site principal à un site d'administration centrale, le site principal réessaye d'établir la connexion en fonction de la valeur de **CASRetryInterval** jusqu'à ce que le délai **WaitForCASTimeout** soit atteint. Vous pouvez spécifier une valeur entre **0** et **100**.

**CloudConnectorOptions**

- **Nom de clé :** CloudConnector
  - **Obligatoire :** oui
  - **Valeurs :** 0 ou 1

    0 = Ne pas installer

    1 = Installer
  - **Détails :** Spécifie s'il faut installer un point de connexion de service sur ce site. Comme le point de connexion de service peut uniquement être installé sur le site de niveau supérieur d'une hiérarchie, cette valeur doit être **0** pour un site principal enfant.
- **Nom de clé :** CloudConnectorServer
  - **Obligatoire :** Obligatoire quand **CloudConnector** est égal à 1
  - **Valeurs :** <*Nom de domaine complet du serveur de point de connexion de service*>
  - **Détails :** spécifie le nom de domaine complet du serveur qui hébergera le rôle de système de site

de point de connexion de service.

- **Nom de clé :** UseProxy
  - **Obligatoire :** Obligatoire quand **CloudConnector** est égal à 1
  - **Valeurs :** 0 ou 1

    0 = Ne pas installer

    1 = Installer
  - **Détails :** spécifie si le point de connexion de service utilise un serveur proxy.
- **Nom de clé :** ProxyName
  - **Obligatoire :** Obligatoire quand **UseProxy** est égal à 1
  - **Valeurs :** <*Nom de domaine complet du serveur proxy*>
  - **Détails :** spécifie le nom de domaine complet du serveur proxy utilisé par le point de connexion de service.
- **Nom de clé :** ProxyPort
  - **Obligatoire :** Obligatoire quand **UseProxy** est égal à 1
  - **Valeurs :** <*Numéro de port*>
  - **Détails :** Spécifie le numéro de port à utiliser pour le port proxy.

**Récupération sans assistance d'un site d'administration centrale**

Utilisez les détails suivants pour récupérer un site d'administration centrale à l'aide d'un fichier de script d'installation sans assistance.

**Identification**

- **Nom de clé :** Action
  - **Obligatoire :** oui
  - **Valeurs :** RecoverCCAR
  - **Détails :** récupère un site d'administration centrale.
- **Nom de la clé :** CDLatest
  - **Obligatoire :** Oui, uniquement en cas d'utilisation de médias du dossier CD.Latest.
  - **Valeurs :** 1. Toute autre valeur est considérée comme signifiant que CD.Latest ne doit pas être utilisé.
  - **Détails :** Le script doit inclure cette clé et cette valeur en cas d'exécution de l'installation à partir de médias du dossier CD.Latest dans le cadre de l'installation d'un site principal ou d'administration centrale, ou de la récupération d'un site principal ou d'administration centrale. Cette valeur indique au programme d'installation que des médias de CD.Latest sont utilisés.

**RecoveryOptions**

- **Nom de clé :** ServerRecoveryOptions
  - **Obligatoire :** oui
  - **Valeurs :** 1, 2 ou 4

1 = Récupérer le serveur de site et SQL Server.

2 = Récupérer le serveur de site uniquement.

4 = Récupérer SQL Server uniquement.

- **Détails :** spécifie si le programme d'installation récupère le serveur de site, SQL Server, ou les deux. Les clés associées sont nécessaires quand vous définissez la valeur suivante pour le paramètre **ServerRecoveryOptions** :
  - Valeur = 1 : vous avez la possibilité de spécifier une valeur pour la clé **SiteServerBackupLocation** afin de récupérer le site à l'aide d'une sauvegarde de site. Si vous ne spécifiez pas de valeur, le site est réinstallé sans être restauré à partir d'un jeu de sauvegarde.
  - Valeur = 2 : vous avez la possibilité de spécifier une valeur pour la clé **SiteServerBackupLocation** afin de récupérer le site à l'aide d'une sauvegarde de site. Si vous ne spécifiez pas de valeur, le site est réinstallé sans être restauré à partir d'un jeu de sauvegarde.
  - Valeur = 4 : la clé **BackupLocation** est obligatoire si vous attribuez la valeur **10** à la clé **DatabaseRecoveryOptions** afin de restaurer la base de données du site à partir d'une sauvegarde.

- **Nom de clé :** DatabaseRecoveryOptions
  - **Obligatoire :** Cette clé est obligatoire quand la valeur du paramètre **ServerRecoveryOptions** est **1** ou **4**.
  - **Valeurs :** 10, 20, 40 ou 80

    10 = Restaurer la base de données du site à partir d'une sauvegarde.

    20 = Utiliser une base de données de site qui a été récupérée manuellement à l'aide d'une autre méthode.

    40 = Créer une nouvelle base de données de site. Utilisez cette option lorsqu'aucune sauvegarde de base de données de site n'est disponible. Les données globales et de site sont récupérées via la réplication à partir d'autres sites.

    80 = Ignorer la récupération de base de données.
  - **Détails :** spécifie comment le programme d'installation récupère la base de données du site dans SQL Server.

- **Nom de clé :** ReferenceSite
  - **Obligatoire :** cette clé est obligatoire quand la valeur du paramètre **DatabaseRecoveryOptions** est **40**.
  - **Valeurs :** <*Nom de domaine complet du site de référence*>
  - **Détails :** Spécifie le site principal de référence que le site d'administration centrale utilise pour récupérer des données globales si la sauvegarde de la base de données est antérieure à la période de rétention du suivi des modifications ou quand vous récupérez le site sans sauvegarde.

    Quand vous ne spécifiez pas de site de référence et que la sauvegarde est antérieure à la période de rétention du suivi des modifications, tous les sites principaux sont réinitialisés avec les données restaurées à partir du site d'administration centrale.

    Quand vous ne spécifiez pas de site de référence et que la sauvegarde est comprise dans la période

de rétention du suivi des modifications, seules les modifications effectuées après la sauvegarde sont répliquées à partir des sites principaux. Lorsqu'il existe des conflits entre des modifications issues de différents sites principaux, le site d'administration centrale utilise la première modification reçue.

- **Nom de clé :** SiteServerBackupLocation
  - **Obligatoire :** non
  - **Valeurs :** <*Chemin du jeu de sauvegarde du serveur de site*>
  - **Détails :** spécifie le chemin vers le jeu de sauvegarde du serveur de site. Cette clé est optionnelle lorsque la valeur du paramètre **ServerRecoveryOptions** est **1** ou **2**. Spécifiez une valeur pour la clé **SiteServerBackupLocation** pour récupérer le site à l'aide d'une sauvegarde de site. Si vous ne spécifiez pas de valeur, le site est réinstallé sans être restauré à partir d'un jeu de sauvegarde.
- **Nom de clé :** BackupLocation
  - **Obligatoire :** Cette clé est obligatoire quand vous configurez la valeur **1** ou **4** pour la clé **ServerRecoveryOptions**, et la valeur **10** pour la clé **DatabaseRecoveryOptions**.
  - **Valeurs :** <*Chemin du jeu de sauvegarde de la base de données du site*>
  - **Détails :** spécifie le chemin d'accès au jeu de sauvegarde de la base de données du site.

**Options**

- **Nom de clé :** ProductID
  - **Obligatoire :** oui
  - **Valeurs :** <*xxxxx-xxxxx-xxxxx-xxxxx-xxxxx*> *ou* Eval
  - **Détails :** Spécifie la clé de produit de l'installation de Configuration Manager avec les tirets. Entrez **Eval** pour installer la version d'évaluation de Configuration Manager.
- **Nom de clé :** SiteCode
  - **Obligatoire :** oui
  - **Valeurs :** <*Code de site*>
  - **Détails :** spécifie les trois caractères alphanumériques qui identifient le site de manière unique dans votre hiérarchie. Indiquez le code de site que le site utilisait avant la défaillance.
- **Nom de clé :** SiteName
  - **Obligatoire :** non
  - **Valeurs :** <*Nom de site*>
  - **Détails :** spécifie le nom de ce site.
- **Nom de clé :** SMSInstallDir
  - **Obligatoire :** oui
  - **Valeurs :** <*Chemin d'installation de Configuration Manager*>
  - **Détails :** spécifie le dossier d'installation des fichiers programmes de Configuration Manager.
- **Nom de clé :** SDKServer
  - **Obligatoire :** oui

- **Valeurs :** <*Nom de domaine complet du fournisseur SMS*>
- **Détails :** spécifie le nom de domaine complet du serveur qui héberge le fournisseur SMS. Spécifiez le serveur qui hébergeait le fournisseur SMS avant la défaillance.

  Vous pouvez configurer d'autres fournisseurs SMS pour le site après l'installation initiale. Pour plus d'informations sur le fournisseur SMS, consultez Planifier le fournisseur SMS pour System Center Configuration Manager.

- **Nom de clé :** PrerequisiteComp
  - **Obligatoire :** oui
  - **Valeurs :** 0 ou 1

    0 = Télécharger

    1 = Déjà téléchargé
  - **Détails :** spécifie si les fichiers d'installation prérequis ont déjà été téléchargés. Par exemple, si vous utilisez la valeur **0**, le programme d'installation télécharge les fichiers.
- **Nom de clé :** PrerequisitePath
  - **Obligatoire :** oui
  - **Valeurs :** <*Chemin des fichiers nécessaires au programme d'installation*>
  - **Détails :** spécifie le chemin des fichiers nécessaires au programme d'installation. Selon la valeur **PrerequisiteComp** , le programme d'installation utilise ce chemin pour stocker les fichiers téléchargés ou localiser des fichiers déjà téléchargés.
- **Nom de clé :** AdminConsole
  - **Obligatoire :** cette clé est obligatoire sauf quand le paramètre **ServerRecoveryOptions** a la valeur **4**.
  - **Valeurs :** 0 ou 1

    0 = Ne pas installer

    1 = Installer
  - **Détails :** spécifie si la console Configuration Manager doit ou non être installée.
- **Nom de clé :** JoinCEIP

  > **NOTE**
  > À compter de Configuration Manager version 1802, la fonctionnalité CEIP ne figure plus dans le produit.

  - **Obligatoire :** oui
  - **Valeurs :** 0 ou 1

    0 = Ne pas participer

    1 = Participer
  - **Détails :** Spécifie s'il faut participer au programme d'amélioration des services.

**SQLConfigOptions**

- **Nom de clé :** SQLServerName
  - **Obligatoire :** oui
  - **Valeurs :** <*Nom du serveur SQL*>
  - **Détails :** spécifie le nom du serveur ou de l'instance en cluster exécutant SQL Server et qui héberge la base de données du site. Spécifiez le serveur qui a hébergé la base de données de site avant la défaillance.
- **Nom de clé :** DatabaseName
  - **Obligatoire :** oui
  - **Valeurs :** <*Nom de la base de données du site*> ou <*Nom de l'instance*>\<*Nom de la base de données du site*>
  - **Détails :** Spécifie le nom de la base de données SQL Server à créer ou de la base de données SQL Server à utiliser pour installer la base de données du site d'administration centrale. Spécifiez le nom de base de données qui était utilisé avant la défaillance.

    > **IMPORTANT**
    > Si vous n'utilisez pas l'instance par défaut, vous devez spécifier le nom d'instance et le nom de base de données de site.
- **Nom de clé :** SQLSSBPort
  - **Obligatoire :** oui
  - **Valeurs :** <*Numéro du port SSB*>
  - **Détails :** Spécifie le port SSB que SQL Server utilise. Généralement, SSB est configuré pour utiliser le port TCP 4022. Spécifiez le port SSB utilisé avant la défaillance.
- **Nom de clé :** SQLDataFilePath
  - **Obligatoire :** non
  - **Valeurs :** <*Chemin du fichier .mdb de la base de données*>
  - **Détails :** Spécifie un autre emplacement pour créer le fichier .mdb de la base de données.
- **Nom de clé :** SQLLogFilePath
  - **Obligatoire :** non
  - **Valeurs :** <*Chemin du fichier .ldf de la base de données*>
  - **Détails :** Spécifie un autre emplacement pour créer le fichier .ldf de la base de données.

**CloudConnectorOptions**

- **Nom de clé :** CloudConnector
  - **Obligatoire :** oui
  - **Valeurs :** 0 ou 1

    0 = Ne pas installer

    1 = Installer

- **Détails :** Spécifie s'il faut installer un point de connexion de service sur ce site. Comme le point de connexion de service peut uniquement être installé sur le site de niveau supérieur d'une hiérarchie, cette valeur doit être **0** pour un site principal enfant.

- **Nom de clé :** CloudConnectorServer
  - **Obligatoire :** Obligatoire quand **CloudConnector** est égal à 1
  - **Valeurs :** <*Nom de domaine complet du serveur de point de connexion de service*>
  - **Détails :** spécifie le nom de domaine complet du serveur qui hébergera le rôle de système de site de point de connexion de service.
- **Nom de clé :** UseProxy
  - **Obligatoire :** Obligatoire quand **CloudConnector** est égal à 1
  - **Valeurs :** 0 ou 1

    0 = Ne pas installer

    1 = Installer
  - **Détails :** spécifie si le point de connexion de service utilise un serveur proxy.
- **Nom de clé :** ProxyName
  - **Obligatoire :** Obligatoire quand **CloudConnector** est égal à 1
  - **Valeurs :** <*Nom de domaine complet du serveur proxy*>
  - **Détails :** spécifie le nom de domaine complet du serveur proxy utilisé par le point de connexion de service.
- **Nom de clé :** ProxyPort
  - **Obligatoire :** Obligatoire quand **CloudConnector** est égal à 1
  - **Valeurs :** <*Numéro de port*>
  - **Détails :** Spécifie le numéro de port à utiliser pour le port proxy.

**Récupération sans assistance d'un site principal**

Utilisez les détails suivants pour récupérer un site principal à l'aide d'un fichier de script d'installation sans assistance.

**Identification**

- **Nom de clé :** Action
  - **Obligatoire :** oui
  - **Valeurs :** <*RecoverPrimarySite*>
  - **Détails :** récupère un site principal.
- **Nom de la clé :** CDLatest
  - **Obligatoire :** Oui, uniquement en cas d'utilisation de médias du dossier CD.Latest.
  - **Valeurs :** 1. Toute autre valeur est considérée comme signifiant que CD.Latest ne doit pas être utilisé.
  - **Détails :** Le script doit inclure cette clé et cette valeur en cas d'exécution de l'installation à partir de

médias du dossier CD.Latest dans le cadre de l'installation d'un site principal ou d'administration centrale, ou de la récupération d'un site principal ou d'administration centrale. Cette valeur indique au programme d'installation que des médias de CD.Latest sont utilisés.

**RecoveryOptions**

- **Nom de clé :** ServerRecoveryOptions
  - **Obligatoire :** oui
  - **Valeurs :** 1, 2 ou 4

    1 = Récupérer le serveur de site et SQL Server.

    2 = Récupérer le serveur de site uniquement.

    4 = Récupérer SQL Server uniquement.
  - **Détails :** spécifie si le programme d'installation récupère le serveur de site, SQL Server, ou les deux. Les clés associées sont nécessaires quand vous définissez la valeur suivante pour le paramètre **ServerRecoveryOptions** :
    - Valeur = 1 : vous avez la possibilité de spécifier une valeur pour la clé **SiteServerBackupLocation** afin de récupérer le site à l'aide d'une sauvegarde de site. Si vous ne spécifiez pas de valeur, le site est réinstallé sans être restauré à partir d'un jeu de sauvegarde.
    - Valeur = 2 : vous avez la possibilité de spécifier une valeur pour la clé **SiteServerBackupLocation** afin de récupérer le site à l'aide d'une sauvegarde de site. Si vous ne spécifiez pas de valeur, le site est réinstallé sans être restauré à partir d'un jeu de sauvegarde.
    - Valeur = 4 : la clé **BackupLocation** est obligatoire si vous attribuez la valeur **10** à la clé **DatabaseRecoveryOptions** afin de restaurer la base de données du site à partir d'une sauvegarde.
- **Nom de clé :** DatabaseRecoveryOptions
  - **Obligatoire :** Cette clé est obligatoire quand la valeur du paramètre **ServerRecoveryOptions** est **1** ou **4**.
  - **Valeurs :** 10, 20, 40 ou 80

    10 = Restaurer la base de données du site à partir d'une sauvegarde.

    20 = Utiliser une base de données de site qui a été récupérée manuellement à l'aide d'une autre méthode.

    40 = Créer une nouvelle base de données de site. Utilisez cette option lorsqu'aucune sauvegarde de base de données de site n'est disponible. Les données globales et de site sont récupérées via la réplication à partir d'autres sites.

    80 = Ignorer la récupération de base de données.
  - **Détails :** spécifie comment le programme d'installation récupère la base de données du site dans SQL Server.
- **Nom de clé :** SiteServerBackupLocation
  - **Obligatoire :** non
  - **Valeurs :** <*Chemin du jeu de sauvegarde du serveur de site*>

- **Détails :**

  Spécifie le chemin d'accès au jeu de sauvegarde du serveur de site. Cette clé est facultative si le paramètre **ServerRecoveryOptions** a la valeur **1** ou **2**. Spécifiez une valeur pour la clé **SiteServerBackupLocation** pour récupérer le site à l'aide d'une sauvegarde de site. Si vous ne spécifiez pas de valeur, le site est réinstallé sans être restauré à partir d'un jeu de sauvegarde.

- **Nom de clé :** BackupLocation
  - **Obligatoire :** cette clé est obligatoire quand vous configurez la valeur **1** ou **4** pour la clé **ServerRecoveryOptions**, et la valeur **10** pour la clé **DatabaseRecoveryOptions**.
  - **Valeurs :** <*Chemin du jeu de sauvegarde de la base de données du site*>
  - **Détails :** spécifie le chemin d'accès au jeu de sauvegarde de la base de données du site.

**Options**

- **Nom de clé :** ProductID
  - **Obligatoire :** oui
  - **Valeurs :** *xxxxx-xxxxx-xxxxx-xxxxx-xxxxx* ou *Eval*
  - **Détails :** Spécifie la clé de produit de l'installation de Configuration Manager avec les tirets. Entrez **Eval** pour installer la version d'évaluation de Configuration Manager.
- **Nom de clé :** SiteCode
  - **Obligatoire :** oui
  - **Valeurs :** <*Code de site*>
  - **Détails :** spécifie les trois caractères alphanumériques qui identifient le site de manière unique dans votre hiérarchie. Indiquez le code de site que le site utilisait avant la défaillance.
- **Nom de clé :** SiteName
  - **Obligatoire :** non
  - **Valeurs :** <*Nom de site*>
  - **Détails :** spécifie le nom de ce site.
- **Nom de clé :** SMSInstallDir
  - **Obligatoire :** oui
  - **Valeurs :** <*Chemin d'installation de Configuration Manager*>
  - **Détails :** spécifie le dossier d'installation des fichiers programmes de Configuration Manager.
- **Nom de clé :** SDKServer
  - **Obligatoire :** oui
  - **Valeurs :** <*Nom de domaine complet du fournisseur SMS*>
  - **Détails :** spécifie le nom de domaine complet du serveur qui héberge le fournisseur SMS. Indiquez le serveur qui hébergeait le fournisseur SMS avant la défaillance. Configurez d'autres fournisseurs SMS pour le site après l'installation initiale. Pour plus d'informations sur le fournisseur SMS, consultez Planifier le fournisseur SMS.
- **Nom de clé :** PrerequisiteComp

- **Obligatoire :** oui
- **Valeurs :** 0 ou 1

  0 = Télécharger

  1 = Déjà téléchargé
- **Détails :** spécifie si les fichiers d'installation prérequis ont déjà été téléchargés. Par exemple, si vous utilisez la valeur **0**, le programme d'installation télécharge les fichiers.

- **Nom de clé :** PrerequisitePath
  - **Obligatoire :** oui
  - **Valeurs :** <*Chemin des fichiers nécessaires au programme d'installation*>
  - **Détails :** spécifie le chemin des fichiers nécessaires au programme d'installation. Selon la valeur **PrerequisiteComp** , le programme d'installation utilise ce chemin pour stocker les fichiers téléchargés ou localiser des fichiers déjà téléchargés.
- **Nom de clé :** AdminConsole
  - **Obligatoire :** cette clé est obligatoire sauf quand le paramètre **ServerRecoveryOptions** a la valeur **4**.
  - **Valeurs :** 0 ou 1

    0 = Ne pas installer

    1 = Installer
  - **Détails :** spécifie si la console Configuration Manager doit ou non être installée.
- **Nom de clé :** JoinCEIP

  > **NOTE**
  > À compter de Configuration Manager version 1802, la fonctionnalité CEIP ne figure plus dans le produit.

  - **Obligatoire :** oui
  - **Valeurs :** 0 ou 1

    0 = Ne pas participer

    1 = Participer
  - **Détails :** Spécifie s'il faut participer au programme d'amélioration des services.

**SQLConfigOptions**

- **Nom de clé :** SQLServerName
  - **Obligatoire :** oui
  - **Valeurs :** <*Nom du serveur SQL*>
  - **Détails :** spécifie le nom du serveur ou de l'instance en cluster exécutant SQL Server et qui héberge la base de données du site. Spécifiez le serveur qui a hébergé la base de données de site avant la défaillance.
- **Nom de clé :** DatabaseName

- **Obligatoire :** oui
- **Valeurs :** <*Nom de la base de données du site*> ou <*Nom de l'instance*>\<*Nom de la base de données du site*>
- **Détails :**

  Spécifie le nom de la base de données SQL Server à créer ou de la base de données SQL Server à utiliser pour installer la base de données du site d'administration centrale. Spécifiez le nom de base de données qui était utilisé avant la défaillance.

  > **IMPORTANT**
  > Si vous n'utilisez pas l'instance par défaut, vous devez spécifier le nom d'instance et le nom de base de données de site.

- **Nom de clé :** SQLSSBPort
  - **Obligatoire :** oui
  - **Valeurs :** <*Numéro du port SSB*>
  - **Détails :** Spécifie le port SSB que SQL Server utilise. Généralement, SSB est configuré pour utiliser le port TCP 4022. Spécifiez le port SSB utilisé avant la défaillance.
- **Nom de clé :** SQLDataFilePath
  - **Obligatoire :** non
  - **Valeurs :** <*Chemin du fichier .mdb de la base de données*>
  - **Détails :** Spécifie un autre emplacement pour créer le fichier .mdb de la base de données.
- **Nom de clé :** SQLLogFilePath
  - **Obligatoire :** non
  - **Valeurs :** <*Chemin du fichier .ldf de la base de données*>
  - **Détails :** Spécifie un autre emplacement pour créer le fichier .ldf de la base de données.

**HierarchyExpansionOptions**

- **Nom de clé :** CCARSiteServer
  - **Obligatoire :** afficher les détails.
  - **Valeurs :** <*Code du site d'administration centrale*>
  - **Détails :** spécifie le site d'administration centrale auquel un site principal s'attache quand il rejoint la hiérarchie Configuration Manager. Ce paramètre est requis si le site principal était attaché à un site d'administration centrale avant la défaillance. Spécifiez le code de site qui était utilisé pour le site d'administration centrale avant la défaillance.
- **Nom de clé :** CASRetryInterval
  - **Obligatoire :** non
  - **Valeurs :** <*intervalle*>
  - **Détails :** spécifie l'intervalle (en minutes) avant une nouvelle tentative de connexion au site d'administration centrale après un échec de connexion. Par exemple, en cas d'échec de la connexion

au site d'administration centrale, le site principal attend le nombre de minutes que vous avez spécifié pour la valeur **CASRetryInterval** et réessaye d'établir la connexion.

- **Nom de clé :** WaitForCASTimeout
  - **Obligatoire :** non
  - **Valeurs :** <*délai_attente*>
  - **Détails :** spécifie la valeur maximale du délai d'attente (en minutes) pour qu'un site principal se connecte au site d'administration centrale. Par exemple, en cas d'échec de la connexion d'un site principal à un site d'administration centrale, le site principal réessaye d'établir la connexion en fonction de la valeur de **CASRetryInterval** jusqu'à ce que le délai **WaitForCASTimeout** soit atteint. Vous pouvez spécifier une valeur entre **0** et **100**.

**CloudConnectorOptions**

- **Nom de clé :** CloudConnector
  - **Obligatoire :** oui
  - **Valeurs :** 0 ou 1

    0 = Ne pas installer

    1 = Installer
  - **Détails :** Spécifie s'il faut installer un point de connexion de service sur ce site. Comme le point de connexion de service peut uniquement être installé sur le site de niveau supérieur d'une hiérarchie, cette valeur doit être **0** pour un site principal enfant.
- **Nom de clé :** CloudConnectorServer
  - **Obligatoire :** Obligatoire quand **CloudConnector** est égal à 1
  - **Valeurs :** <*Nom de domaine complet du serveur de point de connexion de service*>
  - **Détails :** spécifie le nom de domaine complet du serveur qui hébergera le rôle de système de site de point de connexion de service.
- **Nom de clé :** UseProxy
  - **Obligatoire :** Obligatoire quand **CloudConnector** est égal à 1
  - **Valeurs :** 0 ou 1

    0 = Ne pas installer

    1 = Installer
  - **Détails :** spécifie si le point de connexion de service utilise un serveur proxy.
- **Nom de clé :** ProxyName
  - **Obligatoire :** Obligatoire quand **CloudConnector** est égal à 1
  - **Valeurs :** <*Nom de domaine complet du serveur proxy*>
  - **Détails :** spécifie le nom de domaine complet du serveur proxy utilisé par le point de connexion de service.
- **Nom de clé :** ProxyPort
  - **Obligatoire :** Obligatoire quand **CloudConnector** est égal à 1

- **Valeurs :** <*Numéro de port*>
- **Détails :** Spécifie le numéro de port à utiliser pour le port proxy.

# Installer la console System Center Configuration Manager

22/06/2018 • 7 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les administrateurs se servent de la console Configuration Manager pour gérer l'environnement Configuration Manager. Chaque console Configuration Manager peut se connecter à un site d'administration centrale ou à un site principal, Vous ne pouvez pas connecter une console Configuration Manager à un site secondaire.

> **NOTE**
> Les objets visibles par l'administrateur dans la console dépendent des autorisations attribuées à son compte d'utilisateur. Pour plus d'informations sur l'administration basée sur des rôles, consultez Principes de base de l'administration basée sur des rôles.

Quand vous installez le serveur de site, vous pouvez installer la console Configuration Manager en même temps. Pour installer la console indépendamment du serveur de site, exécutez le programme d'installation autonome.

Utilisez les procédures suivantes pour installer la console Configuration Manager à l'aide du programme d'installation autonome.

## Pour installer la console Configuration Manager à l'aide de l'Assistant Installation

1. Vérifiez que vous disposez des droits suivants :
   - Les droits **d'administrateur** local sur l'ordinateur cible pour la console.
   - Les droits de **Lecture** sur l'emplacement des fichiers d'installation de la console Configuration Manager.
2. Accédez à l'un des emplacements suivants :
   - Sur le serveur de site, accédez à :
     ```
     <Configuration Manager site server installation path>\Tools\ConsoleSetup
     ```
   - À partir du support source Configuration Manager, accédez à :
     ```
     <Configuration Manager source files>\Smssetup\Bin\I386
     ```

> **TIP**
> Au titre des bonnes pratiques, démarrez le programme d'installation de la console Configuration Manager à partir d'un serveur de site plutôt que du support d'installation System Center Configuration Manager. Quand vous installez un serveur de site, il copie les fichiers d'installation de la console Configuration Manager et les modules linguistiques pris en charge pour le site dans le sous-dossier **Tools\ConsoleSetup**. Quand vous installez la console Configuration Manager à partir du support d'installation, la version anglaise est toujours installée. Ce comportement se produit même si le serveur de site prend en charge différentes langues ou qu'une autre langue est définie sur le système d'exploitation de l'ordinateur cible. Vous pouvez éventuellement copier le dossier **ConsoleSetup** vers un autre emplacement pour démarrer l'installation.

3. Pour ouvrir l'Assistant Installation de la console Configuration Manager, double-cliquez sur **consolesetup.exe**.

> **IMPORTANT**
> Installez toujours la console Configuration Manager à l'aide de la commande **consolesetup.exe**. Même si vous pouvez installer la console Configuration Manager en exécutant adminconsole.msi, cette méthode n'effectue pas de vérification des prérequis ni des dépendances. Il se peut que l'installation ne se déroule pas correctement.

4. Dans l'Assistant, sélectionnez **Suivant**.
5. Dans la page **Serveur de site**, entrez le nom de domaine complet (FQDN) du serveur de site auquel la console Configuration Manager se connecte.
6. Dans la page **Dossier d'installation**, entrez le dossier d'installation de la console Configuration Manager. Le chemin du dossier ne doit pas contenir d'espaces de fin ni de caractères Unicode.
7. Dans la page **Programme d'amélioration des services**, indiquez si vous voulez participer à ce programme.

> **NOTE**
> À compter de Configuration Manager version 1802, la fonctionnalité CEIP ne figure plus dans le produit.

8. Dans la page **Prêt pour l'installation**, cliquez sur **Installer** pour installer la console Configuration Manager.

## Pour installer la console Configuration Manager à partir d'une invite de commandes

1. Sur le serveur à partir duquel vous installez la console Configuration Manager, ouvrez une fenêtre d'invite de commandes et accédez à l'un des emplacements suivants :
   - `<Configuration Manager site server installation path>\Tools\ConsoleSetup`
   - `<Configuration Manager installation media>\SMSSETUP\BIN\I386`

> **TIP**
> Quand vous installez la console Configuration Manager à partir d'une invite de commandes, la version anglaise est toujours installée. Ce comportement se produit même si une autre langue est définie sur le système d'exploitation de l'ordinateur cible. Pour installer la console Configuration Manager dans une langue autre que l'anglais, vous devez installer la console Configuration Manager à l'aide de l'Assistant Installation.

2. À partir de l'invite de commandes, tapez **consolesetup.exe**. Choisissez l'une des options de ligne de commande suivantes :

| OPTION DE LIGNE DE COMMANDE | DESCRIPTION |
|---|---|
| /q | Installe la console Configuration Manager sans assistance. Les options **EnableSQM**, **TargetDir**et **DefaultSiteServerName** sont obligatoires avec cette option. |

| OPTION DE LIGNE DE COMMANDE | DESCRIPTION |
| --- | --- |
| /uninstall | Désinstalle la console Configuration Manager. Spécifiez cette option en premier quand vous l'utilisez avec l'option **/q**. |
| LangPackDir | Spécifie le chemin d'accès au dossier qui contient les fichiers de langue. Vous pouvez utiliser le **téléchargeur d'installation** pour télécharger les fichiers de langue. Si vous n'utilisez pas cette option, le programme d'installation recherche le dossier de langue dans le dossier actuel. Si le dossier de langue n'est pas trouvé, le programme d'installation poursuit l'installation en anglais uniquement. Pour plus d'informations, consultez Téléchargeur d'installation. |
| TargetDir | Spécifie le dossier où installer la console Configuration Manager. Vous devez spécifier cette option lorsque vous utilisez l'option **/q** . |
| EnableSQM | Permet de préciser si vous souhaitez vous joindre au programme d'amélioration de l'expérience utilisateur. Utilisez la valeur **1** pour participer au programme d'amélioration des services et la valeur **0** pour ne pas participer au programme. Vous devez spécifier cette option lorsque vous utilisez l'option **/q** .<br>Remarque : Depuis Configuration Manager version 1802, la fonctionnalité CEIP ne figure plus dans le produit. |
| DefaultSiteServerName | Spécifie le nom de domaine complet du serveur de site auquel la console se connecte à son ouverture. Vous devez spécifier cette option lorsque vous utilisez l'option **/q** . |

### Exemples

- `consolesetup.exe /q TargetDir="D:\Program Files\ConfigMgr" EnableSQM=1 DefaultSiteServerName=MyServer.Contoso.com`
- `consolesetup.exe /q LangPackDir=C:\Downloads\ConfigMgr TargetDir="D:\Program Files\ConfigMgr Console" EnableSQM=1 DefaultSiteServerName=MyServer.Contoso.com`
- `consolesetup.exe /uninstall /q`

# Mettre à niveau une installation d'évaluation de System Center Configuration Manager vers une installation complète

22/06/2018 • 3 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Si vous avez installé une version d'évaluation de System Center Configuration Manager, après 180 jours, la console Configuration Manager passe en lecture seule jusqu'à ce que vous activiez le produit dans la page **Maintenance de site** du programme d'installation. À tout moment avant ou après la période de 180 jours, vous pouvez mettre à niveau l'installation d'évaluation vers une installation complète.

> **NOTE**
> Quand vous connectez une console Configuration Manager à une installation d'évaluation de Configuration Manager, la barre de titre de la console indique le nombre de jours restants avant l'expiration de l'installation d'évaluation. Le nombre de jours n'est pas actualisé automatiquement et est mis à jour uniquement quand vous effectuez une nouvelle connexion à un site.

Vous pouvez mettre à niveau les sites suivants qui exécutent une installation d'évaluation :

- Site d'administration centrale
- Site principal

Dans la mesure où les sites secondaires ne sont pas considérés comme des installations d'évaluation, il est inutile de modifier un site secondaire après la mise à niveau de son site parent principal vers une installation complète.

Prérequis à la mise à niveau d'une version d'évaluation vers une version sous licence :

- Vous devez disposer d'un produit valide à utiliser pendant la mise à niveau.
- Votre compte doit avoir des droits **administrateur** sur l'ordinateur sur lequel le site est installé.

**Pour mettre à niveau une version d'évaluation de Configuration Manager vers une version sous licence**

1. Sur le serveur de site, exécutez **Setup.exe** (programme d'installation de Configuration Manager) à partir du dossier d'installation de Configuration Manager (**%chemin%\BIN\X64**). Vous devez exécuter la copie du programme d'installation qui se trouve sur le serveur de site dans le dossier Configuration Manager, car les options de maintenance de site ne sont pas disponibles quand vous exécutez le programme d'installation à partir du support d'installation.
2. Dans la page **Avant de commencer**, sélectionnez **Suivant**.
3. Dans la page **Mise en route**, sélectionnez **Effectuer une maintenance de site ou réinitialiser ce site**, puis sélectionnez **Suivant**.
4. Dans la page **Maintenance de site**, sélectionnez **Passer d'une version d'évaluation à une version sous licence**, entrez une clé de produit valide, puis sélectionnez **Suivant**.
5. Dans la page **Termes du contrat de licence logiciel Microsoft**, lisez et acceptez les termes du contrat de licence, puis sélectionnez **Suivant**.
6. Dans la page **Configuration**, sélectionnez **Fermer** pour terminer l'Assistant.

**NOTE**

La barre de titre d'une console Configuration Manager qui reste connectée au site mis à niveau peut indiquer que le site est toujours une version d'évaluation jusqu'à ce que vous reconnectiez la console au site.

# Mettre à niveau vers System Center Configuration Manager

22/06/2018 • 56 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez exécuter une mise à niveau sur place pour mettre à niveau System Center Configuration Manager à partir d'un site et d'une hiérarchie qui exécute System Center 2012 Configuration Manager.

Avant de procéder à la mise à niveau à partir de System Center 2012 Configuration Manager, vous devez préparer les sites en supprimant des configurations spécifiques qui peuvent empêcher la réussite de l'opération et en suivant la séquence de mise à niveau quand plusieurs sites sont concernés.

> **TIP**
> Lors de la gestion de l'infrastructure de site et de hiérarchie de System Center Configuration Manager, les termes *mise à niveau*, *mise à jour* et *installation* sont utilisés pour décrire trois concepts distincts. Pour connaître la signification et l'usage de chaque terme, consultez À propos de la mise à niveau, de la mise à jour et de l'installation de l'infrastructure de site et de hiérarchie.

## Chemins de mise à niveau sur place

**Mise à niveau vers la version 1802**
Si vous avez un support de base de référence de version 1802, vous pouvez mettre à niveau les produits suivants vers une version sous licence complète de System Center Configuration Manager version 1802 :

- Une installation d'évaluation de System Center Configuration Manager version 1802
- System Center 2012 Configuration Manager avec Service Pack 1
- System Center 2012 Configuration Manager avec Service Pack 2
- System Center 2012 R2 Configuration Manager
- System Center 2012 R2 Configuration Manager avec Service Pack 1

**Mise à niveau vers la version 1702**
Si vous avez un support de base de référence 1702, vous pouvez mettre à niveau les produits suivants vers une version sous licence complète de System Center Configuration Manager version 1702 :

- Une installation d'évaluation de System Center Configuration Manager version 1702
- System Center 2012 Configuration Manager avec Service Pack 1
- System Center 2012 Configuration Manager avec Service Pack 2
- System Center 2012 R2 Configuration Manager
- System Center 2012 R2 Configuration Manager avec Service Pack 1

**Mettre à niveau vers la version 1606**
Le 15 décembre 2016, le média de base de la version 1606 a été republié afin d'ajouter la prise en charge d'autres scénarios de mise à niveau. Cette nouvelle version prend en charge la mise à niveau des produits suivants vers une version sous licence complète de System Center Configuration Manager version 1606 :

- Une installation d'évaluation de System Center Configuration Manager version 1606
- Une installation de version finale (RC) de System Center Configuration Manager

- System Center 2012 Configuration Manager avec Service Pack 1
- System Center 2012 Configuration Manager avec Service Pack 2
- System Center 2012 R2 Configuration Manager sans Service Pack
- System Center 2012 R2 Configuration Manager avec Service Pack 1

Si vous utilisez le média de base de la version 1606 téléchargé avant le 15 décembre 2016, vous pouvez mettre à niveau uniquement les produits suivants vers une version sous licence complète de System Center Configuration Manager version 1606 :

- Une installation d'évaluation de System Center Configuration Manager version 1606
- System Center 2012 Configuration Manager avec Service Pack 2
- System Center 2012 R2 Configuration Manager avec Service Pack 1

> **TIP**
> Une mise à niveau à partir d'une version de System Center 2012 Configuration Manager vers Current Branch peut vous permettre de simplifier votre processus de mise à niveau. Pour plus d'informations, consultez :
>
> - La section Versions de base et de mise à jour dans Mises à jour pour System Center Configuration Manager
> - Dossier CD.Latest pour System Center Configuration Manager

**Les éléments suivants ne sont pas pris en charge :**

- La mise à niveau d'une préversion technique de System Center Configuration Manager vers une installation sous licence complète. Une version d'évaluation technique peut uniquement être mise à niveau vers une version ultérieure de la version d'évaluation technique.
- La migration d'une version Technical Preview vers une version sous licence complète n'est pas pris en charge.

## Listes de vérification de mise à niveau

Les listes de vérification suivantes peuvent vous aider à planifier une mise à niveau vers System Center Configuration Manager.

**Avant la mise à niveau :**

**Passez en revue votre environnement System Center 2012 Configuration Manager** et corrigez les problèmes comme détaillé dans l'article KB4018655 : Les clients Configuration Manager se réinstallent toutes les cinq heures en raison d'une tâche périodique de nouvelle tentative, ce qui peut provoquer une mise à niveau du client par inadvertance.

**Vérifiez que votre environnement informatique répond aux configurations prises en charge** nécessaires à la mise à niveau vers System Center Configuration Manager SP1 :

Passez en revue les systèmes d'exploitation de serveur utilisés pour héberger les rôles de système de site :

- Certains anciens systèmes d'exploitation pris en charge par System Center 2012 Configuration Manager ne sont pas pris en charge par System Center Configuration Manager, et les rôles système de site sur ces systèmes d'exploitation doivent être déplacés ou supprimés avant la mise à niveau. Consultez la documentation Systèmes d'exploitation pris en charge pour les serveurs de système de site.
- L'outil de vérification des conditions préalables pour Configuration Manager ne vérifie pas les prérequis pour les rôles de système de site sur le serveur de site ou sur les systèmes de site distants.

Passez en revue les conditions préalables requises pour chaque ordinateur qui héberge un rôle de système de site :

- Par exemple, pour déployer un système d'exploitation, System Center Configuration Manager utilise le Kit de déploiement et d'évaluation Windows 10 (Windows ADK). Avant d'exécuter le programme d'installation, vous devez télécharger et installer Windows 10 ADK sur le serveur de site et sur chaque ordinateur exécutant une instance du fournisseur SMS.

Pour obtenir des informations générales sur les plateformes prises en charge et les configurations requises, voir Configurations prises en charge pour System Center Configuration Manager.

Pour plus d'informations sur l'utilisation de Windows ADK avec Configuration Manager, consultez Configuration requise de l'infrastructure pour le déploiement de système d'exploitation dans System Center Configuration Manager.

**Examinez l'état des sites et de la hiérarchie et vérifiez qu'il ne reste aucun problème non résolu :**
Avant de mettre à niveau un site, veillez à résoudre tous les problèmes fonctionnels touchant le serveur de site, le serveur de base de données de site et les rôles de système de site installés sur les ordinateurs distants. Une mise à niveau de site peut échouer en raison de l'existence de problèmes fonctionnels.

**Installez toutes les mises à jour critiques applicables aux systèmes d'exploitation des ordinateurs hébergeant le site, le serveur de base de données de site et les rôles de système de site distants :**
Avant de mettre à niveau un site, installez toutes les mises à jour critiques pour chaque système de site concerné. Si vous installez une mise à jour qui nécessite un redémarrage, redémarrez les ordinateurs concernés avant d'entreprendre la mise à jour du Service Pack.

Pour plus d'informations, voir Windows Update.

**Désinstallez les rôles de système de site non pris en charge par System Center Configuration Manager :**
Les rôles système de site suivants ne sont plus utilisés dans System Center Configuration Manager et doivent être désinstallées avant la mise à niveau depuis System Center 2012 Configuration Manager :

- Point de gestion hors bande
- Point du programme de validation d'intégrité système

**Désactivez les réplicas de base de données pour les points de gestion au niveau des sites principaux :**
Configuration Manager ne peut pas réussir la mise à niveau d'un site principal ayant un réplica de base de données activé pour les points de gestion. Désactivez la réplication de base de données avant de :

- Créer une sauvegarde de la base de données pour tester la mise à niveau de base de données
- Mettre à niveau le site de production vers System Center Configuration Manager

Pour plus d'informations, consultez :

- System Center 2012 Configuration Manager : Configurer des réplicas de base de données pour les points de gestion
- System Center Configuration Manager : Réplicas de base de données pour les points de gestion de System Center Configuration Manager

**Reconfigurez les points de mise à jour logicielle qui utilisent l'équilibrage de la charge réseau (NLB) :**
Configuration Manager ne peut pas mettre à niveau un site qui utilise un cluster d'équilibrage de la charge réseau pour héberger des points de mise à jour logicielle.

Si vous utilisez des clusters NLB pour les points de mise à jour logicielle, utilisez PowerShell pour supprimer le cluster NLB. (À compter de System Center 2012 Configuration Manager SP1, aucune option n'existe dans la console Configuration Manager pour configurer un cluster d'équilibrage de la charge réseau.)

**Désactivez toutes les tâches de maintenance de site sur chaque site pendant la durée de la mise à niveau de ce site :**
Avant la mise à niveau vers System Center Configuration Manager, désactivez toutes les tâches de maintenance

de site qui peuvent s'exécuter pendant le processus de mise à niveau. Cela inclut, sans toutefois s'y limiter, les tâches suivantes :

- Serveur de site de sauvegarde
- Supprimer les anciennes opérations du client
- Supprimer les données de découverte anciennes

Lorsqu'une tâche de maintenance de base de données de site s'exécute pendant le processus de mise à niveau, la mise à niveau de site peut échouer.

Avant de désactiver une tâche, il convient d'enregistrer sa planification pour pouvoir restaurer sa configuration après avoir accompli la mise à niveau du site.

Pour plus d'informations sur les tâches de maintenance de site, consultez :

- System Center 2012 Configuration Manager : Planification des tâches de maintenance pour Configuration Manager
- System Center Configuration Manager : Informations de référence sur les tâches de maintenance pour System Center Configuration Manager

**Exécutez l'outil de vérification de la configuration requise.**:
Avant de mettre à niveau un site, vous pouvez exécuter le **vérificateur de la configuration requise** indépendamment du programme d'installation pour vous assurer que votre site est conforme à la configuration requise. Plus tard, quand vous mettez à niveau le site, l'outil de vérification des prérequis s'exécute à nouveau.

Si vous utilisez le média de base de la version 1606 à partir de la version d'octobre 2016, la vérification indépendante des prérequis évalue le site pour la mise à niveau vers Current Branch et LTSB (Long-Term Servicing Branch) de System Center Configuration Manager. Étant donné que certaines fonctionnalités ne sont pas prises en charge par l'édition LTSB, des entrées du fichier *ConfigMgrPrereq.log* peuvent ressembler à ce qui suit :

- INFO : Le site est une édition LTSB.
- Rôle de système de site non pris en charge « Point de synchronisation Asset Intelligence » pour l'édition LTSB ; Erreur ; Configuration Manager a détecté que le « Point de synchronisation Asset Intelligence » est installé. Asset Intelligence n'est pas pris en charge dans l'édition LTSB. Vous devez désinstaller le rôle de système de site du point de synchronisation Asset Intelligence pour pouvoir continuer.

Si vous envisagez de mettre à niveau vers l'édition Current Branch, les erreurs concernant l'édition LTSB peuvent être ignorées en toute sécurité. Elles s'appliquent uniquement si vous envisagez de mettre à niveau vers l'édition LTSB.

Plus tard, quand vous exécutez le programme d'installation de Configuration Manager pour effectuer la mise à niveau, la vérification des prérequis s'exécute à nouveau et évalue votre site en fonction de l'édition de System Center Configuration Manager que vous choisissez d'installer (Current Branch ou LTSB). Si vous choisissez de mettre à niveau vers Current Branch, la vérification des fonctionnalités qui ne sont pas prises en charge par LTSB n'est pas exécutée.

Pour plus d'informations, consultez Outil de vérification des conditions préalables pour System Center Configuration Manager et Liste des vérifications de la configuration requise pour System Center Configuration Manager.

**Téléchargez les fichiers prérequis et les fichiers redistribuables pour System Center Configuration Manager :**
Utilisez le **téléchargeur d'installation** pour télécharger les fichiers redistribuables et prérequis, ainsi que les dernières mises à jour de produit pour System Center Configuration Manager.

Pour plus d'informations, consultez Téléchargeur d'installation pour System Center Configuration Manager.

**Planifier la gestion des langues client et serveur**:
Quand vous mettez à niveau un site, la mise à niveau de site installe uniquement les versions des modules linguistiques que vous sélectionnez pendant la mise à niveau.

- Le programme d'installation examine la configuration de langue actuelle de votre site et identifie les modules linguistiques disponibles dans le dossier où vous avez stocké les fichiers prérequis téléchargés précédemment.
- Vous pouvez alors confirmer la sélection des modules linguistiques serveur et client actifs ou modifier les sélections pour ajouter ou supprimer la prise en charge de langues.
- Vous pouvez sélectionner uniquement les modules linguistiques qui sont disponibles quand vous exécutez le programme d'installation (que vous obtenez avec les fichiers prérequis téléchargés).

> **NOTE**
> Vous ne pouvez pas utiliser les modules linguistiques de System Center 2012 Configuration Manager pour activer des langues pour un site System Center Configuration Manager.

Pour plus d'informations sur les modules linguistiques, consultez Modules linguistiques dans System Center Configuration Manager.

**Passez en revue les considérations relatives aux mises à niveau de site**:
Lorsque vous mettez à niveau un site, certaines fonctionnalités et configurations retrouvent leur configuration par défaut. Pour vous aider à préparer ces modifications et les modifications associées, passez en revue les informations contenues dans Considérations sur la mise à niveau.

**Créez une sauvegarde de la base de données du site au niveau du site d'administration centrale et des sites principaux :**
Avant de mettre à niveau un site, sauvegardez la base de données de site pour être certain de disposer d'une sauvegarde utilisable dans le cadre d'une récupération d'urgence.

Consultez Sauvegarde et récupération pour System Center Configuration Manager.

**Sauvegardez un fichier Configuration.mof personnalisé**:
Si vous utilisez un fichier Configuration.mof personnalisé pour définir des classes de données que vous utilisez avec un inventaire matériel, créez une sauvegarde de ce fichier avant la mise à niveau du site. Après la mise à niveau, restaurez ce fichier sur votre site. Pour plus d'informations sur l'utilisation de ce fichier, consultez Comment étendre l'inventaire matériel dans System Center Configuration Manager.

**Testez le processus de mise à niveau de base de données sur une copie de la dernière sauvegarde de la base de données de site :**
Avant de mettre à niveau un site d'administration centrale ou un site principal Configuration Manager, testez le processus de mise à niveau de base de données de site sur une copie de la base de données de site.

- Vous devez tester le processus de mise à niveau de base de données de site, car quand vous mettez à niveau un site, la base de données peut être modifiée.
- Bien que le test de mise à niveau ne soit pas obligatoire, il peut identifier des problèmes liés à la mise à niveau avant que votre base de données de production ne soit affectée.
- Un échec de mise à niveau de base de données de site peut rendre votre base de données de site inutilisable, et une récupération de site peut s'avérer nécessaire pour rétablir les fonctionnalités.
- Bien que la base de données de site soit partagée entre les sites d'une même hiérarchie, prévoyez de tester la base de données sur chacun des sites concernés avant de procéder à leur mise à niveau.
- Si vous utilisez des réplicas de base de données pour les points de gestion d'un site principal, désactivez la réplication avant de créer la sauvegarde de la base de données de site.

Configuration Manager ne prend en charge ni la sauvegarde des sites secondaires, ni le test de mise à niveau

d'une base de données de site secondaire.

L'exécution d'un test de mise à niveau de base de données sur la base de données de site de production n'est pas prise en charge. Cette opération mettrait à niveau la base de données du site et risquerait de rendre votre site inutilisable.

Pour plus d'informations, voir Tester la mise à niveau de base de données de site.

**Redémarrez le serveur de site et chaque ordinateur qui héberge un rôle de système de site** :
Cela permet de vérifier qu'aucune action liée à une installation récente de mises à jour ou aux prérequis n'est en cours. Il s'agit d'un processus interne propre à l'entreprise.

**Effectuez la mise à niveau des sites.**:
En commençant par le site de niveau supérieur dans la hiérarchie, exécutez Setup.exe à partir du média source de System Center Configuration Manager.

Une fois la mise à niveau du site de niveau supérieur effectuée, vous pouvez commencer la mise à niveau de chaque site enfant. Terminez la mise à niveau de chaque site avant de commencer la mise à niveau du site suivant.

Tant que tous les sites de la hiérarchie n'ont pas été mis à niveau vers System Center Configuration Manager, celle-ci fonctionne en mode de version mixte.

Pour plus d'informations sur l'exécution d'une mise à niveau, consultez Mettre à niveau des sites.

**Après la mise à niveau :**

**Mettez à niveau les consoles Configuration Manager autonomes** :
Par défaut, quand vous mettez à niveau un site d'administration centrale ou un site principal, l'installation met également à niveau la console Configuration Manager installée sur le serveur de site. Toutefois, vous devez mettre à niveau manuellement chaque console installée sur un ordinateur autre que le serveur de site.

> **TIP**
> Fermez chaque console ouverte avant de commencer la mise à niveau.

Pour plus d'informations, consultez Installer des consoles System Center Configuration Manager.

**Reconfigurez les réplicas de base de données des points de gestion au niveau des sites principaux :**
Si vous utilisez des réplicas de base de données pour les points de gestion au niveau des sites principaux, vous devez désinstaller ces réplicas avant la mise à niveau du site. Après avoir mis à niveau un site principal, reconfigurez le réplica de base de données des points de gestion.
Pour plus d'informations, consultez Réplicas de base de données pour les points de gestion de System Center Configuration Manager.

**Reconfigurez les tâches de maintenance de base de données désactivées avant la mise à niveau :**
Si vous avez désactivé des tâches de maintenance de base de données pour System Center Configuration Manager sur un site avant la mise à niveau, reconfigurez ces tâches sur le site en utilisant les paramètres existants avant la mise à niveau.

**Mettez à niveau les clients.**:
Une fois que tous vos sites sont mis à niveau vers System Center Configuration Manager, envisagez de mettre à niveau les clients.

Lorsque vous migrez un client, le logiciel client existant est désinstallé et la nouvelle version du logiciel client est installée. Pour mettre à niveau des clients, vous pouvez appliquer n'importe quelle méthode prise en charge par Configuration Manager.

> **TIP**
> Quand vous mettez à niveau le site de niveau supérieur d'une hiérarchie, le package d'installation du client est également mis à jour sur chaque point de distribution de la hiérarchie. Lorsque vous mettez à niveau un site principal, le package de mise à niveau de client disponible auprès de ce site principal est mis à jour.

Pour plus d'informations sur la mise à niveau de clients existants et sur la façon d'installer de nouveaux clients, consultez Comment mettre à niveau les clients pour les ordinateurs Windows dans System Center Configuration Manager.

## Considérations sur la mise à niveau

**Actions automatiques** :
Quand vous effectuez la mise à niveau vers System Center Configuration Manager, les actions suivantes se produisent automatiquement :

- Le site opère une réinitialisation de site, qui comprend la réinstallation de tous les rôles de système de site.
- Si le site est le site de niveau supérieur d'une hiérarchie, il met à jour le package d'installation de client sur chaque point de distribution de la hiérarchie. Le site met également à jour les images de démarrage par défaut pour utiliser la nouvelle version du système Windows PE fournie avec le Kit de déploiement et d'évaluation Windows 10. Toutefois, la mise à niveau ne met pas niveau les médias existants pour une utilisation avec le déploiement d'image.
- Si le site est un site principal, il met à jour le package de mise à niveau de client de ce site.

**Actions manuelles de l'utilisateur administratif après une mise à niveau**
Après la mise à niveau d'un site, effectuez les actions suivantes :

- Vérifiez que les clients qui sont attribués à chaque site principal sont mis à niveau et installez le logiciel client correspondant à la nouvelle version.
- Mettez à niveau chaque console Configuration Manager qui se connecte au site et qui s'exécute sur un ordinateur distant du serveur de site.
- Sur les sites principaux où vous utilisez des réplicas de base de données pour les points de gestion, reconfigurez ces réplicas.
- Une fois le site mis à niveau, vous devez effectuer une mise à niveau manuelle des médias physiques tels que les fichiers ISO pour les CD et les DVD ou les disques mémoire flash USB, ou les médias préparés utilisés pour les déploiements de Windows To Go ou fournis par des fournisseurs de matériel. Bien que la mise à niveau de site mette à jour les images de démarrage par défaut, elle ne peut pas mettre à niveau ces fichiers multimédias ou les appareils utilisés extérieurs à Configuration Manager.
- Effectuez la mise à jour des images de démarrage autres que les images par défaut quand vous n'avez pas besoin de la version d'origine (plus ancienne) de Windows PE.

**Actions affectant les configurations et les paramètres**
Quand un site est mis à niveau vers System Center Configuration Manager, certaines configurations et certains paramètres ne sont pas conservés après la mise à niveau ou utilisent une nouvelle configuration par défaut. Le tableau ci-dessous répertorie des paramètres qui ne sont pas conservés ou sont modifiés, et fournit des informations qui vous aideront à anticiper ce problème dans le cadre d'une mise à niveau de site :

- **Centre logiciel :**
  Les valeurs par défaut des éléments suivants du Centre logiciel sont rétablies :
  - Les heures d'ouverture indiquées dans**Informations professionnelles** sont réinitialisées sur les valeurs par défaut : de **05:00** à **22:00** Monday à Friday.
  - La valeur de **Maintenance de l'ordinateur** est définie sur **Interrompre les activités du Centre logiciel lorsque mon ordinateur est en mode présentation**.

- La valeur de **Contrôle à distance** est définie sur la valeur attribuée à l'ordinateur dans les paramètres du client.

- **Calendriers de synthèse des mises à jour logicielles :**
  Les calendriers de synthèse personnalisés des mises à jour logicielles ou des groupes de mises à jour logicielles sont réinitialisés à la valeur par défaut (1 heure). Au terme de la mise à niveau, réinitialisez les valeurs de synthèse personnalisées sur la fréquence requise.

## Tester la mise à niveau de base de données de site

Les informations suivantes s'appliquent uniquement lorsque vous mettez à niveau une version antérieure telle que System Center 2012 Configuration Manager vers System Center Configuration Manager.

Avant de mettre à niveau un site, testez une copie de la base de données de ce site pour la mise à niveau.

Pour tester la base de données en vue d'une mise à niveau, vous devez dans un premier temps restaurer une copie de la base de données du site sur une instance de SQL Server qui n'héberge pas de site Configuration Manager. La version de SQL Server que vous utilisez pour héberger la copie de la base de données doit être prise en charge par la version de Configuration Manager, qui est la source de la copie de la base de données.

Ensuite, après avoir restauré la base de données de site, sur l'ordinateur SQL Server, exécutez le programme d'installation de Configuration Manager à partir du dossier du support de source d'installation de System Center Configuration Manager avec l'option de ligne de commande **/TESTDBUPGRADE**.

- Pour plus d'informations sur la façon de créer et de restaurer une sauvegarde de base de données de site, consultez Options de ligne de commande pour le programme d'installation.
- Pour plus d'informations sur l'option de ligne de commande **/TESTDBUPGRADE**, consultez le tableau dans Options de ligne de commande pour le programme d'installation.
- Pour plus d'informations sur les versions de SQL Server prises en charge, consultez la rubrique Prise en charge des versions de SQL Server pour System Center Configuration Manager.

> **TIP**
> Si vous intégrez Microsoft Intune à Configuration Manager :
>
> quand vous exécutez un test de mise à niveau de base de données sur une copie de la base de données qui a cinq jours ou plus, vous pouvez recevoir l'un des messages suivants :
>
> - Avertissement : la mise à niveau va forcer la synchronisation complète vers le cloud.
> - Erreur : la mise à niveau de la base de données va forcer la synchronisation complète vers le cloud.
>
> Vous pouvez sans risque ignorer ces deux messages pendant un test de mise à niveau de base de données, car ils ne signalent pas de défaillance ou de problème avec le test de mise à niveau. Ils indiquent plutôt que lors de la mise à niveau réelle, les données du groupe de réplication de base de données **Cloud** peuvent être synchronisées avec Microsoft Intune.

Utilisez la procédure suivante sur chaque site d'administration centrale et site principal que vous envisagez de mettre à niveau.

**Pour tester une base de données de site pour la mise à niveau**

1. Créez une copie de la base de données du site, puis restaurez cette copie sur une instance de SQL Server qui utilise la même édition que la base de données du site et qui n'héberge pas de site Configuration Manager. Par exemple, si la base de données du site s'exécute sur une instance de l'édition Enterprise de SQL Server, veillez à restaurer la base de données sur une instance de SQL Server qui exécute également l'édition Enterprise de SQL Server.

2. Après avoir restauré la copie de la base de données, exécutez le programme d'installation à partir du support de source d'installation de System Center Configuration Manager. Quand vous exécutez le

programme d'installation, utilisez l'option de ligne de commande **/TESTDBUPGRADE** . Si l'instance SQL Server qui héberge la copie de la base de données n'est pas l'instance par défaut, vous devez également fournir les arguments de ligne de commande pour identifier l'instance qui héberge la copie de la base de données du site.

Par exemple, vous prévoyez de mettre à niveau une base de données de site dont le nom de base de données est SMS_ABC. Vous restaurez une copie de cette base de données de site sur une instance prise en charge de SQL Server ayant pour nom d'instance DBTest. Pour tester une mise à niveau de cette copie de la base de données du site, utilisez la ligne de commande suivante : **Setup.exe /TESTDBUPGRADE DBtest\CM_ABC**

Vous trouverez Setup.exe à l'emplacement suivant sur le média source de System Center Configuration Manager : **SMSSETUP\BIN\X64**.

3. Sur l'instance de SQL Server où vous avez exécuté le test de mise à niveau de base de données, examinez ConfigMgrSetup.log à la racine du lecteur système pour connaître la progression et l'issue du test :

   - Si le test de mise à niveau de la base de données du site échoue, remédiez aux problèmes liés à cet échec, créez une sauvegarde de la base de données du site, puis testez la mise à niveau de la nouvelle copie de la base de données du site.
   - Une fois que le processus a abouti, vous pouvez supprimer la copie de la base de données.

   > **NOTE**
   > Il n'est pas possible de restaurer la copie de la base de données du site que vous utilisez dans le cadre du test de mise à niveau afin de l'utiliser comme base de données d'un site quelconque.

Après avoir mis à niveau une copie de la base de données du site, procédez à la mise à niveau du site Configuration Manager et de sa base de données.

## Effectuez la mise à niveau des sites.

Dès lors que vous avez mené à bien les tâches de configuration préalables à la mise à niveau de votre site, testé la mise à niveau de la base de données du site sur une copie de la base de données, puis téléchargé les fichiers et les modules linguistiques prérequis pour la version du Service Pack que vous prévoyez d'installer, vous êtes prêt à mettre à niveau votre site Configuration Manager.

Lorsque vous mettez à niveau un site qui fait partie d'une hiérarchie, vous mettez d'abord à niveau le site situé le plus haut dans la hiérarchie. Ce site de niveau supérieur est soit un site d'administration centrale, soit un site principal autonome. Après avoir effectué la mise à niveau d'un site d'administration centrale, vous pouvez mettre à niveau les sites principaux enfants dans l'ordre que vous voulez. Une fois que vous avez mis à niveau un site principal, vous pouvez mettre à niveau les sites secondaires enfants de ce site ou mettre à niveau d'autres sites principaux avant de mettre à niveau des sites secondaires.

Pour mettre à niveau un site d'administration centrale ou le site principal, vous exécutez le programme d'installation à partir du support de source d'installation de System Center Configuration Manager. Toutefois, il n'est pas nécessaire d'exécuter le programme d'installation pour mettre à niveau des sites secondaires. Au lieu de cela, il convient d'utiliser la console Configuration Manager pour mettre à niveau un site secondaire après avoir accompli la mise à niveau de son site parent principal.

Avant de mettre à niveau un site, fermez la console Configuration Manager installée sur le serveur du site en attendant que la mise à niveau du site soit terminée. De même, fermez chacune des consoles Configuration Manager qui s'exécutent sur des ordinateurs autres que le serveur du site. Une fois la mise à niveau du site terminée, vous pouvez reconnecter la console. Toutefois, tant que vous n'avez pas mis à niveau une console Configuration Manager vers la nouvelle version de Configuration Manager, cette console ne peut pas afficher

certains objets et certaines informations disponibles dans la nouvelle version de Configuration Manager.

Utilisez les procédures suivantes pour mettre à niveau des sites Configuration Manager :

**Pour mettre à niveau un site d'administration centrale ou un site principal**

1. Vérifiez que l'utilisateur qui exécute le programme d'installation possède les droits de sécurité suivants :
   - Droits d'administrateur local sur l'ordinateur serveur du site.
   - Droits d'administrateur local sur le serveur de base de données de site distant du site, s'il est distant.
2. Sur l'ordinateur serveur de site, ouvrez l'Explorateur Windows et accédez à **<SupportSourceInstallationConfigMg>\SMSSETUP\BIN\X64**.
3. Double-cliquez sur **Setup.exe**. L'Assistant Installation de Configuration Manager s'ouvre.
4. Dans la page **Avant de commencer** , cliquez sur **Suivant**.
5. Sur la page **Mise en route** , sélectionnez **Mettre à niveau ce site Configuration Manager**, puis cliquez sur **Suivant**.
6. Sur la page **Clé du produit** , cliquez sur **Suivant**.

   Si vous avez précédemment installé la version d'évaluation de Configuration Manager, vous pouvez sélectionner **Installer la version illimitée de ce produit avec votre clef de licence**, puis entrer votre clé de produit correspondant à l'installation complète de Configuration Manager pour convertir le site en version complète.

   À partir de la version d'octobre 2016 du support de la base de référence de la version 1606 de System Center Configuration Manager, vous pouvez spécifier la date d'expiration de votre contrat Software Assurance. Vous avez également la possibilité de spécifier la **date d'expiration Software Assurance** de votre contrat de licence en guise de rappel pratique pour vous. Si vous ne l'entrez pas pendant l'installation, vous pouvez la spécifier ultérieurement depuis la console Configuration Manager.

   > **NOTE**
   > Microsoft ne valide pas la date d'expiration que vous entrez et ne l'utilise pas pour la validation de la licence. Vous pouvez ainsi l'utiliser en guise de rappel de votre date d'expiration. Ce rappel s'avère pratique car Configuration Manager vérifie régulièrement les nouvelles mises à jour logicielles proposées en ligne et l'état de votre licence Software Assurance doit être actualisé pour prétendre à l'utilisation de ces mises à jour supplémentaires.

   Pour plus d'informations, consultez Licences et branches pour System Center Configuration Manager.
7. Sur la page **Termes du contrat de licence logiciel Microsoft** , lisez et acceptez les termes du contrat de licence, puis cliquez sur **Suivant**.
8. Sur la page **Licences requises** , lisez et acceptez les termes du contrat de licence pour les logiciels requis, puis cliquez sur **Suivant**. Le programme d'installation télécharge et installe automatiquement les logiciels sur les systèmes ou les clients du site, si nécessaire. Vous devez activer toutes les cases à cocher pour passer à la page suivante.
9. Sur la page **Téléchargements requis** , précisez si le programme d'installation doit télécharger les derniers fichiers redistribuables requis, les modules linguistiques et les dernières mises à jour de produit à partir d'Internet ou utilisez les fichiers téléchargés précédemment, puis cliquez sur **Suivant**. Si vous avez précédemment téléchargé les fichiers à l'aide du téléchargeur d'installation, sélectionnez **Utiliser des fichiers précédemment téléchargés** , puis spécifiez le dossier de téléchargement. Pour plus d'informations, consultez Téléchargeur d'installation.

> **NOTE**
> Si vous utilisez des fichiers téléchargés précédemment, vérifiez que le chemin vers le dossier de téléchargement contient la version la plus récente des fichiers.

10. Sur la page **Sélection de la langue du serveur** , examinez la liste des langues actuellement installées pour le site. Effectuez une sélection parmi les autres langues disponibles sur ce site pour la console Configuration Manager et les rapports, ou effacez les langues que vous ne souhaitez plus prendre en charge sur ce site, puis cliquez sur **Suivant**. L'anglais est sélectionné par défaut et ne peut pas être supprimé.

    > **IMPORTANT**
    > Chaque version de Configuration Manager ne peut pas utiliser les modules linguistiques d'une version antérieure de Configuration Manager. Pour activer la prise en charge d'une langue sur un site Configuration Manager que vous mettez à niveau, vous devez utiliser la version du module linguistique de cette nouvelle version. Pour exemple, pendant la mise à niveau de System Center 2012 Configuration Manager vers System Center Configuration Manager, si la version System Center Configuration Manager d'un module linguistique n'est pas disponible avec les fichiers prérequis que vous téléchargez, la prise en charge de cette langue ne peut pas être installée.

11. Sur la page **Sélection de la langue client** , examinez la liste des langues actuellement installées pour le site. Effectuez une sélection parmi les autres langues disponibles sur ce site pour les ordinateurs clients, ou effacez les langues que vous ne voulez plus prendre en charge sur ce site. Précisez si vous souhaitez activer toutes les langues client pour les clients d'appareil mobile, puis cliquez sur **Suivant**. L'anglais est sélectionné par défaut et ne peut pas être supprimé.

    > **IMPORTANT**
    > Chaque version de Configuration Manager ne peut pas utiliser les modules linguistiques d'une version antérieure de Configuration Manager. Pour activer la prise en charge d'une langue sur un site Configuration Manager que vous mettez à niveau, vous devez utiliser la version du module linguistique de cette nouvelle version. Pour exemple, pendant la mise à niveau de System Center 2012 Configuration Manager vers System Center Configuration Manager, si la version System Center Configuration Manager d'un module linguistique n'est pas disponible avec les fichiers prérequis que vous téléchargez, la prise en charge de cette langue ne peut pas être installée.

12. Sur la page **Résumé des paramètres** , cliquez sur **Suivant** pour démarrer l'outil de vérification des prérequis et vérifier si le serveur est prêt pour une mise à niveau du site.

13. Sur la page **Vérification de l'installation préalable** , si aucun problème n'est répertorié, cliquez sur **Suivant** pour mettre à niveau le site et les rôles de système de site. Lorsque l'outil de vérification des prérequis détecte un problème, cliquez sur un élément dans la liste pour plus d'informations sur la résolution du problème. Résolvez tous les éléments de la liste dont l'état est **Erreur** avant de poursuivre l'installation. Après avoir résolu le problème, cliquez sur **Vérifier** pour relancer la vérification des prérequis. Vous pouvez également ouvrir le fichier ConfigMgrPrereq.log à la racine du lecteur système pour passer en revue les résultats de l'outil de vérification des prérequis. Le fichier journal peut contenir des informations supplémentaires qui ne s'affichent pas dans l'interface utilisateur. Pour obtenir la liste des règles et descriptions relatives aux prérequis de l'installation, consultez Outil de vérification des prérequis.

Sur la page **Mettre à niveau** , le programme d'installation affiche l'état de la progression globale. Lorsque le programme d'installation a terminé l'installation du serveur de site principal et du système de site, vous pouvez fermer l'Assistant. La configuration du site se poursuit en arrière-plan.

#### Pour mettre à niveau un site secondaire

1. Vérifiez que l'utilisateur administratif exécutant le programme d'installation possède les droits de sécurité suivants :
   - Droits d'administrateur local sur l'ordinateur du site secondaire.
   - Rôle de sécurité d'administrateur d'infrastructure ou d'administrateur complet sur le site principal parent.
   - Droits d'administrateur système sur la base de données de site du site secondaire.
2. Dans la console Configuration Manager, cliquez sur **Administration**.
3. Dans l'espace de travail **Administration** , développez **Configuration du site**, puis cliquez sur **Sites**.
4. Sélectionnez le site secondaire à mettre à niveau puis, sous l'onglet **Accueil** , dans le groupe **Site** , cliquez sur **Mettre à niveau**.
5. Cliquez sur **Oui** pour confirmer la décision et lancer la mise à niveau du site secondaire.

La mise à niveau du site secondaire progresse en arrière-plan. Une fois la mise à niveau terminée, vous pouvez vérifier l'état de la console Configuration Manager. Pour ce faire, sélectionnez le serveur du site secondaire puis, sous l'onglet **Accueil** , dans le groupe **Site** , cliquez sur **Afficher l'état d'installation**.

## Exécuter les étapes de post-mise à niveau

Après avoir mis à niveau un site vers un nouveau Service Pack, vous pouvez être amené à effectuer des tâches supplémentaires pour finaliser la mise à niveau ou reconfigurer le site. Ces tâches peuvent consister notamment à mettre à niveau des clients Configuration Manager ou des consoles Configuration Manager, à réactiver des réplicas de base de données pour des points de gestion ou à restaurer des paramètres pour la fonctionnalité Configuration Manager que vous utilisez et qui ne subsiste pas après la mise à niveau du Service Pack.

**Problèmes connus pour les sites secondaires :**

- **Quand vous effectuez la mise à niveau vers la version 1511 :** Pour vérifier que les clients sur les sites secondaires peuvent trouver le point de gestion à partir du site secondaire (point de gestion proxy), ajoutez manuellement le point de gestion aux groupes de limites qui incluent également les points de distribution du site secondaire.
- **Quand vous effectuez la mise à niveau vers la version 1606 ou ultérieure :** Des points de gestion proxy sont automatiquement ajoutés aux groupes de limites qui incluent les points de distribution du site secondaire.

# Scénarios pour simplifier votre installation de System Center Configuration Manager

22/06/2018 • 14 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Avec la publication des versions de mise à jour pour la branche Current Branch de System Center Configuration Manager, de nouveaux scénarios sont apparus pour simplifier l'installation d'une nouvelle hiérarchie sur une version de mise à jour (par exemple, la mise à jour 1610), et pour opérer une mise à niveau à partir de Microsoft System Center 2012 Configuration Manager.

Les scénarios pris en charge sont les suivants :

**Installer une nouvelle hiérarchie de branche Current Branch System Center Configuration Manager** exécutant une version de mise à jour.

- Installez uniquement le site de niveau supérieur puis, immédiatement après, mettez-le à jour avec la version que vous voulez utiliser. Vous pouvez ensuite installer d'autres sites directement sur cette version de mise à jour.
- Ce scénario évite de devoir installer d'autres sites à un niveau de référence, puis de les mettre à jour avec la version de mise à jour que vous voulez utiliser.
- Il évite également de devoir installer les clients sur une version de référence, puis de les réinstaller lors de la mise à jour vers une version ultérieure.

**Mettre à niveau une infrastructure System Center 2012 Configuration Manager** vers une version de mise à jour de System Center Configuration Manager.

- Mettez à niveau manuellement votre site d'administration centrale et chaque site principal vers une version de référence (par exemple, la version 1606) avant d'installer une version de mise à jour (par exemple, la version 1610).
- Ne mettez pas à niveau les sites secondaires à partir de Microsoft System Center 2012 Configuration Manager tant que vos sites principaux n'exécutent pas la version de mise à jour que vous voulez utiliser.
- Ne mettez pas à niveau les clients à partir de Microsoft System Center 2012 Configuration Manager tant que vos sites principaux n'exécutent pas la version de mise à jour que vous voulez utiliser.

## Scénario : Installer une nouvelle hiérarchie sur une version de mise à jour

Dans cet exemple de scénario, installez le premier site d'une hiérarchie à l'aide d'une version de référence de System Center Configuration Manager, telle que la version 1610. Ensuite, installez la mise à jour 1610 avant de déployer des sites ou des clients supplémentaires.

- Comme vous prévoyez d'utiliser une version de mise à jour (telle que la version 1610) et de ne pas en rester à la version de référence (telle que la version 1606), vous n'avez pas besoin d'installer des sites supplémentaires puis de les mettre à niveau. Cela s'applique également aux clients.
- N'installez pas les sites secondaires de version 1606 pour les mettre à niveau vers la version 1610. Au lieu de cela, installez les sites secondaires une fois que les sites principaux exécutent la version 1610.

Suivez l'ordre ci-dessous :

1. **Installez un site de niveau supérieur pour votre nouvelle hiérarchie** à l'aide du support de référence.

- Vous pouvez utiliser le support de référence uniquement pour installer le premier site d'une nouvelle hiérarchie.
- Par exemple, installez un site de niveau supérieur à l'aide de la version de référence 1606. Pour plus d'informations, voir Utiliser l'Assistant Installation pour installer des sites.

Après cette étape, votre site de niveau supérieur exécute la version 1606.

2. **Utilisez des mises à jour dans la console pour mettre à jour votre site de niveau supérieur vers une version ultérieure.**

   - Avant d'installer des clients ou des sites enfants, mettez à jour votre site de niveau supérieur vers la version de mise à jour que vous prévoyez d'utiliser.
   - Par exemple, vous pouvez mettre à jour vers la version 1610 votre site de niveau supérieur qui exécute la version 1606. Pour plus d'informations, consultez Mises à jour pour System Center Configuration Manager.

   Après cette étape, votre site de niveau supérieur exécute la version 1610.

3. **Installez les nouveaux sites principaux enfants sous un site d'administration centrale.**

   - Utilisez le support d'installation du dossier CD.Latest sur le serveur du site d'administration centrale pour installer les sites principaux enfants. Pour plus d'informations, voir Dossier CD.Latest pour System Center Configuration Manager.

     Ce support de source d'installation est requis pour s'assurer que la version des nouveaux sites principaux enfants corresponde à celle du site d'administration centrale.

   Après cette étape, vos nouveaux sites principaux enfants exécutent la version 1610.

4. **Au niveau de chaque site principal, utilisez l'option d'installation dans la console pour installer de nouveaux sites secondaires.**

   - Comme vous n'avez pas installé les sites secondaires quand les sites principaux utilisaient la version 1606, vous n'avez pas besoin de mettre à niveau les sites secondaires.
   - Au lieu de cela, installez de nouveaux sites secondaires qui exécutent la version 1610. Pour plus d'informations, consultez Installer un site secondaire dans la rubrique Utiliser l'Assistant Installation pour installer des sites.

   Après cette étape, les nouveaux sites secondaires sont installés et exécutent la version 1610.

5. **Installez les nouveaux clients sur le site principal.**

   - Comme vous n'avez pas installé de clients quand les sites principaux utilisaient la version 1606, vous n'avez pas besoin de mettre à niveau de clients de version 1606 vers la version 1610.
   - Au lieu de cela, installez de nouveaux clients exécutant la version 1610. Pour plus d'informations, voir Déployer des clients dans System Center Configuration Manager.

   Après cette étape, de nouveaux clients exécutant la version 1610 sont installés.

## Scénario : Mettre à niveau System Center 2012 Configuration Manager vers une version de mise à jour de la branche Current Branch de System Center Configuration Manager

Dans cet exemple de scénario, mettez à niveau votre infrastructure System Center 2012 Configuration Manager vers une version de mise à jour de System Center Configuration Manager, telle que la version 1610.

- Le site d'administration centrale et chaque site principal nécessitent une mise à niveau vers la version de référence 1606 avant l'installation de la mise à jour pour la version 1610.
- La version 1606 n'est pas installée ni mise à niveau sur les sites secondaires et les clients. Au lieu de cela, ils

passent directement de Microsoft System Center 2012 Configuration Manager à System Center Configuration Manager version 1610.

Suivez l'ordre ci-dessous :

1. **Mettez à niveau votre site Microsoft System Center 2012 Configuration Manager de niveau supérieur** vers une version de référence de la branche Current Branch (comme la version 1606) à l'aide du support de source d'installation pour System Center Configuration Manager. Pour plus d'informations, consultez Mettre à niveau vers System Center Configuration Manager.

   - Comme dans les scénarios de mise à niveau classiques, vous mettez toujours à niveau d'abord le site de niveau supérieur d'une hiérarchie, puis les sites enfants.

   Après cette étape, votre site de niveau supérieur exécute la version 1606.

2. **Mettez à niveau chaque site principal enfant dans votre hiérarchie** vers cette même version de référence.

   - Quand vous effectuez la mise à niveau à partir de Microsoft System Center 2012 Configuration Manager, vous devez mettre à niveau manuellement chaque site principal vers une version de référence de Current Branch.
   - Vous ne devez pas mettre à niveau les sites secondaires à ce stade.

   Après cette étape, chaque site principal exécute la version 1606.

3. **Définissez des fenêtres de maintenance sur les sites principaux enfants.** Après avoir mis à niveau tous vos sites principaux vers la version de référence, envisagez de configurer des fenêtres de maintenance pour contrôler le moment où ces sites installeront les mises à jour de l'infrastructure. Pour plus d'informations, consultez Guide pratique pour utiliser les fenêtres de maintenance dans System Center Configuration Manager. (Les fenêtres de maintenance sont appelées *fenêtres de service* dans la version 1606.)

   - Un site principal enfant installe automatiquement les mises à jour que vous installez sur un site d'administration centrale.
   - Les sites secondaires n'installent pas automatiquement les nouvelles versions. Vous devez les mettre à niveau manuellement dans la console.

   Après cette étape, lorsque vous installez des mises à jour sur le site d'administration centrale, les sites principaux enfants n'installent ces mises à jour que lorsque leur fenêtre de maintenance les y autorise.

4. **Installez la version de mise à jour sur votre site de niveau supérieur.** Cela a pour effet de mettre à jour votre site de niveau supérieur. Une fois qu'un site d'administration centrale a installé la version de mise à jour, chaque site principal enfant installe automatiquement cette mise à jour, à moins que l'installation soit bloquée par une fenêtre de maintenance.

   - Par exemple, vous pouvez mettre à jour votre site de niveau supérieur de la version 1606 vers la version 1610. Pour plus d'informations, consultez Mises à jour pour System Center Configuration Manager.

   Après cette étape, votre site d'administration centrale et chaque site principal exécutent la version 1610.

5. **Mettez à niveau les sites secondaires.** Une fois qu'un site principal a installé la mise à jour et exécute la version 1610, utilisez l'option dans la console pour mettre à niveau les sites secondaires.

   - Cela a pour effet de mettre à niveau les sites secondaires directement à partir de Microsoft System Center 2012 Configuration Manager vers la version de mise à jour que vous avez installée sur le site principal.
   - Pour plus d'informations sur la mise à niveau d'un site secondaire, consultez la section sur la mise à niveau des sites dans la rubrique Mettre à niveau vers System Center Configuration Manager.
6. **Mettez à niveau les clients.** Pour mettre à niveau les clients, utilisez les informations de la rubrique Comment mettre à niveau les clients pour les ordinateurs Windows dans System Center Configuration

Manager.

- Cela a pour effet de mettre à niveau les clients directement à partir de Microsoft System Center 2012 Configuration Manager vers la version de mise à jour que vous avez installée sur le site principal.

Après cette étape, les clients sont mis à niveau vers la version 1610 sans mise à niveau préalable vers la version 1606.

# Désinstaller des sites et des hiérarchies dans System Center Configuration Manager

22/06/2018 • 13 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez les informations suivantes comme référence si vous devez désinstaller un site System Center Configuration Manager.

Pour retirer une hiérarchie comportant plusieurs sites, l'ordre de suppression est important. Commencez par désinstaller les sites en bas de la hiérarchie, puis remontez la hiérarchie :

1. Supprimez les sites secondaires rattachés aux sites principaux.
2. Supprimez les sites principaux.
3. Une fois tous les sites principaux supprimés, vous pouvez désinstaller le site d'administration centrale.

## Supprimer un site secondaire d'une hiérarchie

Vous ne pouvez pas déplacer ou réattribuer un site secondaire à un nouveau site principal parent. Pour supprimer un site secondaire d'une hiérarchie, vous devez le supprimer de son site parent direct. Pour ce faire, utilisez l'Assistant Suppression d'un site secondaire de la console Configuration Manager. Lors de la suppression d'un site secondaire, vous devez choisir entre le supprimer et le désinstaller :

- **Désinstaller le site secondaire**. Utilisez cette option pour supprimer un site secondaire fonctionnel accessible à partir du réseau. Cette option désinstalle Configuration Manager du serveur de site secondaire et supprime toutes les informations relatives au site et ses ressources de la hiérarchie de sites Configuration Manager. Si Configuration Manager a installé SQL Server Express dans le cadre de l'installation du site secondaire, SQL Express est désinstallé en même temps que le site secondaire. En revanche, si SQL Server Express a été installé avant le site secondaire, Configuration Manager ne désinstalle pas SQL Server Express.

- **Supprimer le site secondaire**. Utilisez cette option dans l'un des cas de figure suivants :

  - L'installation d'un site secondaire a échoué
  - Le site secondaire continue de figurer dans la console Configuration Manager après sa désinstallation

  Cette option supprime toutes les informations relatives au site et ses ressources de la hiérarchie Configuration Manager, mais laisse Configuration Manager installé sur le serveur de site secondaire.

  > **NOTE**
  > Vous pouvez également utiliser l'outil de maintenance hiérarchique et l'option **/DELSITE** pour supprimer un site secondaire. Pour plus d'informations, consultez Outil de maintenance hiérarchique (Preinst.exe) pour System Center Configuration Manager.

**Pour désinstaller ou supprimer un site secondaire**

1. Vérifiez que l'utilisateur administratif exécutant le programme d'installation possède les droits de sécurité suivants :

   - Droits d'administration sur l'ordinateur de site secondaire
   - Droits d'administrateur local sur le serveur de base de données de site distant pour le site principal, s'il

est distant
   - Rôle de sécurité d'administrateur d'infrastructure ou d'administrateur complet sur le site principal parent
   - Droits d'administrateur système sur la base de données de site du site secondaire
2. Dans la console Configuration Manager, sélectionnez **Administration**.
3. Dans l'espace de travail **Administration**, développez **Configuration du site**, puis sélectionnez **Sites**.
4. Sélectionnez le serveur de site secondaire à supprimer.
5. Sous l'onglet **Accueil**, dans le groupe **Site**, sélectionnez **Supprimer**.
6. Dans la page **Général**, indiquez si vous souhaitez désinstaller ou supprimer le site secondaire, puis cliquez sur **Suivant**.
7. Vérifiez les paramètres de la page **Résumé**, puis sélectionnez **Suivant**.
8. Dans la page **Dernière étape**, sélectionnez **Fermer** pour quitter l'Assistant.

# Désinstaller un site principal

Vous pouvez exécuter le programme d'installation de Configuration Manager pour désinstaller un site principal auquel aucun site secondaire n'est associé. Avant de désinstaller un site principal, prenez connaissance des remarques suivantes :

- Quand des clients Configuration Manager se trouvent dans les limites configurées au niveau du site et que le site principal fait partie d'une hiérarchie Configuration Manager, envisagez d'ajouter les limites à un autre site principal de la hiérarchie avant de désinstaller le site principal.
- Lorsque le serveur de site principal n'est plus disponible, vous devez utiliser l'outil de maintenance hiérarchique au niveau du site d'administration centrale afin de supprimer le site principal de la base de données de site. Pour plus d'informations, consultez Outil de maintenance hiérarchique (Preinst.exe) pour System Center Configuration Manager.

Pour désinstaller un site principal, suivez les instructions ci-dessous.

**Pour désinstaller un site principal**

1. Vérifiez que l'utilisateur administratif exécutant le programme d'installation possède les droits de sécurité suivants :
   - Droits d'administrateur local sur le serveur de site d'administration centrale
   - Droits d'administrateur local sur le serveur de base de données de site distant pour le site d'administration centrale, s'il est distant
   - Droits d'administrateur système sur la base de données du site d'administration centrale
   - Droits d'administrateur local sur l'ordinateur de site principal
   - Droits d'administrateur local sur le serveur de base de données de site distant pour le site principal, s'il est distant
   - Nom d'utilisateur associé au rôle de sécurité Administrateur d'infrastructure ou au rôle Administrateur complet sur le site d'administration centrale
2. Démarrez le programme d'installation de Configuration Manager sur le serveur de site principal en utilisant l'une des méthodes suivantes :
   - Dans le menu **Démarrer**, sélectionnez **Installation de Configuration Manager**.
   - Ouvrez Setup.exe à partir de <*SupportInstallationConfigMgr*>\SMSSETUP\BIN\X64.
   - Ouvrez Setup.exe à partir de <*CheminInstallationConfigMgr*>\BIN\X64.
3. Dans la page **Avant de commencer**, sélectionnez **Suivant**.
4. Dans la page **Mise en route**, sélectionnez **Désinstaller le site Configuration Manager**, puis sélectionnez **Suivant**.
5. Dans la page **Désinstaller le site Configuration Manager**, indiquez si vous souhaitez supprimer la base

de données de site du serveur de site principal et si vous souhaitez supprimer la console Configuration Manager. Par défaut, le programme d'installation supprime les deux éléments.

> **IMPORTANT**
> Lorsqu'un site secondaire est associé au site principal, vous devez au préalable supprimer le site secondaire pour pouvoir désinstaller le site principal.

6. Sélectionnez **Oui** pour confirmer la désinstallation du site principal Configuration Manager.

## Désinstaller un site principal configuré avec des vues distribuées

Pour pouvoir désinstaller un site principal enfant dont le lien de réplication vers le site d'administration centrale contient des vues distribuées, vous devez désactiver les vues distribuées dans votre hiérarchie. Avant de désinstaller un site principal, aidez-vous des informations ci-dessous pour désactiver les vues distribuées.

**Pour désinstaller un site principal configuré avec des vues distribuées**

1. Avant de désinstaller un site principal, vous devez désactiver les vues distribuées sur chaque lien de la hiérarchie reliant le site d'administration centrale et un site principal.
2. Après avoir désactivé les vues distribuées sur chaque lien, vérifiez que les données du site principal sont bien réinitialisées au niveau du site d'administration centrale. Pour surveiller l'initialisation des données, dans la console Configuration Manager, dans l'espace de travail **Surveillance**, affichez le lien dans le nœud **Réplication de la base de données**.
3. Une fois les données réinitialisées auprès du site d'administration centrale, vous pouvez désinstaller le site principal. Pour désinstaller un site principal, consultez Désinstaller un site principal.
4. Une fois le site principal entièrement désinstallé, vous pouvez reconfigurer les vues distribuées sur les liens vers les sites principaux.

> **IMPORTANT**
> Si vous désinstallez le site principal avant de désactiver les vues distribuées de chaque site ou avant de réinitialiser les données du site principal au niveau du site d'administration centrale, la réplication des données entre les sites principaux et le site d'administration centrale risque d'échouer. Dans ce scénario, vous devez désactiver les vues distribuées pour chaque lien de la hiérarchie de sites, puis une fois que les données ont bien été réinitialisées au niveau du site d'administration centrale, vous pouvez reconfigurer les vues distribuées.

## Désinstaller le site d'administration centrale

Vous pouvez exécuter le programme d'installation de Configuration Manager pour désinstaller un site d'administration centrale qui n'a pas de sites principaux enfants. Pour désinstaller un site d'administration centrale, suivez les instructions ci-dessous.

**Pour désinstaller un site d'administration centrale**

1. Vérifiez que l'utilisateur administratif exécutant le programme d'installation possède les droits de sécurité suivants :
   - Droits d'administrateur local sur le serveur de site d'administration centrale
   - Droits d'administrateur local sur le serveur de base de données de site pour le site d'administration centrale, si le serveur de base de données de site n'est pas installé sur le serveur de site
2. Démarrez le programme d'installation de Configuration Manager sur le serveur de site d'administration centrale en utilisant l'une des méthodes suivantes :
   - Dans le menu **Démarrer**, cliquez sur **Installation de Configuration Manager**.

- Ouvrez Setup.exe à partir de <*SupportInstallationConfigMgr*>\SMSSETUP\BIN\X64.
- Ouvrez Setup.exe à partir de <*CheminInstallationConfigMgr*>\BIN\X64.

3. Dans la page **Avant de commencer**, sélectionnez **Suivant**.
4. Dans la page **Mise en route**, sélectionnez **Désinstaller le site Configuration Manager**, puis sélectionnez **Suivant**.
5. Dans la page **Désinstaller le site Configuration Manager**, indiquez si vous souhaitez supprimer la base de données de site du serveur de site d'administration centrale et si vous souhaitez supprimer la console Configuration Manager. Par défaut, le programme d'installation supprime les deux éléments.

   > **IMPORTANT**
   > Si un site principal est associé au site d'administration centrale, vous devez désinstaller le site principal pour pouvoir désinstaller le site d'administration centrale.

6. Sélectionnez **Oui** pour confirmer la désinstallation du site d'administration centrale Configuration Manager.

# Configurer les sites et hiérarchies pour System Center Configuration Manager

22/06/2018 • 8 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Après avoir installé votre premier site System Center Configuration Manager ou ajouté des sites supplémentaires à votre hiérarchie, utilisez la liste de vérification suivante relative aux configurations les plus courantes qui affectent les sites et les hiérarchies.

## Liste de vérification des configurations courantes pour les nouveaux sites et les sites supplémentaires

Prenez en compte les remarques suivantes sur la configuration, qui s'appliquent à la plupart des déploiements :

- Certaines options sont liées, telles que les limites, les groupes de limites et la découverte de forêts Active Directory.
- Plusieurs configurations ont des valeurs par défaut que vous pouvez utiliser sans modification de configuration, au moins temporairement.
- D'autres configurations, telles que celles des groupes de limites et des groupes de points de distribution, doivent être configurées avant de pouvoir être utilisées.

| ACTION | DÉTAILS |
|---|---|
| Configurer l'administration basée sur des rôles | Séparez les attributions d'administration pour contrôler la façon dont les utilisateurs administratifs peuvent afficher et gérer les différents objets et données dans votre environnement Configuration Manager.<br><br>Les configurations de l'administration basée sur des rôles sont partagées avec tous les sites dans une hiérarchie.<br><br>Pour plus d'informations, consultez Configurer l'administration basée sur des rôles pour System Center Configuration Manager. |
| Publier les données de site dans les services de domaine Active Directory (AD DS) | Facilitez la recherche de services et l'utilisation efficace des ressources de site pour les clients.<br><br>Vous devez d'abord étendre le schéma Active Directory pour System Center Configuration Manager, puis chaque site doit être configuré individuellement pour publier des données de site pour System Center Configuration Manager. |
| Configurer un point de connexion de service | Planifiez l'installation et la configuration du point de connexion de service sur le site de niveau supérieur de votre hiérarchie. Pour plus d'informations, voir À propos du point de connexion de service dans System Center Configuration Manager. |

| ACTION | DÉTAILS |
| --- | --- |
| Ajouter des rôles de système de site | Installez un ou plusieurs rôles de système de site supplémentaires pour des sites individuels. Pour plus d'informations, consultez Ajouter des rôles de système de site pour System Center Configuration Manager. |
| Configurer les limites et groupes de limites de site | Spécifiez les limites qui définissent les emplacements réseau sur votre intranet pouvant contenir des appareils que vous souhaitez gérer. Configurez ensuite les groupes de limites pour que les clients à ces emplacements réseau puissent trouver les ressources Configuration Manager. Pour plus d'informations, consultez Définir des limites de site et les groupes de limites pour System Center Configuration Manager. |
| Configurer les groupes de points de distribution | Configurez des groupes logiques de points de distribution pour faciliter la gestion des déploiements. Pour plus d'informations, consultez Gérer les groupes de points de distribution dans Installer et configurer des points de distribution pour System Center Configuration Manager. |
| Exécuter la découverte | Exécutez la découverte pour trouver les ressources sur votre réseau, notamment l'infrastructure réseau, les appareils et les utilisateurs.<br><br>Pour plus d'informations, voir Exécuter la découverte pour System Center Configuration Manager. |
| Accroître la redondance et les fonctionnalités pour les administrateurs qui gèrent votre infrastructure | Installez des fournisseurs SMS et des consoles Configuration Manager supplémentaires pour étendre les fonctionnalités à la disposition des administrateurs qui gèrent votre infrastructure :<br><br>**Installez des fournisseurs SMS supplémentaires** pour fournir une redondance aux points de contact qui gèrent votre site et votre hiérarchie. Pour plus d'informations, consultez Gérer le fournisseur SMS dans Modifier votre infrastructure System Center Configuration Manager.<br><br>**Installez des consoles Configuration Manager supplémentaires** pour fournir un accès à d'autres utilisateurs administratifs. Pour plus d'informations, consultez Installer des consoles Configuration Manager. |
| Configurer des composants de site | Configurez des composants de site sur chaque site pour modifier le comportement des rôles de système du site et les rapports d'état du site. Pour plus d'informations, voir Site components for System Center Configuration Manager. |
| Créer des regroupements personnalisés | En utilisant les informations découvertes sur les appareils et les utilisateurs, créez des regroupements personnalisés d'objets pour simplifier les tâches de gestion à venir. Pour plus d'informations, consultez Guide pratique pour créer des regroupements dans System Center Configuration Manager. |
| Configurer les paramètres de gestion des déploiements à haut risque | Configurez les paramètres d'un site pour avertir les utilisateurs administratifs quand ils créent un déploiement de séquence de tâches à haut risque. Pour plus d'informations, consultez Paramètres pour gérer les déploiements à haut risque pour System Center Configuration Manager. |

| ACTION | DÉTAILS |
| --- | --- |
| Configurer des réplicas de base de données pour les points de gestion | Configurez un réplica de base de données pour réduire la charge processeur placée sur le serveur de base de données de site par les points de gestion qui traitent les demandes des clients. Pour plus d'informations, consultez Réplicas de base de données pour les points de gestion de System Center Configuration Manager. |
| Configurer un groupe de disponibilité SQL Server AlwaysOn pour héberger la base de données du site | À compter de la version 1602, configurez des groupes de disponibilité comme solutions de haute disponibilité et de récupération d'urgence pour héberger la base de données des sites principaux et du site d'administration centrale. Pour plus d'informations, consultez SQL Server AlwaysOn pour une base de données de site à haut niveau de disponibilité pour System Center Configuration Manager. |
| Modifier la réplication entre sites | Pour en savoir plus sur les sujets suivants, consultez Transfert de données entre sites dans System Center Configuration Manager :<br><br>Configurer la réplication basée sur les fichiers entre sites secondaires<br><br>Configurer les liens de réplication de base de données<br><br>Configurer les vues distribuées |

# Ajouter des rôles de système de site pour System Center Configuration Manager

22/06/2018 • 3 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Chaque site System Center Configuration Manager prend en charge plusieurs rôles de système de site. Chaque rôle étend les fonctionnalités de votre site, ainsi que sa capacité à fournir des services au site et à gérer des appareils et des utilisateurs. Tous les rôles de système de site sur un serveur de système de site doivent être membres du même site.

Configuration Manager ne prend pas en charge les rôles système de site pour plusieurs sites sur un serveur de système de site unique.

> **TIP**
> Si vous n'êtes pas familiarisé avec les concepts de base des rôles de système de site ou avec les différences entre le serveur de site, les serveurs de système de site et les rôles de système de site, consultez Principes de base de System Center Configuration Manager.

Les rubriques suivantes décrivent des procédures et détails connexes pour l'installation de rôles système de site :

- Installer des rôles système de site pour System Center Configuration Manager

  Cette rubrique fournit des conseils de base sur l'utilisation des deux Assistants dans la console, qui permettent d'installer de nouveaux rôles de système de site.

- Installer des points de distribution cloud dans Microsoft Azure pour System Center Configuration Manager

  Si vous souhaitez utiliser Microsoft Azure pour héberger le contenu que vous déployez sur des clients, les informations contenues dans cette rubrique vous aideront à configurer les fichiers de certificats nécessaires pour permettre à Configuration Manager de communiquer avec votre abonnement Microsoft Azure et de l'utiliser. En outre, vous devrez configurer la résolution de nom pour permettre à vos clients de rechercher vos points de distribution cloud.

- Installer des rôles système de site pour la gestion des appareils mobiles locale dans System Center Configuration Manager

  Cette rubrique va vous aider à configurer correctement vos rôles de système de site pour prendre en charge la gestion d'appareils modernes à l'aide de la gestion des appareils mobiles locale de Configuration Manager.

- Options de configuration pour les rôles système de site pour System Center Configuration Manager

  Certains rôles de système de site prennent en charge des configurations qui nécessitent plus de détails que ce qui peut être expliqué dans l'interface utilisateur. Cette rubrique fournit ces détails.

# Installer des rôles de système de site pour System Center Configuration Manager

22/06/2018 • 7 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

La console System Center Configuration Manager comporte deux Assistants, que vous pouvez utiliser pour installer des rôles système de site :

- **Assistant Ajout de rôles de système de site**: utilisez cet Assistant pour ajouter des rôles de système de site à un serveur de système de site existant dans le site.
- **Assistant Création d'un serveur de système de site**: utilisez cet Assistant pour spécifier un nouveau serveur comme un serveur de système de site, puis installez un ou plusieurs rôles de système de site sur le serveur. Cet Assistant est le même que l' **Assistant Ajout de rôles de système de site**, sauf que sur la première page, vous devez spécifier le nom du serveur à utiliser et le site dans lequel vous souhaitez l'installer.

Lorsque vous installez un rôle de système de site sur un ordinateur distant (y compris une instance du fournisseur SMS), le compte d'ordinateur de l'ordinateur distant est ajouté à un groupe local du serveur de site. Quand le site est installé sur un contrôleur de domaine, le groupe sur le serveur de site est un groupe de domaine au lieu d'un groupe local. Dans ce cas, le rôle de système de site distant est uniquement opérationnel après le redémarrage de l'ordinateur de rôle de système de site ou après l'actualisation du ticket Kerberos pour le compte de l'ordinateur distant. Pour plus d'informations, consultez Comptes utilisés dans System Center Configuration Manager.

Juste avant d'installer le rôle système de site, Configuration Manager vérifie si l'ordinateur de destination satisfait aux prérequis des rôles système de site que vous avez sélectionnés. Retenez les points suivants concernant l'installation des rôles de système de site :

- Par défaut, quand Configuration Manager installe un rôle système de site, les fichiers d'installation sont installés sur le premier lecteur de disque formaté NTFS disponible dont l'espace libre disponible est le plus grand. Pour empêcher l'installation de Configuration Manager sur des lecteurs spécifiques, créez un fichier vide nommé **no_sms_on_drive.sms**. Copiez-le dans le dossier racine du lecteur avant d'installer le serveur de système de site.
- Configuration Manager utilise le **compte d'installation du système de site** pour installer les rôles système de site. Vous spécifiez ce compte lorsque vous exécutez l'Assistant applicable pour créer un nouveau serveur de système de site ou ajouter des rôles de système de site à un serveur de système de site existant. Par défaut, ce compte est le compte de système local de l'ordinateur du serveur de site, mais vous pouvez spécifier un compte d'utilisateur de domaine à utiliser comme le compte d'installation du système de site. Pour plus d'informations, consultez Comptes utilisés dans System Center Configuration Manager.

## Pour installer des rôles système de site sur un serveur de système de site existant

1. Dans la console Configuration Manager, cliquez sur **Administration**.
2. Dans l'espace de travail **Administration** , développez **Configuration du site**, puis cliquez sur **Serveurs et rôles de système de site**. Ensuite, sélectionnez le serveur que vous souhaitez utiliser pour les nouveaux rôles de système de site.

3. Sous l'onglet **Accueil** , dans le groupe **Serveur** , cliquez sur **Ajouter des rôles de système de site**.
4. Sur la page **Général** , vérifiez les paramètres, puis cliquez sur **Suivant**.

> **TIP**
> Pour accéder au rôle de système de site à partir d'Internet, veillez à spécifier un nom de domaine complet Internet.

5. Dans la page **Proxy**, spécifiez les paramètres d'un serveur proxy si les rôles de système de site qui s'exécutent sur ce serveur de système de site ont besoin d'un serveur proxy pour se connecter à des emplacements sur Internet. Cliquez ensuite sur **Suivant**.
6. Sur la page **Sélection du rôle système** , sélectionnez les rôles de système de site que vous souhaitez ajouter, puis cliquez sur **Suivant**.
7. Effectuez toutes les étapes de l'Assistant.

> **TIP**
> L'applet de commande Windows PowerShell, New-CMSiteSystemServer, assure la même fonction que cette procédure. Pour plus d'informations, consultez New-CMSiteSystemServer dans la documentation de référence des applets de commande System Center 2012 Configuration Manager SP1.

## Pour installer des rôles de système de site sur un nouveau serveur de système de site

1. Dans la console Configuration Manager, cliquez sur **Administration**.
2. Dans l'espace de travail **Administration** , développez **Configuration du site**, puis cliquez sur **Serveurs et rôles de système de site**.
3. Sur l'onglet **Accueil** , dans le groupe **Créer** , cliquez sur **Créer un serveur de système de site**.
4. Sur la page **Général** , spécifiez les paramètres généraux du système de site, puis cliquez sur **Suivant**.

> **TIP**
> Pour accéder au nouveau rôle de système de site à partir d'Internet, veillez à spécifier un nom de domaine complet Internet.

5. Dans la page **Proxy**, spécifiez les paramètres d'un serveur proxy si les rôles de système de site qui s'exécutent sur ce serveur de système de site ont besoin d'un serveur proxy pour se connecter à des emplacements sur Internet. Cliquez ensuite sur **Suivant**.
6. Sur la page **Sélection du rôle système** , sélectionnez les rôles de système de site que vous souhaitez ajouter, puis cliquez sur **Suivant**.
7. Effectuez toutes les étapes de l'Assistant.

> **TIP**
> L'applet de commande Windows PowerShell, New-CMSiteSystemServer, assure la même fonction que cette procédure. Pour plus d'informations, consultez New-CMSiteSystemServer dans la documentation de référence des applets de commande System Center 2012 Configuration Manager SP1.

# Installer des points de distribution cloud dans Microsoft Azure pour System Center Configuration Manager

22/06/2018 • 14 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez installer des points de distribution cloud System Center Configuration Manager dans Microsoft Azure. Si vous n'êtes pas familiarisé avec les points de distribution cloud, consultez Utiliser un point de distribution cloud avant de poursuivre.

Avant de commencer l'installation, vérifiez que vous disposez bien des fichiers de certificat nécessaires :

- Un certificat de gestion Microsoft Azure exporté dans un fichier .cer et un fichier .pfx.
- Un certificat de service de point de distribution cloud Configuration Manager exporté dans un fichier .pfx.

> **TIP**
> Pour plus d'informations sur ces certificats, consultez la section consacrée aux points de distribution cloud dans la rubrique Configuration requise des certificats PKI pour System Center Configuration Manager. Pour obtenir un exemple de déploiement du certificat de service de point de distribution cloud, consultez la section « Déploiement du certificat de service pour les points de distribution cloud » dans la rubrique Exemple de déploiement pas à pas des certificats PKI pour System Center Configuration Manager : autorité de certification Windows Server 2008.

Une fois que vous avez installé le point de distribution cloud, Azure génère automatiquement un GUID pour le service et l'ajoute au suffixe DNS de **cloudapp.net**. En utilisant ce GUID, vous devez configurer DNS avec un alias DNS (enregistrement CNAME). Cela vous permet de mapper le nom de service que vous définissez dans le certificat de service de point de distribution cloud Configuration Manager au GUID généré automatiquement.

Si vous utilisez un serveur Web proxy, vous serez peut-être amené à configurer les paramètres de proxy pour permettre la communication avec le service cloud hébergeant le point de distribution.

## Configurer Azure et installer des points de distribution cloud

Utilisez les procédures suivantes pour configurer la prise en charge par Azure des points de distribution et installer le point de distribution cloud dans Configuration Manager.

**Pour configurer un service cloud dans Azure pour un point de distribution**

1. Dans un navigateur web, accédez au portail Azure sur https://manage.windowsazure.com, puis accédez à votre compte.
2. Cliquez sur **Services hébergés, Comptes de stockage et CDN**, puis sélectionnez **Certificats de gestion**.
3. Cliquez avec le bouton droit sur votre abonnement, puis sélectionnez **Ajouter un certificat**.
4. Pour **Fichier de certificat**, spécifiez le fichier .cer contenant le certificat de gestion Azure exporté à utiliser pour ce service cloud, puis cliquez sur **OK**.

Le certificat de gestion est chargé dans Azure, ce qui vous permet maintenant d'installer un point de distribution

cloud.

**Pour installer un point de distribution cloud pour Configuration Manager**

1. Exécutez les étapes de la procédure précédente pour configurer un service cloud dans Azure avec un certificat de gestion.
2. Dans l'espace de travail **Administration** de la console Configuration Manager, développez **Services cloud**, puis sélectionnez **Points de distribution cloud**. Sous l'onglet **Accueil**, cliquez sur **Créer un point de distribution cloud**.
3. Dans la page **Général** de l'Assistant Création d'un point de distribution cloud, configurez les éléments suivants :
   - Spécifiez l'**ID d'abonnement** de votre compte Azure.

     > **TIP**
     > Vous pouvez trouver votre ID d'abonnement Azure dans le portail Azure.

   - Spécifiez le **Certificat de gestion**. Cliquez sur **Parcourir** pour spécifier le fichier .pfx contenant le certificat de gestion Azure exporté, puis entrez le mot de passe du certificat. Vous pouvez également spécifier un fichier .publishsettings version 1 issu du Kit de développement logiciel Azure SDK 1.7.
4. Cliquez sur **Suivant**. Configuration Manager se connecte à Azure pour valider le certificat de gestion.
5. Dans la page **Paramètres**, effectuez les opérations suivantes et cliquez sur **Suivant** :
   - Pour **Région**, sélectionnez la région Azure dans laquelle vous souhaitez créer le service cloud qui héberge ce point de distribution.
   - Pour **Fichier de certificat**, spécifiez le fichier .pfx qui contient le certificat exporté pour le service de point de distribution cloud Configuration Manager. Entrez ensuite le mot de passe.

     > **NOTE**
     > La zone **FQDN du service** est complétée automatiquement avec le nom d'objet du certificat. Dans la plupart des cas, vous n'avez pas à le modifier. Vous le devrez exceptionnellement si vous utilisez un certificat générique dans un environnement de test. Par exemple, dans ce cas, vous pouvez ne pas spécifier le nom d'hôte pour que plusieurs ordinateurs dotés du même suffixe DNS puissent utiliser ce certificat. Dans ce scénario, l'objet du certificat contient une valeur similaire à **CN=*.contoso.com** et Configuration Manager affiche un message indiquant que vous devez spécifier le nom de domaine complet correct. Cliquez sur **OK** pour fermer le message, puis entrez un nom spécifique avant le suffixe DNS pour fournir un nom de domaine complet. Par exemple, vous pouvez ajouter **clouddp1** pour spécifier le nom de domaine complet du service **clouddp1.contoso.com**. Le nom de domaine complet du service doit être unique dans votre domaine et ne doit correspondre à aucun périphérique joint à un domaine.
     >
     > Les certificats génériques sont pris en charge pour tester les environnements uniquement.
6. Dans la page **Alertes**, configurez les quotas de stockage, les quotas de transfert, ainsi que le pourcentage de ces quotas auquel Configuration Manager doit générer des alertes. Cliquez ensuite sur **Suivant**.
7. Effectuez toutes les étapes de l'Assistant.

L'Assistant crée un service hébergé pour le point de distribution cloud. Après avoir fermé l'Assistant, vous pouvez surveiller la progression de l'installation du point de distribution cloud dans la console Configuration Manager. Vous pouvez également surveiller le fichier **CloudMgr.log** sur le serveur de site principal. Vous pouvez surveiller la mise en service du service cloud dans le portail Azure.

> **NOTE**
> La mise en service d'un nouveau point de distribution dans Azure peut prendre jusqu'à 30 minutes. Le message suivant est répété dans le fichier **CloudMgr.log** tant que le compte de stockage n'est pas approvisionné : **En attente de vérification de l'existence du conteneur. Une nouvelle vérification sera effectuée dans 10 secondes**. Le service est ensuite créé et configuré.

Pour savoir si l'installation du point de distribution cloud est terminée, employez les méthodes suivantes :

- Dans le portail Azure, le **Déploiement** du point de distribution cloud indique l'état **Prêt**.
- Dans la console Configuration Manager, dans l'espace de travail **Administration**, sous le nœud **Configuration de la hiérarchie**, **Cloud**, le point de distribution cloud indique l'état **Prêt**.
- Configuration Manager affiche l'ID de message d'état **9409** pour le composant SMS_CLOUD_SERVICES_MANAGER.

## Configurer la résolution de noms pour les points de distribution cloud

Pour pouvoir accéder au point de distribution cloud, les clients doivent être en mesure de résoudre le nom du point de distribution cloud de manière à fournir une adresse IP gérée par Azure. Pour ce faire, les clients procèdent en deux étapes :

1. Ils mappent le nom de service que vous avez fourni avec le certificat du service de point de distribution cloud Configuration Manager au nom de domaine complet de votre service Azure. Ce nom de domaine complet contient un GUID et le suffixe DNS de **cloudapp.net**. Le GUID est généré automatiquement après l'installation du point de distribution cloud. Vous pouvez afficher le nom de domaine complet dans le portail Azure, en référençant l'**URL du site** dans le tableau de bord du service cloud. Exemple d'URL de site : **http://d1594d4527614a09b934d470.cloudapp.net**.
2. Ils résolvent le nom de domaine complet du service Azure pour fournir l'adresse IP allouée par Azure. Cette adresse IP peut également être identifiée dans le tableau de bord pour le service cloud du portail Azure, et elle est nommée **ADRESSE IP VIRTUELLE PUBLIQUE (VIP)**.

Pour mapper le nom de service que vous avez fourni avec le certificat de service de point de distribution cloud Configuration Manager (par exemple **clouddp1.contoso.com**) au nom de domaine complet de votre service Azure (par exemple **d1594d4527614a09b934d470.cloudapp.net**), les serveurs DNS sur Internet doivent avoir un alias DNS (enregistrement CNAME). Les clients peuvent ensuite résoudre le nom de domaine complet du service Azure pour fournir l'adresse IP en utilisant des serveurs DNS sur Internet.

## Configurer les paramètres de proxy pour des sites principaux gérant des services cloud

Quand vous utilisez des services cloud avec Configuration Manager, le site principal qui gère le point de distribution cloud doit pouvoir se connecter au portail Azure. Le site se connecte à l'aide du compte **Système** de l'ordinateur de site principal. Cette connexion est établie à l'aide du navigateur Web par défaut sur l'ordinateur serveur de site principal.

Sur le serveur de site principal qui gère le point de distribution cloud, vous devrez peut-être configurer les paramètres de proxy pour permettre au site principal d'accéder à Internet et à Azure.

Pour configurer les paramètres de proxy du serveur de site principal dans la console Configuration Manager, exécutez la procédure ci-dessous.

**TIP**

Vous pouvez également configurer le serveur proxy lors de l'installation de nouveaux rôles de système de site sur le serveur de site principal à l'aide de l'**Assistant Ajout des rôles de système de site**.

**Pour configurer les paramètres de proxy pour le serveur de site principal**

1. Dans la console Configuration Manager, cliquez sur **Administration**.
2. Dans l'espace de travail **Administration** , développez **Configuration du site**, puis cliquez sur **Serveurs et rôles de système de site**. Ensuite, sélectionnez le serveur de site principal qui gère le point de distribution cloud.
3. Dans le volet d'informations, cliquez avec le bouton droit sur **Système de site**, puis cliquez sur **Propriétés**.
4. Dans **Propriétés du système de site**, sélectionnez l'onglet **Proxy**, puis configurez les paramètres de proxy de ce serveur de site principal.
5. Cliquez sur **OK** pour enregistrer les paramètres.

# À propos du point de connexion de service dans System Center Configuration Manager

10/07/2018 • 10 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Le point de connexion de service System Center Configuration Manager est un rôle système de site qui remplit plusieurs fonctions importantes pour la hiérarchie. Avant de configurer le point de connexion de service, vous devez comprendre et planifier sa plage d'utilisation. La planification de l'utilisation peut affecter la manière dont vous configurez ce rôle de système de site :

- **Gérer les appareils mobiles avec Microsoft Intune** : ce rôle remplace le connecteur Windows Intune utilisé par les versions précédentes de Configuration Manager et peut être configuré avec les détails de votre abonnement Intune. Consultez Gestion des appareils mobiles (MDM) hybride avec System Center Configuration Manager et Microsoft Intune.
- **Gérer les appareils mobiles avec la gestion MDM locale** : Ce rôle assure la prise en charge des appareils locaux que vous gérez et qui ne se connectent pas à Internet. Consultez Gérer des appareils mobiles avec une infrastructure locale dans System Center Configuration Manager.
- **Charger les données d'utilisation à partir de votre infrastructure Configuration Manager** : vous pouvez contrôler le niveau ou la quantité de détails que vous chargez. Les données chargées permettent ce qui suit :
  - identifier et résoudre les problèmes de manière proactive ;
  - améliorer nos produits et services ;
  - identifier les mises à jour pour Configuration Manager applicables à la version de Configuration Manager que vous utilisez.

  Pour plus d'informations sur les données collectées par chaque niveau et sur la façon de changer le niveau de regroupement après l'installation du rôle, consultez Données d'utilisation et de diagnostic. Ensuite, suivez le lien correspondant à la version de Configuration Manager que vous utilisez.

  Pour plus d'informations, consultez Paramètres et niveaux de données d'utilisation.
- **Télécharger les mises à jour applicables à votre infrastructure Configuration Manager** : seules les mises à jour appropriées pour votre infrastructure sont disponibles, en fonction des données d'utilisation que vous chargez.
- **Chaque hiérarchie prend en charge une seule instance de ce rôle :**
  - Ce rôle de système de site ne peut être installé que sur le site de niveau supérieur de votre hiérarchie (site d'administration centrale ou site principal autonome).
  - Si vous étendez un site principal autonome à une hiérarchie plus importante, vous devez désinstaller ce rôle du site principal pour pouvoir l'installer ensuite sur le site d'administration centrale.

## Modes opératoires

Le point de connexion de service prend en charge deux modes de fonctionnement :

- En **mode en ligne**, le point de connexion de service recherche automatiquement les mises à jour toutes les 24 heures. Il télécharge dans la console Configuration Manager les nouvelles mises à jour disponibles pour la version actuelle de vos infrastructure et produits.
- En **mode hors connexion**, le point de connexion de service ne se connecte pas au service cloud Microsoft. Utilisez l'outil de connexion de service pour System Center Configuration Manager pour importer manuellement les mises à jour disponibles.

Quand vous basculez entre le mode en ligne ou hors connexion après avoir installé le point de connexion de service, vous devez redémarrer le thread SMS_DMP_DOWNLOADER du service SMS_Executive Configuration Manager pour appliquer cette modification. Vous pouvez utiliser Configuration Manager Service Manager pour redémarrer uniquement le thread SMS_DMP_DOWNLOADER du service SMS_Executive. Vous pouvez également redémarrer le service SMS_Executive pour Configuration Manager, ce qui redémarre la plupart des composants de site. Sinon, vous pouvez attendre une tâche planifiée, comme une sauvegarde de site, qui arrête puis redémarre ensuite le service SMS_Executive pour vous.

Pour utiliser le Gestionnaire de service de Configuration Manager, dans la console, accédez à **Surveillance** > **État du système** > **État du composant**, choisissez **Démarrer**, puis **Gestionnaire de service de Configuration Manager**. Dans le Gestionnaire de service :

- Dans le volet de navigation, développez le site, développez **Composants**, puis choisissez le composant à redémarrer.
- Dans le volet d'informations, cliquez avec le bouton droit sur le composant, puis choisissez **Requête**.
- Une fois l'état du composant confirmé, recliquez avec le bouton droit sur le composant, puis choisissez **Arrêter**.
- **Réinterrogez** le composant pour confirmer qu'il est arrêté. Recliquez avec le bouton droit sur le composant, puis choisissez **Démarrer**.

> **IMPORTANT**
> Le processus qui ajoute un abonnement Microsoft Intune au point de connexion de service définit automatiquement le rôle de système de site en ligne. Le point de connexion de service ne prend pas en charge le mode hors connexion en cas de configuration avec un abonnement Intune.

**Quand le rôle s'installe sur un ordinateur distant du serveur de site :**

- Le compte d'ordinateur du serveur de site doit être un administrateur local sur l'ordinateur qui héberge une connexion de service distant.
- Vous devez configurer le serveur de système de site qui héberge le rôle avec un compte d'installation du système de site.
- Le gestionnaire de distribution sur le serveur de site le compte d'installation du système de site pour transférer les mises à jour à partir du point de connexion de service.

## Conditions requises pour l'accès Internet

Pour activer le fonctionnement, l'ordinateur qui héberge le point de connexion de service et les éventuels pare-feu entre cet ordinateur et Internet doivent transmettre les communications via le port sortant **TCP 443** pour HTTPS et le port sortant **TCP 80** pour HTTP aux emplacements Internet suivants. Le point de connexion de service prend également en charge l'utilisation d'un proxy web (avec ou sans authentification) pour utiliser ces emplacements. Si vous devez configurer un compte de proxy web, consultez Prise en charge du serveur proxy dans System Center Configuration Manager.

**Mises à jour et maintenance**

- *.akamaiedge.net
- *.akamaitechnologies.com
- *.manage.microsoft.com
- go.microsoft.com
- blob.core.windows.net
- download.microsoft.com
- download.windowsupdate.com
- sccmconnected-a01.cloudapp.net
- configmgrbits.azureedge.net

**Microsoft Intune**

- *manage.microsoft.com
- https://bspmts.mp.microsoft.com/V
- https://login.microsoftonline.com/{TenantID}

**Maintenance de Windows 10**

- download.microsoft.com
- https://go.microsoft.com/fwlink/?LinkID=619849

## Installer le point de connexion de service

Quand vous exécutez le **programme d'installation** pour installer le site de plus haut niveau d'une hiérarchie, vous avez la possibilité d'installer le point de connexion de service.

Après l'exécution du programme d'installation ou si vous réinstallez le rôle de système de site, utilisez l'Assistant **Ajout des rôles de système de site** ou l'Assistant **Créer un serveur de système de Site** pour installer le système de site sur un serveur au plus haut niveau de votre hiérarchie (c'est-à-dire le site d'administration centrale ou un site principal autonome). Les deux Assistants se trouvent sous l'onglet **Accueil** dans la console, dans **Administration** > **Configuration du site** > **Serveurs et rôles de système de Site**.

## Fichiers journaux utilisés par le point de connexion de service

Pour consulter des informations sur les chargements vers Microsoft, affichez **Dmpuploader.log** sur l'ordinateur qui exécute le point de connexion de service. Pour voir les téléchargements, y compris la progression du téléchargement des mises à jour, affichez **Dmpdownloader.log**. Pour obtenir la liste complète des journaux liés au point de connexion de service, consultez Point de connexion de service dans l'article sur les fichiers journaux de Configuration Manager.

Vous pouvez également utiliser les organigrammes suivants pour comprendre le flux des processus et les entrées du journal principales pour le téléchargement et la réplication des mises à jour vers d'autres sites :

- Organigramme - Téléchargement des mises à jour
- Organigramme - Réplication de mise à jour

# Options de configuration pour les rôles de système de site pour System Center Configuration Manager

22/06/2018 • 19 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

La plupart des options de configuration pour les rôles de système de site System Center Configuration Manager sont explicites ou décrites dans l'Assistant ou des boîtes de dialogue lors de la configuration. Les sections suivantes expliquent les rôles de système de site dont les paramètres peuvent nécessiter des informations supplémentaires.

## Point du site web du catalogue des applications

Pour plus d'informations sur la procédure de configuration du point du site web du catalogue des applications, consultez Planifier et configurer la gestion des applications dans System Center Configuration Manager.

**Connexions client**

Sélectionnez **HTTPS** pour utiliser le paramètre de connexion le plus sécurisé et pour vérifier si les clients se connectent à partir d'Internet. Cette option nécessite un certificat PKI sur le serveur pour l'authentification du serveur sur les clients et pour le chiffrement des données sur le protocole SSL (Secure Socket Layer). Pour en savoir plus sur la configuration requise pour les certificats, consultez Configuration requise des certificats PKI pour System Center Configuration Manager.

Pour obtenir un exemple de déploiement du certificat de serveur et des informations sur la manière de le configurer dans Internet Information Services (IIS), consultez la section *Déploiement du certificat de serveur Web pour les systèmes de site qui exécutent IIS* dans la rubrique Exemple détaillé de déploiement des certificats PKI pour Configuration Manager : Autorité de certification Windows Server 2008.

**Ajouter le site web du catalogue des applications à la zone de sites de confiance**

Ce message affiche la valeur dans les paramètres du client par défaut, que le paramètre client **Ajouter le site Web du catalogue des applications dans la zone Sites approuvés d'Internet Explorer** ait la valeur **True** ou **False**. Si vous avez utilisé des paramètres client personnalisés pour configurer ce paramètre, vous devez vérifier cette valeur vous-même.

Si ce système de site est configuré pour un nom de domaine complet et si le site web ne se trouve pas dans la zone de sites approuvés dans Internet Explorer, les utilisateurs sont invités à entrer leurs informations d'identification quand ils se connectent au catalogue d'applications.

**Nom de l'organisation**

Entrez le nom que voient les utilisateurs dans le catalogue d'applications. Ces informations personnalisées aident les utilisateurs à identifier ce site web comme une source approuvée.

## Point de service web du catalogue des applications

Pour plus d'informations sur la procédure de configuration du point de service web du catalogue des applications, consultez Planifier et configurer la gestion des applications dans System Center Configuration Manager.

**HTTPS**

Sélectionnez **HTTPS** pour authentifier les points de site Web du catalogue d'applications vers ce point de service Web du catalogue des applications. Cette option nécessite un certificat PKI sur les serveurs qui exécutent le point

de site web du catalogue d'applications pour l'authentification du serveur et le chiffrement des données sur le protocole SSL. Pour en savoir plus sur la configuration requise pour les certificats, consultez Configuration requise des certificats PKI pour System Center Configuration Manager.

Pour obtenir un exemple de déploiement du certificat de serveur et des informations sur la manière de le configurer dans IIS, consultez la section *Déploiement du certificat de serveur Web pour les systèmes de site qui exécutent IIS* dans la rubrique Exemple détaillé de déploiement des certificats PKI pour Configuration Manager : Autorité de certification Windows Server 2008.

## Point d'enregistrement de certificat

Pour en savoir plus sur la configuration du point d'enregistrement de certificat, consultez Présentation des profils de certificat.

## Point de distribution

Pour en savoir plus sur la configuration du point de distribution pour le déploiement de contenu, consultez Gérer le contenu et l'infrastructure de contenu pour System Center Configuration Manager.

Pour en savoir plus sur la configuration du point de distribution pour les déploiements PXE, consultez Utiliser PXE pour déployer Windows sur le réseau avec System Center Configuration Manager.

Pour en savoir plus sur la configuration du point de distribution pour les déploiements de multidiffusion, consultez Utiliser la multidiffusion pour déployer Windows sur le réseau avec System Center Configuration Manager.

**Installer et configurer IIS si requis par Configuration Manager**
Sélectionnez cette option pour permettre à Configuration Manager d'installer et de configurer IIS sur le système de site s'il n'est pas déjà installé. IIS doit être installé sur tous les points de distribution, et vous devez sélectionner ce paramètre pour continuer dans l'Assistant.

**Compte d'installation du système de site**
Pour les points de distribution qui sont installés sur un serveur de site, seul le compte d'ordinateur du serveur du site est pris en charge pour être utilisé comme compte d'installation de système de site.

**Créer un certificat auto-signé ou importer un certificat client PKI**
Ce certificat a deux objectifs :

1. Il authentifie le point de distribution à un point de gestion avant que le point de distribution n'envoie des messages d'état.
2. Quand l'option **Activer la prise en charge PXE pour les clients** est sélectionnée, le certificat est envoyé aux ordinateurs qui effectuent un démarrage PXE pour qu'ils puissent se connecter à un point de gestion pendant le déploiement du système d'exploitation.

Quand tous vos points de gestion du site sont configurés pour le protocole HTTP, créez un certificat auto-signé. Quand vos points de gestion sont configurés pour le protocole HTTPS, importez un certificat client PKI.

Pour importer le certificat, accédez à un fichier PKCS #12 (Public Key Cryptography Standard #12) qui contient un certificat PKI avec les spécifications suivantes pour Configuration Manager :

- L'utilisation prévue doit inclure l'authentification du client.
- La clé privée doit être configurée pour l'exportation.

Il n'existe aucune exigence particulière pour le Nom d'objet ou l'Autre nom de l'objet du certificat, et vous pouvez utiliser le même certificat pour plusieurs points de distribution.

Pour en savoir plus sur la configuration requise pour les certificats, consultez Configuration requise des certificats

PKI pour System Center Configuration Manager. Pour obtenir un exemple de déploiement de ce certificat, consultez la section *Déploiement du certificat client pour les points de distribution* de la rubrique Exemple détaillé de déploiement des certificats PKI pour Configuration Manager : Autorité de certification Windows Server 2008.

**Activer ce point de distribution pour le contenu préparé**
Cochez cette case pour activer le point de distribution pour le contenu préparé. Quand cette case est cochée, vous pouvez configurer le comportement de distribution durant la distribution du contenu. Vous pouvez choisir de toujours préparer le contenu sur le point de distribution, de préparer le contenu initial pour le package mais d'utiliser le processus de distribution de contenu normal pour les mises à jour du contenu, ou de toujours utiliser le processus de distribution de contenu normal pour le contenu du package.

**Groupes de limites**
Vous pouvez associer des groupes de limites à un point de distribution. Lors d'un déploiement de contenu, les clients doivent se trouver dans un groupe de limites associé au point de distribution pour l'utiliser comme emplacement source pour le contenu.

- **Avant la version 1610**, vous pouviez cocher la case **Autoriser un emplacement source de secours pour le contenu** pour permettre aux clients situés en dehors de ces groupes de limites de revenir et d'utiliser le point de distribution comme emplacement source pour le contenu quand aucun autre point de distribution n'est disponible.
- **À partir de la version 1610**, vous ne pouvez plus configurer l'option **Autoriser un emplacement source de secours pour le contenu**. Au lieu de cela, vous configurez des relations entre les groupes de limites qui vérifient quand un client peut commencer à rechercher des emplacements sources pour le contenu valides dans d'autres groupes de limites.

## Point d'inscription

Les points d'inscription sont utilisés pour installer les ordinateurs Mac et inscrire les appareils que vous gérez avec la gestion des appareils mobiles locale. Pour plus d'informations, consultez :

- Guide pratique pour déployer des clients sur des ordinateurs Mac dans System Center Configuration Manager
- Comment les utilisateurs inscrivent des appareils avec la gestion des appareils mobiles locale dans System Center Configuration Manager

**Connexions autorisées**
Ce paramètre HTTPS est sélectionné automatiquement et nécessite un certificat PKI sur le serveur pour l'authentification du serveur sur le point proxy d'inscription, l'authentification du serveur sur le point de service hors bande, ainsi que le chiffrement des données sur SSL. Pour en savoir plus sur la configuration requise pour les certificats, consultez Configuration requise des certificats PKI pour System Center Configuration Manager.

Pour obtenir un exemple de déploiement du certificat de serveur et des informations sur la manière de le configurer dans IIS, consultez la section *Déploiement du certificat de serveur Web pour les systèmes de site qui exécutent IIS* dans la rubrique Exemple détaillé de déploiement des certificats PKI pour Configuration Manager : Autorité de certification Windows Server 2008.

## Point proxy d'inscription

Pour en savoir plus sur la configuration d'un point proxy d'inscription pour les appareils mobiles, consultez Comment les utilisateurs inscrivent des appareils avec la gestion des appareils mobiles locale dans System Center Configuration Manager.

**Connexions client**
Le paramètre HTTPS est sélectionné automatiquement. Il nécessite un certificat PKI sur le serveur pour l'authentification du serveur sur les appareils mobiles et les ordinateurs Mac inscrits par Configuration Manager,

ainsi que pour le chiffrement des données avec SSL (Secure Sockets Layer). Pour en savoir plus sur la configuration requise pour les certificats, consultez Configuration requise des certificats PKI pour System Center Configuration Manager.

Pour obtenir un exemple de déploiement du certificat de serveur et des informations sur la manière de le configurer dans IIS, consultez la section *Déploiement du certificat de serveur Web pour les systèmes de site qui exécutent IIS* dans la rubrique Exemple détaillé de déploiement des certificats PKI pour Configuration Manager : Autorité de certification Windows Server 2008.

## Point d'état de secours

**Nombre de messages d'état** et **Intervalle d'accélération (en secondes)**
Bien que les paramètres par défaut pour ces options (10 000 messages d'état et 3 600 secondes pour l'intervalle d'accélération) suffisent dans la plupart des cas, vous pouvez être amené à les modifier lorsque les deux conditions suivantes sont vraies :

- Le point d'état de secours accepte les connexions uniquement à partir de l'intranet.
- Vous utilisez le point d'état de secours pendant un déploiement du client pour de nombreux ordinateurs.

Dans ce scénario, un flux continu de messages d'état peut créer un retard des messages d'état susceptible d'entraîner une utilisation élevée du processeur sur le serveur de site pendant une période prolongée. En outre, vous risquez de ne pas voir les informations récentes sur le déploiement du client dans la console Configuration Manager et dans les rapports de déploiement du client.

Ces paramètres de point d'état de secours visent à être configurés pour les messages d'état générés durant le déploiement du client. Ils ne sont pas destinés à être configurés pour les problèmes de communication que peuvent rencontrer les clients, notamment lorsque ceux-ci se trouvent sur Internet et qu'ils ne parviennent pas à se connecter à leur point de gestion Internet. Comme le point d'état de secours ne peut pas appliquer ces paramètres aux seuls messages d'état générés lors du déploiement du client, ne configurez pas ces paramètres lorsque le point d'état de secours accepte les connexions en provenance d'Internet.

Chaque ordinateur qui installe correctement le client System Center 2012 Configuration Manager envoie les quatre messages d'état ci-dessous au point d'état de secours :

- Démarrage du déploiement du client
- Déploiement du client réussi
- Démarrage de l'attribution du client
- Attribution du client réussie

Les ordinateurs qui ne peuvent pas être installés ou qui affectent le client Configuration Manager envoient des messages d'état supplémentaires.

Par exemple, si vous déployez le client Configuration Manager sur 20 000 ordinateurs, le déploiement peut envoyer 80 000 messages d'état au point d'état de secours. La configuration d'accélération par défaut permet l'envoi d'un maximum de 10 000 messages d'état au point d'état de secours toutes les 3,600 secondes (1 heure), c'est pourquoi les messages d'état peuvent être retardés sur le point d'état de secours. Vous devez également prendre en compte la largeur de bande réseau disponible entre le point d'état de secours et le serveur de site, ainsi que la capacité du serveur de site à traiter de nombreux messages d'état.

Pour éviter ces problèmes, envisagez d'augmenter le nombre de messages d'état et de diminuer l'intervalle d'accélération.

Réinitialisez les valeurs d'accélération pour le point d'état de secours si l'une des conditions suivantes est vraie :

- Les valeurs d'accélération actuelles sont supérieures aux valeurs requises pour traiter les messages d'état à

partir du point d'état de secours.

- Vous trouvez que les paramètres d'accélération actuels entraînent une utilisation élevée du processeur sur le serveur de site.

Ne modifiez pas les paramètres d'accélération du point d'état de secours avant d'en avoir mesuré les conséquences. Par exemple, lorsque vous augmentez les paramètres d'accélération jusqu'à ce qu'ils atteignent un niveau élevé, l'utilisation du processeur sur le serveur de site peut devenir élevée, ce qui ralentit tout le fonctionnement du site.

# Réplicas de base de données pour les points de gestion de System Center Configuration Manager

10/07/2018 • 50 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les sites principaux System Center Configuration Manager peuvent utiliser un réplica de base de données pour réduire la charge processeur placée sur le serveur de base de données du site par les points de gestion à mesure qu'ils traitent les demandes des clients.

- Quand un point de gestion utilise un réplica de base de données, il demande des données de l'ordinateur SQL Server qui héberge le réplica de base de données au lieu du serveur de base de données du site.
- Cela contribue à réduire les besoins de traitement du processeur sur le serveur de base de données du site, grâce au déchargement des tâches de traitement fréquentes liées aux clients. Un exemple de tâche de traitement fréquente pour les clients est celui des sites comportant un grand nombre de clients qui effectuent des demandes fréquentes de stratégie de configuration de client.

## Préparation à l'utilisation de réplicas de base de données

**À propos des réplicas de base de données pour les points de gestion :**

- Les réplicas sont une copie partielle de la base de données du site répliquée sur une instance distincte de SQL Server :
  - Les sites principaux prennent en charge un réplica de base de données dédié pour chaque point de gestion au niveau du site (les sites secondaires ne prennent pas en charge les réplicas de base de données).
  - Un réplica de base de données unique peut être utilisé par plusieurs points de gestion d'un même site.
  - Un serveur SQL Server peut héberger plusieurs réplicas de base de données pour une utilisation par différents points de gestion à condition que chacun s'exécute sur une instance distincte de SQL Server.
- Les réplicas synchronisent une copie de la base de données du site, selon une planification fixe, à partir des données publiées par le serveur de base de données du site à cet effet.
- Vous pouvez configurer un point de gestion pour qu'il utilise un réplica soit au moment de l'installation du point de gestion, soit ultérieurement en reconfigurant le point de gestion déjà installé afin qu'il utilise le réplica de base de données.
- Vérifiez régulièrement le serveur de base de données du site et chaque serveur réplica de base de données pour vous assurer que la réplication s'effectue correctement entre eux, et que les performances du serveur réplica de base de données sont suffisantes pour les performances requises du site et du client.

**Conditions préalables pour les réplicas de base de données :**

- **Configuration requise de SQL Server :**
  - Le serveur SQL Server qui héberge le réplica de base de données doit présenter la même

configuration que le serveur de base de données du site. En revanche, le serveur réplica n'est pas tenu d'exécuter la même version ou édition de SQL Server que le serveur de base de données du site, tant qu'il exécute une version et une édition prises en charge de SQL Server. Pour plus d'informations, consultez Prise en charge des versions de SQL Server pour System Center Configuration Manager.

  - Le service SQL Server sur l'ordinateur qui héberge la base de données réplica doit s'exécuter en tant que compte **système** .
  - La **réplication SQL Server** doit être installée sur les serveurs SQL Server qui hébergent la base de données du site et le réplica de base de données.
  - La base de données du site doit **publier** le réplica de base de données, et chaque serveur réplica de base de données distant doit **s'abonner** aux données publiées.
  - Les serveurs SQL Server qui hébergent la base de données du site et le réplica de base de données doivent être configurés pour prendre en charge une taille de réplication de texte maximale ( **Max Text Repl Size** ) de 2 Go. Pour obtenir un exemple de configuration de cette option pour SQL Server 2012, voir Configurer l'option de configuration du serveur max text repl size.

- **Certificat auto-signé** : pour configurer un réplica de base de données, vous devez créer un certificat auto-signé sur le serveur réplica de base de données et le rendre disponible pour chaque point de gestion devant utiliser ce serveur.
  - Le certificat est automatiquement disponible pour un point de gestion installé sur le serveur de réplica de base de données.
  - Pour rendre ce certificat disponible pour un point de gestion distant, vous devez exporter le certificat, puis l'ajouter au magasin de certificats **Personnes autorisées** sur le point de gestion distant.
- **Notification de client** : pour prendre en charge la notification de client avec un réplica de base de données pour un point de gestion, vous devez configurer la communication entre le serveur de base de données du site et le serveur réplica de base de données pour **SQL Server Service Broker**. Pour cela, vous devez :
  - Configurer chaque base de données avec les informations relatives à l'autre base de données
  - Échanger les certificats entre les deux bases de données pour permettre une communication sécurisée

**Limitations relatives à l'utilisation de réplicas de base de données :**

- Si votre site est configuré pour publier des réplicas de base de données, vous devez suivre les procédures suivantes à la place des instructions standard :
  - Désinstallation d'un serveur de site qui publie un réplica de base de données
  - Déplacement d'une base de données d'un serveur de site qui publie un réplica de base de données
- **Mises à niveau vers System Center Configuration Manager** : avant d'effectuer la mise à niveau d'un site System Center 2012 Configuration Manager vers System Center Configuration Manager Current Branch ou la mise à jour de Configuration Manager Current Branch vers la dernière version, vous devez désactiver les réplicas de base de données pour les points de gestion. Après avoir mis à niveau votre site, reconfigurez les réplicas de base de données pour les points de gestion.
- **Plusieurs réplicas sur un même serveur SQL Server :** si vous configurez un serveur réplica de base

de données pour héberger plusieurs réplicas de base de données pour des points de gestion (chaque réplica devant être sur une instance distincte), vous devez utiliser un script de configuration modifié (voir l'étape 4 de la section suivante) afin que le certificat auto-signé utilisé par les réplicas de base de données précédemment configurés sur ce serveur ne soit pas remplacé.

## Configuration des réplicas de base de données

Pour configurer un réplica de base de données, procédez comme suit :

- Étape 1 : Configuration du serveur de base de données du site pour publier le réplica de base de données
- Étape 2 : Configuration du serveur réplica de base de données
- Étape 3 : Configuration des points de gestion pour utiliser le réplica de base de données
- Étape 4 : Configuration d'un certificat auto-signé pour le serveur réplica de base de données
- Étape 5 : Configuration de Service Broker SQL Server pour le serveur réplica de base de données

**Étape 1 : Configuration du serveur de base de données du site pour publier le réplica de base de données**

Utilisez la procédure suivante comme exemple pour configurer le serveur de base de données de site sur un ordinateur Windows Server 2008 R2 pour publier le réplica de la base de données. Si vous disposez d'une version du système d'exploitation différente, consultez la documentation de votre version de système d'exploitation et adaptez les étapes de la présente procédure en fonction de vos besoins.

Pour configurer le serveur de base de données de site

1. Sur le serveur de base de données de site, définissez le démarrage automatique de l'Agent SQL Server.
2. Sur le serveur de base de données de site, créez un groupe d'utilisateurs local nommé **ConfigMgr_MPReplicaAccess**. Vous devez ajouter le compte d'ordinateur pour chaque serveur de réplica de base de données que vous utilisez sur ce site à ce groupe afin de permettre la synchronisation entre ces serveurs de réplica de base de données et le réplica de base de données publié.
3. Sur le serveur de base de données de site, configurez un fichier de partage nommé **ConfigMgr_MPReplica**.
4. Ajoutez les autorisations suivantes au partage **ConfigMgr_MPReplica** :

   > **NOTE**
   > Si l'Agent SQL Server utilise un compte autre que le compte système local, remplacez SYSTEM par ce nom de compte dans la liste ci-après.

   - **Autorisations de partage**:
     - SYSTEM : **Écriture**
     - ConfigMgr_MPReplicaAccess : **Lecture**
   - **Autorisations NTFS**:
     - SYSTEM : **Contrôle intégral**
     - ConfigMgr_MPReplicaAccess : **Lecture**, **Lecture et exécution**, **Affichage du contenu du dossier**
5. Utilisez **SQL Server Management Studio** pour vous connecter à la base de données de site et exécutez la procédure stockée suivante en tant que requête : **spCreateMPReplicaPublication**

Lorsque la procédure stockée est terminée, le serveur de base de données de site est configuré pour publier le réplica de la base de données.

**Étape 2 : Configuration du serveur réplica de base de données**

Le serveur de réplica de base de données est un ordinateur exécutant SQL Server et hébergeant un réplica de la base de données de site destiné aux points de gestion. Selon une planification fixe, le serveur de réplica de base de données synchronise sa copie de la base de données avec le réplica de base de données qui est publié par le serveur de base de données de site.

Le serveur de réplica de base de données doit répondre aux mêmes exigences que le serveur de base de données de site. Cependant, le serveur de réplica de la base de données peut exécuter une édition ou version de SQL Server différente de celle du serveur de base de données de site. Pour plus d'informations sur les versions de SQL Server prises en charge, consultez la rubrique Prise en charge des versions de SQL Server pour System Center Configuration Manager.

> **IMPORTANT**
> Le service SQL Server sur l'ordinateur qui héberge la base de données de réplica doit s'exécuter comme un compte système.

Utilisez la procédure suivante comme exemple pour configurer un serveur de réplica de base de données sur un ordinateur Windows Server 2008 R2. Si vous disposez d'une version du système d'exploitation différente, consultez la documentation de votre version de système d'exploitation et adaptez les étapes de la présente procédure en fonction de vos besoins.

Pour configurer le serveur de réplica de base de données

1. Sur le serveur de réplica de base de données, définissez le démarrage automatique de l'Agent SQL Server.
2. Sur le serveur de réplica de base de données, utilisez **SQL Server Management Studio** pour vous connecter au serveur local, accédez au dossier **Réplication** , cliquez sur Abonnements locaux, puis sélectionnez **Nouvel abonnement** pour ouvrir l' **Assistant Nouvel abonnement**.
   a. Sur la page **Publication** , dans la liste **Éditeur** , sélectionnez **Rechercher un serveur de publication SQL**, entrez le nom du serveur de base de données de site, puis cliquez sur **Connecter**.
   b. Sélectionnez **ConfigMgr_MPReplica**, puis cliquez sur **Suivant**.
   c. Sur la page **Emplacement de l'Agent de distribution** , sélectionnez **Exécuter chaque agent sur son Abonné (abonnements par extraction de données (pull))**, puis cliquez sur **Suivant**.
   d. Sur la page **Abonnés** , effectuez l'une des opérations ci-après.
      - Sélectionnez une base de données existante à partir du serveur de réplica de base de données à utiliser pour le réplica de base de données, puis cliquez sur **OK**.
      - Sélectionnez **Nouvelle base de données** pour créer une base de données pour le réplica de base de données. Sur la page **Nouvelle base de données** , spécifiez un nom de base de données, puis cliquez sur **OK**.
   e. Cliquez sur **Suivant** pour continuer.
   f. Dans la page **Sécurité de l'Agent de distribution**, cliquez sur le bouton des propriétés **(....)** dans le champ Connexion de l'Abonné de la boîte de dialogue, puis configurez les paramètres de sécurité pour la connexion.

> **TIP**
> Le bouton des propriétés, **(....)**, se trouve dans la quatrième colonne de la zone d'affichage.

**Paramètres de sécurité :**

- Configurez le compte qui exécute le processus de l'Agent de distribution (le compte de processus) :
  - Si l'Agent SQL Server s'exécute en tant que système local, sélectionnez **Exécuter sous le compte du service de l'Agent SQL Server (non recommandé pour des raisons de sécurité.)**.
  - Si l'Agent SQL Server s'exécute à l'aide d'un autre compte, sélectionnez **Exécuter sous le compte Windows suivant**, puis configurez ce compte. Vous pouvez spécifier un compte Windows ou un compte SQL Server.

> **IMPORTANT**
> Vous devez accorder au compte qui exécute l'Agent de distribution des autorisations sur l'éditeur comme un abonnement par extraction. Pour plus d'informations sur la configuration de ces autorisations, consultez Sécurité de l'Agent de distribution dans la bibliothèque TechNet de SQL Server.

- Pour **Se connecter au serveur de distribution**, sélectionnez **En imitant le compte de processus**.
- Pour **Connexion à l'Abonné**, sélectionnez **En imitant le compte de processus**.

  Après la configuration des paramètres de sécurité de connexion, cliquez sur **OK** pour les enregistrer, puis cliquez sur **Suivant**.

g. Sur la page **Planification des synchronisations** , dans la zone de liste **Planification de l'agent** , sélectionnez **Définir la planification**, puis configurez **Nouvelle planification du travail**. Définissez la fréquence sur **Quotidienne**, toutes les **5 minute(s)**, et la durée sur **aucune date de fin**. Cliquez sur **Suivant** pour enregistrer la planification, puis cliquez sur **Suivant** de nouveau.

h. Sur la page **Actions de l'Assistant** , activez la case à cocher **Créer les abonnements**, puis cliquez sur **Suivant**.

i. Dans la page **Terminer l'Assistant** , cliquez sur **Terminer**, puis cliquez sur **Fermer** pour fermer l'Assistant.

3. Immédiatement après la fin de l'exécution de l'Assistant Nouvel abonnement, utilisez **SQL Server Management Studio** pour vous connecter à la base de données du serveur de réplication de base de données, puis exécutez la requête suivante pour activer la propriété de base de données TRUSTWORTHY : `ALTER DATABASE <MP Replica Database Name> SET TRUSTWORTHY ON;`

4. Vérifiez l'état de la synchronisation pour valider la réussite de l'abonnement :
   - Sur l'ordinateur de l'abonné :
     - Dans **SQL Server Management Studio**, connectez-vous au serveur de réplica de base de données, puis développez le dossier **Réplication**.
     - Développez **Abonnements locaux**, cliquez avec le bouton droit sur l'abonnement à la publication de la base de données de site, puis sélectionnez **Afficher l'état de**

**synchronisation**.

- Sur l'ordinateur de l'éditeur :
  - Dans **SQL Server Management Studio**, connectez-vous à l'ordinateur de base de données de site, cliquez avec le bouton droit sur le dossier **Réplication** , puis sélectionnez **Lancer le moniteur de réplication**.

5. Pour activer l'intégration du CLR pour le réplica de base de données, utilisez **SQL Server Management Studio** pour vous connecter au réplica de base de données sur le serveur de réplica de base de données, puis exécutez la procédure stockée suivante en tant que requête : **exec sp_configure 'clr enabled', 1; RECONFIGURE WITH OVERRIDE**

6. Pour chaque point de gestion qui utilise un serveur de réplica de base de données, ajoutez le compte d'ordinateur de ce point de gestion au groupe local **Administrateurs** sur le serveur de réplica de base de données.

   > **TIP**
   > Cette étape n'est pas nécessaire pour un point de gestion qui s'exécute sur le serveur de réplica de base de données.

   Le réplica de base de données est maintenant prêt à l'utilisation par un point de gestion.

**Étape 3 : Configuration des points de gestion pour utiliser le réplica de base de données**

Vous pouvez configurer un point de gestion sur un site principal pour utiliser un réplica de base de données lorsque vous installez un rôle de point de gestion, ou bien, vous pouvez reconfigurer un point de gestion existant pour utiliser le réplica de base de données.

Pour configurer un point de gestion pour utiliser un réplica de base de données, utilisez les informations suivantes :

- **Pour configurer un nouveau point de gestion :** Dans la page **Base de données du point de gestion** de l'Assistant d'installation du point de gestion, sélectionnez **Utiliser un réplica de la base de données**, puis spécifiez le nom de domaine complet de l'ordinateur qui héberge le réplica de base de données. Ensuite, sous **Nom de base de données de site ConfigMgr**, spécifiez le nom de base de données du réplica de base de données sur cet ordinateur.
- **Pour configurer un point de gestion précédemment installé**: Sur la page Propriétés du point de gestion, sélectionnez l'onglet **Base de données du point de gestion** , sélectionnez **Utiliser un réplica de la base de données**, puis spécifiez le nom de domaine complet de l'ordinateur hébergeant le réplica de base de données. Ensuite, sous **Nom de base de données de site ConfigMgr**, spécifiez le nom de base de données du réplica de base de données sur cet ordinateur.
- **Pour chaque point de gestion qui utilise un réplica de base de données**, vous devez ajouter manuellement le compte d'ordinateur du serveur de point de gestion au rôle **db_datareader** pour le réplica de base de données.

Outre la configuration du point de gestion pour utiliser le serveur de réplica de base de données, vous devez activer l'option **Authentification Windows** dans **IIS** sur le point de gestion :

1. Ouvrez **Gestionnaire des services Internet (IIS)**.
2. Sélectionnez le site Web utilisé par le point de gestion, puis cliquez sur **Authentification**.
3. Définissez **Authentification Windows** sur **Activé**, puis fermez le **Gestionnaire des services Internet (IIS)**.

### Étape 4 : Configuration d'un certificat auto-signé pour le serveur réplica de base de données

Vous devez créer un certificat auto-signé sur le serveur de réplica de base de données et le rendre disponible pour chaque point de gestion qui utilisera ce serveur.

Le certificat est automatiquement disponible pour un point de gestion installé sur le serveur de réplica de base de données. Cependant, pour rendre ce certificat disponible pour les points de gestion distants, vous devez exporter le certificat, puis l'ajouter au magasin de certificats Personnes autorisées sur le point de gestion distant.

Utilisez les procédures suivantes comme exemple pour configurer le certificat auto-signé sur le serveur de réplica de base de données d'un ordinateur Windows Server 2008 R2. Si vous disposez d'une version du système d'exploitation différente, consultez la documentation de votre version de système d'exploitation et adaptez les étapes des présentes procédures en fonction de vos besoins.

#### Pour configurer un certificat auto-signé pour le serveur de réplica de base de données

1. Sur le serveur de réplica de base de données, ouvrez une invite de commande PowerShell avec des privilèges d'administration, puis exécutez la commande suivante : **set-executionpolicy UnRestricted**
2. Copiez le script PowerShell suivant et enregistrez-le sous un fichier portant le nom **CreateMPReplicaCert.ps1**. Placez une copie de ce fichier dans le dossier racine de la partition système du serveur de réplica de base de données.

> **IMPORTANT**
> Si vous configurez plusieurs réplicas de base de données sur un serveur SQL Server unique, pour chaque nouveau réplica que vous configurez, vous devez utiliser une version modifiée de ce script pour cette procédure. Consultez Script complémentaire pour les réplicas de base de données supplémentaires sur un même serveur SQL Server.

```
# Script for creating a self-signed certificate for the local machine and configuring SQL Server to
use it.

Param($SQLInstance)

$ConfigMgrCertFriendlyName = "ConfigMgr SQL Server Identification Certificate"

# Get local computer name
$computerName = "$env:computername"

# Get the sql server name
#$key="HKLM:\SOFTWARE\Microsoft\SMS\MP"
#$value="SQL Server Name"
#$sqlServerName= (Get-ItemProperty $key).$value
#$dbValue="Database Name"
#$sqlInstance_DB_Name= (Get-ItemProperty $key).$dbValue

$sqlServerName = [System.Net.Dns]::GetHostByName("localhost").HostName
$sqlInstanceName = "MSSQLSERVER"
$SQLServiceName = "MSSQLSERVER"

if ($SQLInstance -ne $Null)
{
    $sqlInstanceName = $SQLInstance
    $SQLServiceName = "MSSQL$" + $SQLInstance
}

# Delete existing cert if one exists
function Get-Certificate($storename, $storelocation)
{
    $store=new-object
System.Security.Cryptography.X509Certificates.X509Store($storename,$storelocation)
    $store.Open([Security.Cryptography.X509Certificates.OpenFlags]::ReadWrite)
    $store.Certificates
```

```
    $store.Certificates
}

$cert = Get-Certificate "My" "LocalMachine" | ?{$_.FriendlyName -eq $ConfigMgrCertFriendlyName}
if($cert -is [Object])
{
    $store = new-object System.Security.Cryptography.X509Certificates.X509Store("My","LocalMachine")
    $store.Open([Security.Cryptography.X509Certificates.OpenFlags]::ReadWrite)
    $store.Remove($cert)
    $store.Close()

    # Remove this cert from Trusted People too...
    $store = new-object
System.Security.Cryptography.X509Certificates.X509Store("TrustedPeople","LocalMachine")
    $store.Open([Security.Cryptography.X509Certificates.OpenFlags]::ReadWrite)
    $store.Remove($cert)
    $store.Close()
}

# Create the new cert
$name = new-object -com "X509Enrollment.CX500DistinguishedName.1"
$name.Encode("CN=" + $sqlServerName, 0)

$key = new-object -com "X509Enrollment.CX509PrivateKey.1"
$key.ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
$key.KeySpec = 1
$key.Length = 1024
$key.SecurityDescriptor = "D:PAI(A;;0xd01f01ff;;;SY)(A;;0xd01f01ff;;;BA)(A;;0x80120089;;;NS)"
$key.MachineContext = 1
$key.Create()

$serverauthoid = new-object -com "X509Enrollment.CObjectId.1"
$serverauthoid.InitializeFromValue("1.3.6.1.5.5.7.3.1")
$ekuoids = new-object -com "X509Enrollment.CObjectIds.1"
$ekuoids.add($serverauthoid)
$ekuext = new-object -com "X509Enrollment.CX509ExtensionEnhancedKeyUsage.1"
$ekuext.InitializeEncode($ekuoids)

$cert = new-object -com "X509Enrollment.CX509CertificateRequestCertificate.1"
$cert.InitializeFromPrivateKey(2, $key, "")
$cert.Subject = $name
$cert.Issuer = $cert.Subject
$cert.NotBefore = get-date
$cert.NotAfter = $cert.NotBefore.AddDays(3650)
$cert.X509Extensions.Add($ekuext)
$cert.Encode()

$enrollment = new-object -com "X509Enrollment.CX509Enrollment.1"
$enrollment.InitializeFromRequest($cert)
$enrollment.CertificateFriendlyName = "ConfigMgr SQL Server Identification Certificate"
$certdata = $enrollment.CreateRequest(0x1)
$enrollment.InstallResponse(0x2, $certdata, 0x1, "")

# Add this cert to the trusted peoples store
[Byte[]]$bytes = [System.Convert]::FromBase64String($certdata)

$trustedPeople = new-object System.Security.Cryptography.X509certificates.X509Store "TrustedPeople",
"LocalMachine"
$trustedPeople.Open([Security.Cryptography.X509Certificates.OpenFlags]::ReadWrite)
$trustedPeople.Add([Security.Cryptography.X509Certificates.X509Certificate2]$bytes)
$trustedPeople.Close()

# Get thumbprint from cert
$sha = new-object System.Security.Cryptography.SHA1CryptoServiceProvider
$certHash = $sha.ComputeHash($bytes)
$certHashCharArray = "";
$certThumbprint = "";

# Format the bytes into a hexadecimal string
foreach($byte in $certHash)
```

```
foreach($byte in $certHash)
{
    $temp = ($byte | % {"{0:x}" -f $_}) -join ""
    $temp = ($temp | % {"{0,2}" -f $_})
    $certHashCharArray = $certHashCharArray+ $temp;
}
$certHashCharArray = $certHashCharArray.Replace(' ', '0');

# SQL needs the thumbprint in lower case
foreach($char in $certHashCharArray)
{
    [System.String]$myString = $char;
    $certThumbprint = $certThumbprint + $myString.ToLower();
}

# Configure SQL to use this cert
$path = "HKLM:\SOFTWARE\Microsoft\Microsoft SQL Server\Instance Names\SQL"
$subKey = (Get-ItemProperty $path).$sqlInstanceName
$realPath = "HKLM:\SOFTWARE\Microsoft\Microsoft SQL Server\" + $subKey +
"\MSSQLServer\SuperSocketNetLib"
$certKeyName = "Certificate"
Set-ItemProperty -path $realPath -name $certKeyName -Type string -Value $certThumbprint

# restart sql service
Restart-Service $SQLServiceName -Force
```

3. Sur le serveur de réplica de base de données, exécutez la commande suivante, s'appliquant à la configuration de votre serveur SQL Server :

   - Pour une instance par défaut de SQL Server : Cliquez avec le bouton droit sur le fichier **CreateMPReplicaCert.ps1** , puis sélectionnez **Exécuter avec PowerShell**. Lorsque le script s'exécute, celui-ci crée le certificat auto-signé et configure SQL Server pour utiliser le certificat.
   - Pour une instance nommée de SQL Server : Utilisez PowerShell pour exécuter la commande **%path%\CreateMPReplicaCert.ps1 xxxxxx** où **xxxxxx** est le nom de l'instance de SQL Server.
   - Une fois le script terminé, vérifiez que l'agent SQL Server est en cours d'exécution. Si ce n'est pas le cas, redémarrez SQL Server Agent.

#### Pour configurer des points de gestion à distance pour utiliser le certificat auto-signé du serveur de réplica de base de données

1. Sur le serveur réplica de base de données, effectuez les opérations suivantes pour exporter le certificat auto-signé du serveur :

   a. Cliquez sur **Démarrer**, cliquez sur **Exécuter**, puis tapez **mmc.exe**. Dans la console vide, cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.

   b. Dans la boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables** , sélectionnez **Certificats** dans la liste **Composants logiciels enfichables disponibles**, puis cliquez sur **Ajouter**.

   c. Dans la boîte de dialogue **Composant logiciel enfichable des certificats** , cliquez sur **Compte d'ordinateur**, puis sur **Suivant**.

   d. Dans la boîte de dialogue **Sélectionner un ordinateur** , vérifiez que **L'ordinateur local (l'ordinateur sur lequel cette console s'exécute)** est sélectionné, puis cliquez sur **Terminer**.

   e. Dans la boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables** , cliquez sur **OK**.

   f. Dans la console, développez **Certificats (ordinateur local)**, développez **Personnel**, puis sélectionnez **Certificats**.

g. Cliquez avec le bouton droit sur le certificat portant le nom convivial **certificat d'identification ConfigMgr SQL Server**, cliquez sur **Toutes les tâches**, puis sélectionnez **Exporter**.

h. Effectuez toutes les étapes de l' **Assistant Exportation de certificat** à l'aide des options par défaut et enregistrez le certificat avec l'extension de nom de fichier **.cer** .

2. Effectuez les opérations suivantes sur l'ordinateur du point de gestion pour ajouter le certificat auto-signé pour le serveur de réplica de base de données dans le magasin de certificats Personnes autorisées sur le point de gestion :

a. Répétez les étapes précédentes de 1.a à 1.e pour configurer le composant logiciel enfichable MMC **Certificat** sur l'ordinateur du point de gestion.

b. Dans la console, développez **Certificats (ordinateur local)** et **Personnes autorisées**, cliquez avec le bouton droit sur **Certificats**, sélectionnez **Toutes les tâches**, puis sélectionnez **Importer** pour lancer l' **Assistant Importation de certificat**.

c. Sur la page **Fichier à importer** , cliquez sur le certificat sauvegardé à l'étape 1.h, puis cliquez sur **Suivant**.

d. Sur la page **Magasin de certificats** , sélectionnez **Placer tous les certificats dans le magasin suivant**, lorsque le **Magasin de certificats** est paramétré sur **Personnes autorisées**, puis cliquez sur **Suivant**.

e. Cliquez sur **Terminer** pour fermer l'Assistant et terminer la configuration des certificats sur le point de gestion.

**Étape 5 : Configuration de Service Broker SQL Server pour le serveur réplica de base de données**

Pour prendre en charge la notification de client avec un réplica de base de données pour un point de gestion, vous devez configurer la communication entre le serveur de base de données de site et le serveur de réplica de base de données pour SQL Server Service Broker. Cela nécessite la configuration de chaque base de données avec des informations sur l'autre base de données et d'échanger les certificats entre les deux bases de données pour une communication sécurisée.

> **NOTE**
> Avant de pouvoir utiliser la procédure suivante, le serveur de réplica de la base de données doit réussir la synchronisation initiale avec le serveur de base de données de site.

La procédure suivante ne modifie pas le port Service Broker configuré dans SQL Server pour le serveur de base de données de site ou le serveur de réplica de la base de données. Au lieu de cela, cette procédure configure chaque base de données pour qu'elle communique avec l'autre base de données en utilisant le port Service Broker correct.

Exécutez la procédure suivante pour configurer le Service Broker pour le serveur de base de données de site et le serveur de réplica de la base de données.

**Pour configurer le Service Broker pour un réplica de base de données**

1. Utilisez **SQL Server Management Studio** pour vous connecter à la base de données du serveur réplica de base de données, puis exécutez la requête suivante pour activer Service Broker sur le serveur réplica de base de données : **ALTER DATABASE <nom du réplica de base de données> SET ENABLE_BROKER, HONOR_BROKER_PRIORITY ON WITH ROLLBACK IMMEDIATE**

2. Cliquez ensuite sur le serveur de réplica de la base de données, configurez le Service Broker pour la notification de client et exportez le certificat Service Broker. Pour cela, exécutez une procédure stockée SQL Server qui configure le Service Broker et exporte le certificat comme une seule action. Lorsque vous exécutez la procédure stockée, vous devez définir le nom de domaine complet du serveur de réplica

de la base de données, le nom de la base de données des réplicas de la base de données, ainsi qu'un emplacement pour l'exportation du fichier de certificat.

Exécutez la requête suivante pour configurer les informations nécessaires sur le serveur réplica de base de données et pour exporter le certificat pour le serveur réplica de base de données : **EXEC sp_BgbConfigSSBForReplicaDB '<nom_domaine_complet_réplica_SQL Server>', '<nom_base_de_données_réplica>', '<chemin_fichier_sauvegarde_certificat>'**

> **NOTE**
> Lorsque le serveur de réplica de base de données ne se trouve pas sur l'instance par défaut de SQL Server, dans cette étape, vous devez définir le nom de l'instance en plus du nom de la base de données réplica. Pour cela, remplacez **<nom_base_de_données_réplica>** par **<nom_instance\nom_base_de_données_réplica>**.

Une fois le certificat exporté depuis le serveur de réplica de base de données, placez une copie du certificat sur le serveur de base de données de sites principaux.

3. Utilisez **SQL Server Management Studio** pour vous connecter à la base de données du site principal. Après la connexion à la base de données des sites principaux, exécutez une requête pour importer le certificat et spécifiez le port Service Broker utilisé sur le serveur de réplica de base de données, le nom de domaine complet du serveur de réplica de base de données et le nom de la base de données de réplicas de base de données. Cela configure la base de données de sites principaux de sorte qu'elle utilise Service Broker pour communiquer avec la base de données du serveur de réplica de base de données.

   Exécutez la requête suivante pour importer le certificat à partir du serveur réplica de base de données et spécifier les informations nécessaires : **EXEC sp_BgbConfigSSBForRemoteService 'REPLICA', '<Port_SQL_Service_Broker>', '<chemin_fichier_certificat>', '<nom_domaine_complet_réplica_SQL Server>', '<nom_base_de_données_réplica>'**

   > **NOTE**
   > Lorsque le serveur de réplica de base de données ne se trouve pas sur l'instance par défaut de SQL Server, dans cette étape, vous devez définir le nom de l'instance en plus du nom de la base de données réplica. Pour cela, remplacez **<nom_base_de_données_réplica>** par **\nom_instance\nom_base_de_données_réplica>**.

4. Ensuite, sur le serveur de base de données du site, exécutez la commande suivante pour exporter le certificat du serveur de base de données du site : **EXEC sp_BgbCreateAndBackupSQLCert '<chemin_fichier_sauvegarde_certificat>'**

   Une fois le certificat exporté depuis le serveur de base de données de site, placez une copie du certificat sur le serveur de réplica de base de données.

5. Utilisez **SQL Server Management Studio** pour vous connecter à la base de données de serveur de réplica de base de données. Après la connexion à la base de données du serveur de réplica de base de données, exécutez une requête pour importer le certificat et spécifier le code de site du site principal et le port Service Broker utilisé sur le serveur de base de données de site. Cela configure le serveur de réplica de base de données de sorte qu'il utilise Service Broker pour communiquer avec la base de données du site principal.

   Exécutez la requête suivante pour importer le certificat à partir du serveur de base de données du site : **EXEC sp_BgbConfigSSBForRemoteService '<code_site>', '<Port_SQL_Service_Broker>', '<chemin_fichier_certificat>'**

   Après la configuration de la base de données de site et de la base de données de réplica de base de données, le gestionnaire de notification sur le site principal prend quelques minutes pour configurer la

conversation Service Broker pour la notification de client depuis la base de données du site principal vers le réplica de la base de données.

**Script complémentaire pour les réplicas de base de données supplémentaires sur un même serveur SQL Server**

Si vous utilisez le script de l'étape 4 pour configurer un certificat auto-signé pour le serveur réplica de base de données sur un serveur SQL Server comportant déjà un réplica de base de données que vous voulez continuer à utiliser, vous devez utiliser une version modifiée du script d'origine. Les modifications suivantes empêchent le script de supprimer un certificat existant sur le serveur, et créent les certificats suivants avec un nom convivial unique. Modifiez le script d'origine comme suit :

- Commentez (pour empêcher l'exécution) chaque ligne entre les entrées du script **# Delete existing cert if one exists** et **# Create the new cert**. Pour ce faire, ajoutez le signe **#** au tout début de chaque ligne concernée.
- Pour chaque réplica de base de données suivant que vous configurez à l'aide de ce script, mettez à jour le nom convivial du certificat. Pour cela, modifiez la ligne **$enrollment.CertificateFriendlyName = "ConfigMgr SQL Server Identification Certificate"** en remplaçant **ConfigMgr SQL Server Identification Certificate** par un nouveau nom, tel que **ConfigMgr SQL Server Identification Certificate1**.

## Gestion des configurations de réplica de base de données

Lorsque vous utilisez un réplica de base de données d'un site, utilisez les informations indiquées dans les sections suivantes pour compléter la procédure de désinstallation d'un réplica de base de données, désinstallation d'un site utilisant un réplica de base de données ou déplacement de la base de données de site vers une nouvelle installation de SQL Server. Lorsque vous utilisez les informations indiquées dans les sections suivantes pour supprimer des publications, suivez les instructions de suppression d'une réplication transactionnelle pour la version de SQL Server que vous utilisez pour le réplica de base de données. Par exemple, si vous utilisez SQL Server 2008 R2, consultez Procédure : supprimer une publication (programmation Transact-SQL de la réplication).

> **NOTE**
> Après avoir restauré une base de données de site configurée pour des réplicas de base de données et avant de pouvoir utiliser les réplicas de base de données, vous devez reconfigurer chaque réplica de base de données en recréant les publications et les abonnements.

**Désinstallation d'un réplica de base de données**

Lorsque vous utilisez un réplica de base de données pour un point de gestion, il peut être nécessaire de désinstaller le réplica de base de données pendant un certains temps, puis de le reconfigurer pour l'utiliser. Par exemple, vous devez supprimer les réplicas de base de données avant la mise à niveau d'un site Configuration Manager vers un nouveau Service Pack. Après la mise à niveau du site, vous pouvez restaurer le réplica de base de données pour l'utiliser.

Utilisez les étapes suivantes pour désinstaller un réplica de base de données.

1. Dans l'espace de travail **Administration** de la console Configuration Manager, développez **Configuration du site**, sélectionnez **Serveurs et rôles de système de site** puis, dans le volet d'informations, sélectionnez le serveur de système de site hébergeant le point de gestion qui utilise le réplica de base de données à désinstaller.
2. Dans le volet **Rôles système de site** , cliquez avec le bouton droit sur **Point de gestion** , puis sélectionnez **Propriétés**.

3. Sous l'onglet **Base de données du point de gestion** , sélectionnez **Utiliser la base de données du site** pour configurer le point de gestion de sorte qu'il utilise la base de données de site à la place du réplica de base de données. Cliquez ensuite sur **OK** pour enregistrer la configuration.

4. Ensuite, utilisez **SQL Server Management Studio** pour effectuer les tâches suivantes :

   - Supprimer la publication pour le réplica de base de données de la base de données du serveur de site.
   - Supprimer l'abonnement pour le réplica de base de données du serveur de réplica de base de données.
   - Supprimer la base de données réplica du serveur de réplica de base de données.
   - Désactiver la publication et la distribution sur le serveur de base de données de site. Pour désactiver la publication et la distribution, cliquez avec le bouton droit sur le dossier de réplication, puis cliquez sur **Désactiver la publication et la distribution**.

5. Après la suppression de la publication, de l'abonnement, de la base de données réplica et la désactivation de la publication sur le serveur de base de données de site, le réplica de base de données est désinstallé.

**Désinstallation d'un serveur de site qui publie un réplica de base de données**

Avant de désinstaller un site qui publie un réplica de la base de données, procédez comme suit pour nettoyer la publication ainsi que tous les abonnements.

1. Utilisez **SQL Server Management Studio** pour supprimer la publication du réplica de la base de donnée depuis la base de données du serveur de site.

2. Utilisez **SQL Server Management Studio** pour supprimer l'abonnement de réplica de base de données de chaque serveur SQL distant qui héberge un réplica de base de données pour ce site.

3. Désinstallez le site.

**Déplacement d'une base de données d'un serveur de site qui publie un réplica de base de données**

Lorsque vous déplacez la base de données de site vers un nouvel ordinateur, procédez comme suit :

1. Utilisez **SQL Server Management Studio** pour supprimer la publication du réplica de la base de donnée depuis la base de données du serveur de site.

2. Utilisez **SQL Server Management Studio** pour supprimer l'abonnement au réplica de la base de données de chaque serveur de réplica de base de données pour ce site.

3. Déplacez la base de données vers le nouvel ordinateur SQL Server. Pour plus d'informations, consultez la section Modifier la configuration de base de données de site dans la rubrique Modifier votre infrastructure System Center Configuration Manager .

4. Recréez la publication pour le réplica de la base de données sur le serveur de la base de données du site. Pour plus d'informations, consultez Étape 1 : Configuration du serveur de base de données du site pour publier le réplica de base de données dans cette rubrique.

5. Recréez les abonnements pour le réplica de la base de données sur chaque serveur de réplica de base de données. Pour plus d'informations, consultez Étape 2 : Configuration du serveur réplica de base de données dans cette rubrique.

# Composants de site pour System Center Configuration Manager

22/06/2018 • 12 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Sur chaque site System Center Configuration Manager, vous pouvez configurer des composants de site pour modifier le comportement des rôles système de site et la création des rapports d'état de site. Les configurations de composants de site s'appliquent à un site donné et à chaque instance d'un rôle de système de site applicable au niveau de ce site.

## À propos des composants de site

La plupart des options des différents composants de site sont suffisamment explicites quand elles apparaissent dans la console Configuration Manager. Toutefois, les informations suivantes peuvent être utiles pour mieux comprendre certaines configurations plus complexes ou vous diriger vers du contenu supplémentaire qui les explique.

**Distribution de logiciels**

- **Paramètres de distribution de contenu :** vous pouvez spécifier des paramètres qui modifient la façon dont le serveur de site transfère du contenu vers ses points de distribution. Si vous augmentez les valeurs des paramètres de distribution simultanée, la distribution de contenu risque d'utiliser davantage de bande passante réseau.

- **Compte d'accès réseau :** pour plus d'informations sur la configuration et l'utilisation du compte d'accès réseau, consultez Compte d'accès réseau.

**Point de mise à jour logicielle**

- Pour plus d'informations sur les options de configuration du composant de point de mise à jour logicielle, consultez Installer un point de mise à jour logicielle.

**Point de gestion**

- **Points de gestion :** vous pouvez configurer le site pour publier des informations sur ses points de gestion dans les services de domaine Active Directory.

  Les clients Configuration Manager utilisent des points de gestion pour localiser les services et pour rechercher des informations sur le site, telles que les options de sélection de certificats PKI et d'appartenance à des groupes de limites. Les clients utilisent également des points de gestion pour rechercher d'autres points de gestion du site, ainsi que des points de distribution d'où ils peuvent télécharger des logiciels. Les points de gestion aident également les clients à terminer l'attribution de site et à télécharger la stratégie client et leurs informations client.

  Comme la plus sûre des méthodes pour que les clients trouvent des points de gestion est de publier ceux-ci dans les services de domaines Active Directory, vous aurez généralement toujours besoin de sélectionner tous les points de gestion en fonctionnement pour publier dans les services de domaine Active Directory. Toutefois, pour pouvoir utiliser cette méthode de localisation de service, les éléments suivants doivent être vrais :

  - Le schéma est étendu pour Configuration Manager.
  - Il existe un conteneur **Gestion du système** disposant des autorisations de sécurité appropriées pour que le serveur de site puisse publier dans ce conteneur.

- Le site Configuration Manager est configuré pour publier dans les services de domaine Active Directory.
- Les clients appartiennent à la même forêt Active Directory que le serveur de site.

  Quand les clients sur l'intranet ne peuvent pas utiliser les services de domaine Active Directory pour rechercher des points de gestion, utilisez la publication DNS à la place.

Pour obtenir des informations générales sur l'emplacement du service, consultez Comprendre comment les clients recherchent des services et des ressources de site pour System Center Configuration Manager.

- **Publier les points de gestion intranet sélectionnés dans DNS :** spécifiez cette option quand des clients sur l'intranet ne trouvent pas de points de gestion à partir des services de domaine Active Directory. Au lieu de cela, ils peuvent utiliser un enregistrement de ressource d'emplacement de service DNS (SRV RR) pour trouver un point de gestion dans leur site attribué.

  Pour que Configuration Manager puisse publier des points de gestion intranet dans DNS, toutes les conditions suivantes doivent être remplies :

  - Vos serveurs DNS ont une version de BIND 8.1.2 ou ultérieure.
  - Vos serveurs DNS sont configurés pour les mises à jour automatiques et prennent en charge les enregistrements de ressource d'emplacement de service.
  - Les noms de domaine complets spécifiés pour les points de gestion dans Configuration Manager ont des entrées d'hôte (enregistrements A ou AAA) dans DNS.

  > **WARNING**
  > Pour que les clients trouvent des points de gestion publiés dans DNS, vous devez affecter les clients à un site spécifique (plutôt qu'utiliser l'attribution automatique de site). Configurez ces clients pour qu'ils utilisent le code de site avec le suffixe du domaine de leur point de gestion. Pour plus d'informations, consultez Localisation de points de gestion dans Guide pratique pour affecter des clients à un site dans System Center Configuration Manager.

  Si les clients Configuration Manager ne peuvent pas utiliser les services de domaine Active Directory ou DNS pour rechercher des points de gestion sur l'intranet, ils peuvent utiliser WINS. Le premier point de gestion installé pour le site est automatiquement publié dans WINS lorsqu'il est configuré pour accepter les connexions client HTTP sur l'intranet.

**édition de rapports d'état ;**

- Ces paramètres configurent directement le niveau de détail qui est fourni dans les rapports d'état à partir de sites et de clients.

**Notification par courrier électronique**

- Spécifiez les détails de compte ou de serveur de messagerie pour que Configuration Manager envoie des notifications par e-mail en cas d'alertes.

**Évaluation de l'appartenance au regroupement**

- Cette tâche permet de définir la fréquence à laquelle l'appartenance à un regroupement est évaluée de façon incrémentielle. L'évaluation incrémentielle met à jour une appartenance à un regroupement uniquement avec de nouvelles ressources ou des ressources modifiées.

**Modifier les composants de site sur un site**

Utilisez la procédure suivante pour modifier les composants de site :

1. Dans la console Configuration Manager, cliquez sur **Administration** > **Configuration du site** > **Sites**, puis sélectionnez le site comportant les composants de site que vous voulez configurer.

2. Sous l'onglet **Accueil**, dans le groupe **Paramètres**, cliquez sur **Configurer les composants de site**. Sélectionnez ensuite le composant de site que vous souhaitez configurer.

## Utiliser Configuration Manager Service Manager pour gérer les composants de site

Vous pouvez utiliser Configuration Manager Service Manager pour contrôler les services Configuration Manager et afficher l'état de tout service ou thread de travail Configuration Manager (collectivement appelés composants Configuration Manager). Retenez les points suivants concernant les composant Configuration Manager :

- Les composants peuvent s'exécuter sur n'importe quel système de site.
- Ils sont gérés de la même façon que les services dans Windows. Vous pouvez les démarrer, les arrêter, les suspendre, les reprendre et les interroger.

Un service Configuration Manager s'exécute dès qu'il a une tâche à effectuer (quand un fichier de configuration est enregistré dans la boîte de réception d'un composant, par exemple). Si vous devez identifier le composant impliqué dans une opération, vous pouvez utiliser Configuration Manager Service Manager pour agir sur plusieurs services et threads. Vous pouvez ensuite afficher les effets sur le comportement de Configuration Manager. Vous pouvez par exemple arrêter les services Configuration Manager un par un, jusqu'à ce qu'une réponse spécifique disparaisse. Vous pourrez ainsi déterminer le service qui provoque ce comportement.

> **TIP**
> La procédure suivante peut servir à manipuler des opérations de composants Configuration Manager.

**Utiliser le Gestionnaire de service de Configuration Manager**

1. Dans la console Configuration Manager, cliquez sur **Surveillance** > **État du système**, puis cliquez sur **État du composant**.
2. Sous l'onglet **Accueil**, dans le groupe **Composant**, cliquez sur **Démarrer**. Sélectionnez ensuite **Gestionnaire de service de Configuration Manager**.
3. Lorsque le Gestionnaire de service de Configuration Manager s'ouvre, connectez-vous au site que vous souhaitez gérer.

   Si vous ne voyez pas le site que vous souhaitez gérer, cliquez sur **Site**, puis sur **Connecter**, et entrez le nom du serveur de site du site correct.
4. Développez le site et accédez à **Composants** ou à **Serveurs**selon l'emplacement où se trouvent les composants que vous souhaitez gérer.
5. Dans le volet de droite, sélectionnez un ou plusieurs composants. Puis, dans le menu **Composant**, cliquez sur **Requête** pour mettre à jour l'état de votre sélection.
6. Après la mise à jour de l'état du composant, utilisez l'une des quatre actions en option dans le menu **Composant** pour modifier le fonctionnement du composant. Après avoir demandé une action, vous devez demander au composant d'afficher son nouvel état.
7. Fermez Configuration Manager Service Manager quand vous avez fini de modifier l'état opérationnel des composants.

# Publication de données de site pour System Center Configuration Manager

09/05/2018 • 5 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Après avoir développé le schéma Active Directory pour System Center Configuration Manager, vous pouvez publier des sites Configuration Manager sur Active Directory Domain Services (AD DS). Les ordinateurs Active Directory peuvent ainsi récupérer en toute sécurité des informations de site à partir d'une source approuvée. La publication des informations de site sur AD DS n'est pas obligatoire pour les fonctionnalités de base de Configuration Manager, mais elle peut réduire la surcharge administrative.

- **Quand un site est configuré pour publier dans AD DS**, les clients Configuration Manager peuvent trouver automatiquement des points de gestion par le biais de la publication Active Directory. Ils utilisent une requête LDAP à un serveur de catalogue global.
- **Quand un site ne publie pas dans AD DS**, les clients doivent utiliser une autre méthode pour rechercher leur point de gestion par défaut.

Pour plus d'informations sur la façon dont les clients trouvent un point de gestion, consultez Comprendre comment les clients recherchent des services et des ressources de site pour System Center Configuration Manager.

## Configuration des sites à publier dans AD DS

Les étapes principales sont les suivantes :

- Vous devez étendre le schéma Active Directory pour System Center Configuration Manager dans chaque forêt où vous allez publier des données de site. Vérifiez aussi que le conteneur **System Management** est présent.
- Vous devez accorder au compte d'ordinateur de chaque site principal devant publier des données le **contrôle total** sur le conteneur **System Management** et tous ses objets enfants.

**Pour autoriser un site Configuration Manager à publier des informations de site sur une forêt Active Directory**

1. Dans la console Configuration Manager, cliquez sur **Administration**.
2. Dans l'espace de travail **Administration** , développez **Configuration du site**, puis cliquez sur **Sites**. Sélectionnez le site dont vous souhaitez publier les données. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, cliquez sur **Propriétés**.
3. Sous l'onglet **Publication** des propriétés du site, sélectionnez les forêts sur lesquelles ce site devra publier les données de site.
4. Cliquez sur **OK** pour enregistrer la configuration.

**Pour configurer des forêts Active Directory pour la publication**

1. Dans la console Configuration Manager, cliquez sur **Administration**.
2. Dans l'espace de travail **Administration** , cliquez sur **Forêts Active Directory**. Si la découverte de forêts Active Directory a été exécutée précédemment, vous pouvez voir chaque forêt découverte dans le volet des résultats. La forêt locale et toutes les forêts approuvées sont découvertes lorsque la Découverte de forêts Active Directory s'exécute. Seules les forêts non approuvées doivent être ajoutées manuellement.

- Pour configurer une forêt qui a été découverte, sélectionnez la forêt dans le volet de résultats. Ensuite, sous l'onglet **Accueil**, dans le groupe **Propriétés**, cliquez sur **Propriétés** pour ouvrir les propriétés de la forêt. Passez à l'étape 3.
- Pour configurer une nouvelle forêt qui n'est pas répertoriée, sous l'onglet **Accueil**, dans le groupe **Créer**, cliquez sur **Ajouter une forêt** pour ouvrir la boîte de dialogue **Ajouter une forêt**. Passez à l'étape 3.

3. Sous l'onglet **Général**, remplissez les configurations pour la forêt que vous souhaitez découvrir et spécifiez le **Compte de forêt Active Directory**.

   > **NOTE**
   > La découverte de forêts Active Directory requiert un compte global pour découvrir et publier les forêts non approuvées. Si vous n'utilisez pas le compte d'ordinateur du serveur du site, vous pouvez uniquement sélectionner un compte global.

4. Si vous prévoyez d'autoriser des sites à publier des données de site pour cette forêt, dans l'onglet **Publication** , remplissez la configuration de la publication de cette forêt.

   > **NOTE**
   > Si vous autorisez les sites à publier sur une forêt, vous devez étendre le schéma Active Directory de cette forêt pour Configuration Manager. Le compte de forêt Active Directory doit avoir des autorisations Contrôle total sur le conteneur système dans cette forêt.

5. Lorsque vous terminez la configuration de cette forêt pour une utilisation avec la Découverte de forêts Active Directory, cliquez sur **OK** pour enregistrer la configuration.

# Gérer le contenu et l'infrastructure de contenu pour System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Quand vous êtes prêt à configurer et à gérer votre infrastructure de gestion de contenu pour System Center Configuration Manager, aidez-vous des informations dans les rubriques suivantes :

- Installer et configurer des points de distribution pour System Center Configuration Manager. Avant de déployer du contenu, vous devez installer et configurer des points de distribution. Vous pouvez ensuite configurer des groupes de points de distribution pour simplifier la gestion de contenu dans votre infrastructure. Les informations de cette rubrique peuvent vous aider à effectuer ces tâches, et détaillent les paramètres approfondis et variés pris en charge par les points de distribution individuels.
- Déployer et gérer du contenu pour System Center Configuration Manager. Le déploiement de contenu transfère des fichiers et logiciels aux serveurs de point de distribution sur le réseau. En plus du transfert proprement dit, vous pouvez préparer le contenu, ce qui permet d'éviter une utilisation excessive de la bande passante réseau. Les informations contenues dans cette rubrique peuvent vous aider à exécuter les tâches de base liées à l'envoi de ce contenu ou à l'utilisation efficace d'un contenu préparé.
- Surveiller le contenu que vous avez distribué avec System Center Configuration Manager. À mesure que vous déployez du contenu, vous pouvez analyser son état dans votre infrastructure. Vous pouvez également redistribuer du contenu qui n'atteint pas des points de distribution, ou annuler les distributions en cours. Les informations contenues dans cette rubrique vous aident à comprendre comment analyser votre contenu et comment résoudre certains problèmes en cas d'échec du transfert de contenu.

# Installer et configurer des points de distribution pour System Center Configuration Manager

22/06/2018 • 51 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Installez des points de distribution Configuration Manager pour héberger les fichiers de contenu que vous déployez sur des appareils et des utilisateurs. Créez des groupes de points de distribution pour simplifier la gestion des points de distribution, ainsi que la distribution du contenu aux points de distribution.

Lorsque vous *installez un nouveau point de distribution* (à l'aide de l'Assistant Installation) ou que vous *gérez les propriétés d'un point de distribution* (en les modifiant), vous pouvez configurer la plupart des paramètres du point de distribution. Certains paramètres ne sont disponibles que lorsque vous effectuez une installation ou une modification, mais pas les deux :

- Paramètres disponibles uniquement lors de l'installation d'un point distribution :
  - **Allow Configuration Manager to install IIS on the distribution point computer (Autoriser Configuration Manager à installer IIS sur l'ordinateur du point de distribution)**
  - **Configure drive space settings for the distribution point (Configurer les paramètres d'espace disque pour le point de distribution)**
- Paramètres disponibles seulement pendant lorsque vous modifiez les propriétés d'un point distribution :
  - **Manage distribution point group relationships (Gérer les relations d'un groupe de points de distribution)**
  - **View Content deployed to the distribution point (Afficher le contenu déployé sur le point de distribution)**
  - **Configure Rate limits for data transfers to distribution points (Configurer des limites de taux pour les transferts de données vers les points de distribution)**
  - **Configure Schedules for data transfers to distribution points (Configurer des planifications pour les transferts de données vers les points de distribution)**

## Installer un point de distribution

Désignez un serveur de système de site comme point de distribution pour rendre le contenu disponible pour les ordinateurs clients. Affectez un point de distribution à au moins un groupe de limites pour que les ordinateurs clients locaux puissent utiliser ce point de distribution comme emplacement source de contenu. Ajoutez le rôle de site de point de distribution à un nouveau serveur de système de site ou ajoutez le rôle de site à un serveur de système de site existant.

Quand vous installez un nouveau point de distribution, vous utilisez un Assistant d'installation qui vous guide à travers les paramètres disponibles. Avant de commencer, tenez compte des prérequis suivants :

- Pour créer et configurer un point de distribution, vous devez disposer des autorisations de sécurité suivantes :
  - **Lecture** pour l'objet **Point de distribution**
  - **Copier vers le point de distribution** pour l'objet **Point de distribution**

- **Modifier** pour l'objet **Site**
- **Gérer des certificats pour le déploiement de système d'exploitation** pour l'objet **Site**

- Installez IIS (Internet Information Services) sur le serveur qui héberge le point de distribution. Quand vous installez le rôle de système de site, Configuration Manager peut installer et configurer IIS automatiquement.

Utilisez les procédures de base suivantes pour installer ou modifier un point de distribution. Pour plus d'informations sur les options de configuration disponibles, consultez la section Configurer un point de distribution de cette rubrique.

#### Pour installer un point de distribution

1. Dans la console Configuration Manager, choisissez **Administration** > **Configuration du site** > **Serveurs et rôles de système de site**.
2. Ajoutez le rôle de système de site de point de distribution à un serveur de système de site nouveau ou existant :
   - **Nouveau serveur de système de site** : dans l'onglet **Accueil** puis dans le groupe **Créer**, choisissez **Créer un serveur de système de site**. L'Assistant Création de serveur de système de site s'ouvre.
   - **Serveur de système de site existant** : choisissez le serveur sur lequel vous souhaitez installer le rôle de système de site du point de distribution. Lorsque vous choisissez un serveur, la liste des rôles de système de site déjà installés sur le serveur s'affiche dans le panneau des résultats.

     Dans l'onglet **Accueil** puis dans le groupe **Serveur**, choisissez **Ajouter des rôles de système de site**. L'Assistant Ajout de rôles de système de site s'ouvre.
3. Sur la page **Général** , spécifiez les paramètres généraux du serveur de système de site. Lorsque vous ajoutez le point de distribution à un serveur de système de site existant, vérifiez les valeurs qui ont été précédemment configurées.
4. Dans la page **Sélection du rôle système**, choisissez **Point de distribution** dans la liste des rôles disponibles, puis choisissez **Suivant**.
5. Pour les pages suivantes de l'Assistant, consultez les informations fournies dans la section Configurer un point de distribution.

   Par exemple, si vous souhaitez installer le point de distribution en tant que point de distribution d'extraction, choisissez **Activer ce point de distribution pour extraire le contenu à partir d'autres points de distribution**, puis procédez aux configurations supplémentaires requises par les points de distribution d'extraction.
6. Après avoir fermé l'Assistant, le rôle de site du point de distribution est ajouté au serveur de système de site.

#### Pour modifier un point de distribution

1. Dans la console Configuration Manager, choisissez **Administration** > **Points de distribution**, puis sélectionnez le point de distribution à configurer.
2. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
3. Utilisez les informations de la section Configurer un point de distribution pour modifier les propriétés du point de distribution.
4. Après avoir apporté les modifications souhaitées, enregistrez vos paramètres et fermez la page des propriétés.

# Gérer les groupes de points de distribution

Les groupes de points de distribution fournissent un regroupement logique de points de distribution pour la distribution de contenu. Vous pouvez utiliser ces groupes pour gérer et surveiller de manière centralisée le contenu des points de distribution qui s'étendent sur plusieurs sites. Gardez à l'esprit les points suivants :

- Vous pouvez ajouter un ou plusieurs points de distribution à partir de n'importe quel site de la hiérarchie, dans un groupe de points de distribution.
- Vous pouvez ajouter un point de distribution à plusieurs groupes de points de distribution.
- Lorsque vous diffusez du contenu à un groupe de points de distribution, Configuration Manager le distribue à tous les points de distribution membres de ce groupe.
- Si vous ajoutez un point de distribution au groupe de points de distribution après une distribution de contenu initiale, Configuration Manager distribue automatiquement le contenu au nouveau membre du groupe.
- Vous pouvez associer un regroupement à un groupe de points de distribution. Lorsque vous distribuez du contenu à ce regroupement, Configuration Manager identifie les groupes de points de distribution associés au regroupement. Le contenu est ensuite distribué à tous les points de distribution qui sont membres de ces groupes de points de distribution.

  > **NOTE**
  > Si, après avoir distribué du contenu à un regroupement, vous associez ce regroupement à un nouveau groupe de points de distribution, vous devez redistribuer le contenu au regroupement pour pouvoir distribuer le contenu au nouveau groupe.

**Pour créer et configurer un nouveau groupe de points de distribution**

1. Dans la console Configuration Manager, choisissez **Administration** > **Groupes de points de distribution**.
2. Dans l'onglet **Accueil** puis dans le groupe **Créer**, choisissez **Créer un groupe**.
3. Entrez le nom et la description du groupe de points de distribution.
4. Dans l'onglet **Regroupements**, cliquez sur **Ajouter**, sélectionnez les regroupements à associer au groupe de points de distribution, puis choisissez **OK**.
5. Dans l'onglet **Membres**, choisissez **Ajouter**, sélectionnez les points de distribution à ajouter comme membres du groupe de points de distribution, puis choisissez **OK**.
6. Choisissez **OK** pour créer le groupe de points de distribution.

**Pour ajouter des points de distribution et associer des regroupements à un groupe de points de distribution**

1. Dans la console Configuration Manager, choisissez **Administration** > **Groupes de points de distribution**.
2. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
3. Dans l'onglet **Regroupements**, choisissez **Ajouter** pour sélectionner les regroupements à associer au groupe de points de distribution, puis choisissez **OK**.
4. Dans l'onglet **Membres**, choisissez **Ajouter** pour sélectionner les points de distribution à ajouter comme membres du groupe de points de distribution, puis choisissez **OK**.
5. Choisissez **OK** pour enregistrer les modifications apportées au groupe de points de distribution.

#### Pour ajouter les points de distribution sélectionnés à un nouveau groupe de points de distribution

1. Dans la console Configuration Manager, choisissez **Administration** > **Points de distribution**, puis sélectionnez les points de distribution à ajouter au nouveau groupe de points de distribution.
2. Dans l'onglet **Accueil** puis dans le groupe **Point de distribution**, développez **Ajouter les éléments sélectionnés**, puis choisissez **Ajouter les éléments sélectionnés au nouveau groupe de points de distribution**.
3. Entrez le nom et la description du groupe de points de distribution.
4. Dans l'onglet **Regroupements**, choisissez **Ajouter** pour sélectionner les regroupements à associer au groupe de points de distribution, puis choisissez **OK**.
5. Sous l'onglet **Membres**, confirmez votre souhait de voir Configuration Manager ajouter les points de distribution répertoriés en tant que membres du groupe de points de distribution. Choisissez **Ajouter** pour ajouter les points de distribution, puis choisissez **OK**.
6. Choisissez **OK** pour créer le groupe de points de distribution.

#### Pour ajouter les points de distribution sélectionnés à des groupes de points de distribution existants

1. Dans la console Configuration Manager, choisissez **Administration** > **Points de distribution**, puis sélectionnez les points de distribution à ajouter au nouveau groupe de points de distribution.
2. Dans l'onglet **Accueil** puis dans le groupe **Point de distribution**, développez **Ajouter les éléments sélectionnés**, puis choisissez **Ajouter les éléments sélectionnés aux groupes de points de distribution existants**.
3. Dans **Groupes de points de distribution disponibles**, sélectionnez les groupes de points de distribution auxquels les points de distribution sélectionnés doivent être ajoutés en tant que membres, puis choisissez **OK**.

## Réaffecter un point de distribution

De nombreux clients ont de grandes infrastructures Configuration Manager et réduisent le nombre de sites principaux ou secondaires pour simplifier leur environnement. Ils doivent néanmoins toujours conserver des points de distribution aux emplacements des filiales pour délivrer du contenu aux clients gérés. Ces points de distribution contiennent souvent plusieurs téraoctets ou plus de contenus. Ce contenu est coûteux en termes de temps et de bande passante réseau pour le distribuer à ces serveurs distants.

Depuis la version 1802, cette fonctionnalité vous permet de réaffecter un point de distribution à un autre site principal sans redistribuer le contenu. Cette action met à jour l'affectation du système de site tout en conservant la totalité du contenu sur le serveur. Si vous devez réaffecter plusieurs points de distribution, effectuez d'abord cette action sur un seul point de distribution, puis poursuivez avec les serveurs supplémentaires, un par un.

> **IMPORTANT**
> Le serveur cible peut seulement héberger le rôle de point de distribution. Si le serveur de système de site héberge un autre rôle serveur Configuration Manager, comme le point de migration d'état, vous ne pouvez pas réaffecter le point de distribution. Vous ne pouvez pas réaffecter un point de distribution cloud.

Avant de réaffecter un point de distribution, ajoutez le compte d'ordinateur du serveur de site de destination au groupe Administrateur local sur le serveur de point de distribution cible.

Effectuez les étapes suivantes pour réaffecter un point de distribution :

1. Dans la console Configuration Manager, connectez-vous au site d'administration centrale.
2. Accédez à l'espace de travail **Administration**, puis sélectionnez le nœud **Points de distribution**.

3. Cliquez avec le bouton droit sur le point de distribution cible, puis sélectionnez **Réaffecter le point de distribution**.
4. Sélectionnez le serveur de site cible auquel vous voulez réaffecter ce point de distribution ainsi que le code de site.

Surveillez la réaffectation de la même façon que quand vous ajoutez un nouveau rôle. La méthode la plus simple consiste à actualiser l'affichage de la console après quelques minutes. Ajoutez la colonne de code de site à l'affichage. Cette valeur change quand Configuration Manager réaffecte le serveur. Si vous essayez d'effectuer une autre action sur le serveur cible avant d'actualiser l'affichage de la console, une erreur « objet introuvable » se produit. Vérifiez que le processus est terminé et actualisez l'affichage de la console avant de démarrer d'autres actions sur le serveur.

Après la réaffectation d'un point de distribution, actualisez le certificat du serveur. Le nouveau serveur de site doit chiffrer à nouveau ce certificat à l'aide de sa clé publique et le stocker dans la base de données de site. Pour plus d'informations, consultez le paramètre **Créez un certificat auto-signé ou importez un certificat client d'infrastructure à clé publique (PKI) pour le point de distribution** sous l'onglet Général des propriétés du point de distribution.

- Pour les certificats d'infrastructure à clé publique, vous n'avez pas besoin de créer un certificat. Importez le même fichier .PFX et entrez le mot de passe.
- Pour les certificats auto-signés, réglez la date ou l'heure d'expiration pour la mettre à jour. Si vous n'actualisez pas le certificat, le point de distribution délivre toujours le contenu, mais les fonctions suivantes échouent :
  - Messages de validation du contenu (le fichier distmgr.log indique qu'il ne peut pas déchiffrer le certificat)
  - Prise en charge PXE pour les clients

**Conseils**

- Effectuez cette action à partir du site d'administration centrale. Cette pratique facilite la réplication vers les sites principaux.
- Ne distribuez pas de contenu vers le serveur cible pour tenter ensuite de le réaffecter. Les tâches de distribution de contenu en cours risquent d'échouer pendant le processus de réaffectation, mais elles sont retentées comme d'habitude.
- Si le serveur est également un client Configuration Manager, veillez à réaffecter également le client au nouveau site principal. Cette étape est particulièrement importante pour les points de distribution d'extraction, qui utilisent des composants clients pour télécharger du contenu.
- Ce processus supprime le point de distribution du groupe de limites par défaut de l'ancien site. Vous devez l'ajouter manuellement au groupe de limites par défaut du nouveau site, si nécessaire. Toutes les autres affectations de groupes de limites restent les mêmes.

# Configurer un point de distribution

Chaque point de distribution prend en charge plusieurs configurations différentes. Toutefois, tous les types de point de distribution ne prennent pas en charge toutes les configurations. Par exemple, les points de distribution cloud ne prennent pas en charge les déploiements de contenu activés pour PXE ou la multidiffusion. Les rubriques suivantes contiennent des informations sur certaines limitations :

- Utiliser un point de distribution cloud avec System Center Configuration Manager
- Utiliser un point de distribution d'extraction avec System Center Configuration Manager

Les sections suivantes décrivent les configurations que vous pouvez sélectionner pendant l'installation d'un nouveau point de distribution ou la modification des propriétés d'un point de distribution.

**Général**

Configurez les paramètres généraux des points de distribution :

- **Installer et configurer IIS si requis par Configuration Manager** : sélectionnez ce paramètre pour permettre à Configuration Manager d'installer et de configurer IIS sur le serveur si IIS n'est pas déjà installé. Les services Internet doivent être installés sur tous les points de distribution. Si IIS n'est pas installé sur le serveur et si vous ne sélectionnez pas ce paramètre, vous devez installer IIS pour pouvoir installer le point de distribution.

  > **NOTE**
  > Cette option n'est disponible que lorsque vous installez un nouveau point de distribution.

- **Activer et configurer BranchCache pour ce point de distribution** : sélectionnez ce paramètre pour permettre à Configuration Manager de configurer Windows BranchCache sur le serveur de point de distribution. Pour plus d'informations sur l'utilisation de Windows BranchCache avec System Center Configuration Manager, consultez BranchCache dans *Prise en charge des fonctionnalités de Windows et des réseaux dans System Center Configuration Manager*.

- **Configure how client devices communicate with the distribution point (Configurer comment les appareils clients communiquent avec le point de distribution)** : l'utilisation de HTTP et de HTTPS présente des avantages et des inconvénients. Pour plus d'informations, consultez Meilleures pratiques de sécurité pour la gestion de contenu dans Principes de base de la gestion de contenu dans System Center Configuration Manager.

- **Autoriser les clients à se connecter anonymement** : ce paramètre indique si le point de distribution autorise les connexions anonymes des clients Configuration Manager à la bibliothèque de contenu.

  > **IMPORTANT**
  > La réparation d'une application Windows Installer sur un client peut échouer si vous n'utilisez pas ce paramètre.
  >
  > Lorsque vous déployez une application Windows Installer sur un client Configuration Manager, Configuration Manager télécharge le fichier dans le cache local du client. Les fichiers sont supprimés, une fois l'installation terminée.
  >
  > Le client Configuration Manager met à jour la liste source Windows Installer des applications Windows Installer installées avec le chemin de contenu de la bibliothèque de contenu sur les points de distribution associés. Par la suite, si vous démarrez l'action de réparation via Ajout/Suppression de programmes sur un client Configuration Manager, MSIExec tente d'accéder au chemin de contenu avec un compte d'utilisateur anonyme.
  >
  > Vous pouvez toutefois changer ce comportement en installant la mise à jour décrite dans l'article 2619572 de la Base de connaissances Microsoft, puis en modifiant une clé de Registre.
  >
  > Une fois la mise à jour installée sur les clients, MSIExec accède au chemin du contenu en utilisant le compte d'utilisateur connecté, lorsque vous ne choisissez pas le paramètre **Autoriser les clients à se connecter anonymement**.

- **Create a self-signed certificate or import a public key infrastructure (PKI) client certificate for the distribution point (Créer un certificat auto-signé ou importer un certificat client d'infrastructure à clé publique (PKI) pour le point de distribution)** : le certificat remplit les fonctions suivantes :

  - Il authentifie le point de distribution à un point de gestion avant que le point de distribution n'envoie des messages d'état.

  - Lorsque vous activez la case à cocher **Activer la prise en charge PXE pour les clients** sur la page **Paramètres PXE**, le certificat est envoyé aux ordinateurs qui redémarrent PXE pour pouvoir se

connecter à un point de gestion pendant le déploiement du système d'exploitation.

Lorsque tous vos points de gestion du site sont configurés pour le protocole HTTP, créez un certificat auto-signé. Lorsque vos points de gestion sont configurés pour le protocole HTTPS, importez un certificat client PKI.

Pour importer le certificat, accédez à un fichier PKCS #12 (Public Key Cryptography Standard #12) qui contient un certificat PKI avec les spécifications suivantes pour Configuration Manager :

- L'utilisation prévue doit inclure l'authentification du client.
- La clé privée doit être activée pour l'exportation.

> **TIP**
> Il n'existe aucune exigence particulière pour l'objet du certificat ou le nom alternatif d'objet du certificat (SAN), et vous pouvez utiliser le même certificat pour plusieurs points de distribution.

Pour plus d'informations sur la configuration requise pour les certificats, consultez Configuration requise des certificats PKI pour System Center Configuration Manager.

Pour obtenir un exemple de déploiement de ce certificat, consultez la section Déployer le certificat client pour les points de distribution de la rubrique Exemple de déploiement pas à pas des certificats PKI pour System Center Configuration Manager : autorité de certification Windows Server 2008.

- **Activer ce point de distribution pour le contenu préparé** : choisissez ce paramètre pour activer le point de distribution du contenu préparé. Lorsque ce paramètre est sélectionné, vous pouvez configurer le comportement de distribution lors de la distribution du contenu. Vous pouvez choisir de toujours effectuer l'une des actions suivantes :
  - Préparer le contenu sur le point de distribution.
  - Préparer le contenu initial du package, puis utiliser le processus de distribution de contenu standard lorsque le contenu fait l'objet de mises à jour.
  - Utiliser le processus de distribution standard pour le contenu du package.

**Paramètres du lecteur**

> **NOTE**
> Ces options ne sont disponibles que lorsque vous installez un nouveau point de distribution.

Spécifiez les paramètres du lecteur pour le point de distribution. Vous pouvez configurer jusqu'à deux lecteurs de disque pour la bibliothèque de contenu et deux lecteurs de disque pour le partage de package. Configuration Manager peut utiliser des lecteurs supplémentaires lorsque les deux premiers atteignent la réserve d'espace disque configurée. La page **Paramètres du lecteur** permet de configurer la priorité des lecteurs de disque et la quantité d'espace disque libre restant sur chaque lecteur de disque.

- **Réserve d'espace libre sur le lecteur (Mo)** : la valeur que vous configurez pour ce paramètre détermine la quantité d'espace libre sur un lecteur avant que Configuration Manager choisisse un autre lecteur et poursuive le processus de copie sur ce lecteur. Les fichiers de contenu peuvent s'étendre sur plusieurs lecteurs.

- **Emplacements du contenu**: Spécifiez les emplacements de contenu pour le partage de bibliothèque et de package de contenu. Configuration Manager copie le contenu à l'emplacement de contenu principal jusqu'à ce que la quantité d'espace libre atteigne la valeur spécifiée dans **Réserve d'espace libre sur le lecteur (Mo)**. Par défaut, les emplacements du contenu sont définis sur **Automatique**. L'emplacement de

contenu principal est défini sur le lecteur de disque disposant le plus d'espace lors de l'installation. L'emplacement secondaire, quant à lui, est attribué au deuxième lecteur de disque disposant le plus d'espace. Quand le lecteur principal et le lecteur secondaire atteignent la réserve d'espace libre sur le lecteur, Configuration Manager sélectionne un autre lecteur disponible ayant le plus d'espace disque libre et poursuit le processus de copie.

> **NOTE**
>
> Pour empêcher l'installation de Configuration Manager sur un lecteur spécifique, créez un fichier vide intitulé **no_sms_on_drive.sms** et copiez-le dans le dossier racine du lecteur avant d'installer le point de distribution.

**Point de distribution d'extraction**

Quand vous choisissez **Activer ce point de distribution pour extraire le contenu à partir d'autres points de distribution**, vous modifiez la méthode employée par l'ordinateur pour obtenir le contenu que vous distribuez au point de distribution. Ce point de distribution devient un point de distribution d'extraction.

Pour chaque point de distribution d'extraction que vous configurez, vous devez spécifier un ou plusieurs points de distribution sources à partir desquels le point de distribution d'extraction obtient le contenu :

- Choisissez **Ajouter**, puis sélectionnez un ou plusieurs des points de distribution disponibles comme points de distribution sources.
- Choisissez **Supprimer** pour supprimer le point de distribution sélectionné comme point de distribution source.
- Utilisez les boutons fléchés pour définir l'ordre dans lequel le point de distribution d'extraction contacte les points de distribution sources lorsqu'il tente de transférer du contenu. Les points de distribution associés à la valeur la plus faible sont contactés en premier.

**Environnement PXE**

Indiquez si vous souhaitez activer l'environnement PXE sur le point de distribution. Quand vous activez l'environnement PXE, Configuration Manager installe les services de déploiement Windows (WDS) sur le serveur, si nécessaire. WDS est le service qui démarre PXE pour installer les systèmes d'exploitation. Après avoir effectué toutes les étapes de l'Assistant pour créer le point de distribution, Configuration Manager installe dans WDS un fournisseur qui utilise les fonctions de démarrage PXE.

Lorsque vous choisissez **Activer la prise en charge PXE pour les clients**, configurez les paramètres suivants :

> **NOTE**
>
> Cliquez sur **Oui** dans la boîte de dialogue **Consulter les ports requis pour PXE** pour confirmer que vous souhaitez activer PXE. Configuration Manager configure automatiquement les ports par défaut dans le Pare-feu Windows. Vous devez configurer manuellement les ports si vous utilisez un autre pare-feu.
>
> Si WDS et DHCP sont installés sur le même serveur, vous devez configurer WDS pour écouter sur un port différent. Par défaut, DHCP écoute sur le même port. Pour plus d'informations, consultez Considérations quand vous avez WDS et DHCP sur le même serveur.

- **Autoriser ce point de distribution à répondre aux requêtes PXE entrantes** : indiquez si WDS doit être activé pour répondre aux demandes de service PXE. Utilisez cette case à cocher pour activer et désactiver le service sans supprimer la fonctionnalité PXE du point de distribution.
- **Activer la prise en charge d'ordinateur inconnu** : indiquez si la prise en charge des ordinateurs non gérés par Configuration Manager doit être activée.
- **Exiger un mot de passe lorsque les ordinateurs utilisent PXE**: pour renforcer la sécurité de vos

déploiements PXE, spécifiez un mot de passe fort.

- **Affinité entre appareil et utilisateur**: indiquez de quelle manière le point de distribution doit associer les utilisateurs à l'ordinateur de destination dans le cadre des déploiements PXE. Choisissez l'une des options suivantes :

  - **Autoriser une affinité entre périphérique et utilisateur avec approbation automatique** : choisissez ce paramètre pour associer automatiquement les utilisateurs à l'ordinateur de destination sans attendre l'approbation.

  - **Autoriser une affinité entre périphérique et utilisateur en attente de l'approbation de l'administrateur** : choisissez ce paramètre pour attendre l'approbation d'un utilisateur administratif avant d'associer des utilisateurs à l'ordinateur de destination.

  - **Ne pas autoriser d'affinité entre périphérique et utilisateur** : choisissez ce paramètre pour empêcher l'association d'utilisateurs à l'ordinateur de destination.

    Pour plus d'informations sur l'affinité entre utilisateur et appareil, consultez Lier des utilisateurs et des appareils avec l'affinité entre utilisateur et appareil dans System Center Configuration Manager.

- **Interfaces réseau**: Spécifiez que le point de distribution répond aux requêtes PXE à partir de toutes les interfaces réseau ou d'interfaces réseau spécifiques. Si le point de distribution répond à des interfaces réseau spécifiques, vous devez fournir l'adresse MAC pour chaque interface réseau.

- **Spécifier le délai de réponse du serveur PXE (secondes)** : indiquez, en secondes, le délai d'attente à l'issue duquel le point de distribution répond aux requêtes de l'ordinateur lorsque plusieurs points de distribution PXE sont utilisés. Par défaut, le point de service PXE de Configuration Manager répond d'abord aux demandes PXE du réseau.

> **NOTE**
>
> Le protocole PXE permet de démarrer les déploiements de système d'exploitation sur les ordinateurs clients Configuration Manager. Configuration Manager utilise le rôle de site du point de distribution PXE pour lancer le processus de déploiement du système d'exploitation. Le point de distribution PXE doit être configuré pour :
>
> 1. Répondre aux demandes de démarrage PXE émanant des clients Configuration Manager sur le réseau.
> 2. Interagir avec l'infrastructure Configuration Manager pour déterminer les actions de déploiement appropriées à entreprendre.

**Multidiffusion**

Indiquez si vous souhaitez activer la multidiffusion sur le point de distribution. Quand vous activez la multidiffusion, Configuration Manager installe les services de déploiement Windows (WDS) sur le serveur, si nécessaire.

Quand vous cochez la case **Activer la multidiffusion pour envoyer simultanément des données à plusieurs clients**, configurez les paramètres suivants :

- **Compte de connexion multidiffusion** : indiquez le compte à utiliser quand vous configurez des connexions de base de données Configuration Manager pour la multidiffusion.

- **Paramètres de l'adresse de multidiffusion** : spécifiez les adresses IP pour envoyer des données vers les ordinateurs de destination. Par défaut; l'adresse IP est fournie par un serveur DCHP chargé de distribuer des adresses de multidiffusion. Selon l'environnement réseau, vous pouvez spécifier une plage d'adresses IP entre 239.0.0.0 et 239.255.255.255.

> **IMPORTANT**
> Les adresses IP que vous configurez doivent être accessibles par les ordinateurs de destination qui demandent l'image du système d'exploitation. Vérifiez que les routeurs et pare-feu autorisent le trafic de multidiffusion entre l'ordinateur de destination et le serveur de site.

- **Étendue du port UDP pour la multidiffusion** : spécifiez la plage de ports UDP (User Datagram Protocol) utilisés pour envoyer des données aux ordinateurs de destination.

  > **IMPORTANT**
  > Les ports UDP doivent être accessibles par les ordinateurs de destination qui demandent l'image du système d'exploitation. Vérifiez que les routeurs et pare-feu autorisent le trafic de multidiffusion entre l'ordinateur de destination et le serveur de site.

- **Taux de transfert client**: Sélectionnez la vitesse de transfert utilisée pour télécharger des données sur les ordinateurs de destination.
- **Nombre maximum de clients**: Spécifiez le nombre maximal d'ordinateurs de destination qui peuvent télécharger le système d'exploitation à partir de ce point de distribution.
- **Activer la multidiffusion planifiée** : indiquez comment Configuration Manager contrôle le lancement du déploiement des systèmes d'exploitation sur les ordinateurs de destination. Configurez les options suivantes :
  - **Délai de démarrage de session (en minutes)** : indiquez le nombre de minutes écoulé avant que Configuration Manager réponde à la première demande de déploiement.
  - **Taille minimale de la session (clients)** : indiquez le nombre de demandes qui doivent être reçues avant que Configuration Manager commence à déployer le système d'exploitation.

> **NOTE**
> Les déploiements de multidiffusion économisent la bande passante réseau en envoyant de manière simultanée des données à plusieurs clients Configuration Manager au lieu d'envoyer une copie des données à chaque client via une connexion distincte. Pour plus d'informations sur l'utilisation de la multidiffusion pour le déploiement de systèmes d'exploitation, consultez Utiliser la multidiffusion pour Windows sur le réseau avec System Center Configuration Manager.

**Relations de groupe**

> **NOTE**
> Ces options ne sont disponibles que quand vous modifiez les propriétés d'un point de distribution déjà installé.

Gérez les groupes de points de distribution dont ce point de distribution est membre.

Pour ajouter ce point de distribution en tant que membre à un groupe de points de distribution, choisissez **Ajouter**. Sélectionnez un groupe de points de distribution dans la liste de la boîte de dialogue **Ajouter aux groupes de points de distribution**, puis choisissez **OK**.

Pour supprimer ce point de distribution d'un groupe de points de distribution, sélectionnez le groupe dans la liste, puis choisissez **Supprimer**.

**Content**

> **NOTE**
> Ces options ne sont disponibles que quand vous modifiez les propriétés d'un point de distribution déjà installé.

Gérez le contenu qui a été distribué au point de distribution. La section **Packages de déploiement** fournit la liste des packages distribués à ce point de distribution. Vous pouvez sélectionner un package dans la liste, puis effectuer les actions suivantes :

- **Valider**: Démarre le processus de validation de l'intégrité des fichiers de contenu dans le package. Pour afficher les résultats du processus de validation du contenu, dans l'espace de travail **Surveillance**, développez **État de distribution**, puis choisissez le nœud **État du contenu**.
- **Redistribuer**: Copie tous les fichiers de contenu dans le package vers le point de distribution et remplace les fichiers existants. Vous utilisez généralement cette opération pour réparer les fichiers de contenu dans le package.
- **Supprimer**: Supprime les fichiers de contenu du point de distribution du package.

**Validation du contenu**

Indiquez si vous souhaitez définir une planification pour valider l'intégrité des fichiers de contenu sur le point de distribution. Quand vous activez la validation de contenu selon une planification, Configuration Manager démarre le processus à l'heure planifiée, et tout le contenu est vérifié sur le point de distribution. Vous pouvez également configurer la priorité de la validation du contenu. Par défaut, la priorité est définie sur **La plus faible**.

Pour afficher les résultats du processus de validation du contenu, dans l'espace de travail **Surveillance**, développez **État de distribution**, puis choisissez le nœud **État du contenu**. Le contenu de chaque type de package (par exemple, application, package de mises à jour logicielles et image de démarrage) s'affiche.

> **WARNING**
> Même si vous planifiez la validation du contenu en utilisant l'heure locale de l'ordinateur, la planification affichée dans la console Configuration Manager est exprimée en heure UTC.

**Groupes de limites**

Gérez les groupes de limites pour lesquels ce point de distribution est attribué. Prévoyez d'ajouter le point de distribution à au moins un groupe de limites. Au cours du déploiement de contenu, les clients doivent se trouver dans un groupe de limites associé à un point de distribution pour utiliser ce dernier comme emplacement source de contenu.

Configurez des *relations* qui définissent à quel moment et auprès de quels groupes de limites un client peut effectuer une action de secours pour trouver du contenu. Pour plus d'informations, consultez Groupes de limites.

**Planification**

> **NOTE**
> Ces options ne sont disponibles que quand vous modifiez les propriétés d'un point de distribution déjà installé.

> **TIP**
> Cet onglet n'est disponible que lorsque vous modifiez les propriétés d'un point de distribution distant de l'ordinateur du serveur de site.

Indiquez s'il convient de configurer une planification qui limite la période de transfert de données de

Configuration Manager vers le point de distribution.

> **IMPORTANT**
> La planification est basée sur le fuseau horaire du site émetteur, et non sur celui du point de distribution.

Pour restreindre les données, sélectionnez la période, puis choisissez l'un des paramètres suivants sous **Disponibilité** :

- **Ouvrir pour toutes les priorités** : indique que Configuration Manager envoie les données au point de distribution sans restriction.
- **Autoriser les priorités moyennes et élevées** : indique que Configuration Manager n'envoie au point de distribution que les données de priorité moyenne et élevée.
- **Autoriser uniquement la priorité élevée** : indique que Configuration Manager n'envoie au point de distribution que les données de priorité élevée.
- **Fermé** : indique que Configuration Manager n'envoie pas de données au point de distribution.

Vous pouvez limiter les données par priorité ou fermer la connexion durant des périodes sélectionnées.

**Limites du taux de transfert**

> **NOTE**
> Ces options ne sont disponibles que quand vous modifiez les propriétés d'un point de distribution déjà installé.

> **TIP**
> Cet onglet n'est disponible que lorsque vous modifiez les propriétés d'un point de distribution distant de l'ordinateur du serveur de site.

Spécifiez si vous souhaitez configurer des limites du taux de transfert pour contrôler la bande passante réseau utilisée lorsque Configuration Manager transfère du contenu vers le point de distribution. Vous pouvez choisir parmi les options suivantes :

- **Illimité lors de l'expédition de données à cette destination** : cette option spécifie que Configuration Manager envoie le contenu au point de distribution sans aucune limite de taux de transfert.
- **Mode impulsion** : cette option spécifie la taille des blocs de données qui sont envoyés au point de distribution. Vous pouvez également spécifier un délai entre l'envoi de chaque bloc de données. Utilisez cette option lorsque vous devez envoyer des données au point de distribution via une connexion réseau à très faible bande passante. Par exemple, vous pouvez forcer l'envoi de 1 Ko de données toutes les cinq secondes, quelle que soit la vitesse de la liaison ou son utilisation.
- **Limité aux taux de transfert maximaux indiqués par heure**: spécifiez ce paramètre pour qu'un site envoie des données à un point de distribution en utilisant uniquement le pourcentage de temps que vous avez configuré. Quand vous utilisez cette option, Configuration Manager n'identifie pas la bande passante disponible du réseau, mais divise le temps pendant lequel il peut envoyer des données. Puis les données sont envoyées pendant une courte plage horaire, suivie de plages horaires pendant lesquelles aucune donnée n'est envoyée. Par exemple, si le taux maximal est fixé à **50 %**, Configuration Manager transmet les données sur une période, qui est suivie d'une période égale où aucune donnée n'est envoyée. La taille effective des donnés ou la taille des blocs de données ne sont pas gérées. En revanche, seule la durée pendant laquelle des données sont envoyées est gérée.

# Déployer et gérer du contenu pour System Center Configuration Manager

22/06/2018 • 53 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Après avoir installé des points de distribution pour System Center Configuration Manager, vous pouvez commencer à y déployer du contenu. En règle générale, le contenu est transféré aux points de distribution via le réseau, mais il existe d'autres options pour placer du contenu aux points de distribution. Une fois le contenu transféré vers un point de distribution, vous pouvez mettre à jour, redistribuer, supprimer et valider ce contenu sur les points de distribution.

## Distribuer du contenu

En règle générale, vous distribuez du contenu sur des points de distribution pour le rendre accessible aux ordinateurs clients. (Ceci ne s'applique pas si vous utilisez la distribution de contenu à la demande pour un déploiement spécifique.) Quand vous distribuez du contenu, Configuration Manager stocke les fichiers de contenu dans un package, puis distribue ce package sur le point de distribution. Les types de contenu que vous pouvez distribuer incluent les suivants :

- Types de déploiement d'application
- Packages
- Packages de déploiement
- Packages de pilotes
- Images du système d'exploitation
- Programmes d'installation de système d'exploitation
- Images de démarrage
- Séquences de tâches

Quand vous créez un package qui contient des fichiers sources, tels qu'un type de déploiement d'application ou un package de déploiement, le site sur lequel le package est créé devient le site propriétaire de la source de contenu du package. Configuration Manager copie les fichiers sources à partir du chemin de fichier source spécifié pour l'objet vers la bibliothèque de contenu située sur le serveur de site propriétaire de la source de contenu du package. Ensuite, Configuration Manager réplique les informations vers les sites supplémentaires. (Pour plus d'informations à ce sujet, consultez Bibliothèque de contenu.)

Pour distribuer du contenu vers les points de distribution, procédez comme suit.

#### Pour distribuer du contenu vers les points de distribution

1. Dans la console Configuration Manager, cliquez sur **Bibliothèque de logiciels**.
2. Dans l'espace de travail **Bibliothèque de logiciels** , sélectionnez l'une des étapes suivantes pour le type de contenu que vous souhaitez distribuer :
   - **Applications** : Développez **Gestion d'applications** > **Applications**, puis sélectionnez les applications à distribuer.

- **Packages** : Développez **Gestion d'applications** > **Packages**, puis sélectionnez les packages à distribuer.
- **Packages de déploiement** : Développez **Mises à jour logicielles** > **Packages de déploiement**, puis sélectionnez les packages de déploiement à distribuer.
- **Packages de pilotes** : Développez **Systèmes d'exploitation** > **Packages de pilotes**, puis sélectionnez les packages de pilotes à distribuer.
- **Images de système d'exploitation** : Développez **Systèmes d'exploitation** > **Images du système d'exploitation**, puis sélectionnez les images de système d'exploitation à distribuer.
- **Programmes de système d'exploitation** : Développez **Systèmes d'exploitation** > **Programmes d'installation de système d'exploitation**, puis sélectionnez les programmes d'installation de système d'exploitation à distribuer.
- **Images de démarrage** : Développez **Systèmes d'exploitation** > **Images de démarrage**, puis sélectionnez les images de démarrage à distribuer.
- **Séquences de tâches** : Développez **Systèmes d'exploitation** > **Séquences de tâches**, puis sélectionnez la séquence de tâches à distribuer. Les séquences de tâches ne contiennent pas de contenu, mais elles comportent des dépendances de contenu associées qui sont distribuées.

  > **NOTE**
  > Si vous modifiez la séquence de tâches, vous devez redistribuer le contenu.

3. Dans l'onglet **Accueil** , dans le groupe **Déploiement** , cliquez sur **Distribuer du contenu**. L'Assistant Distribuer du contenu s'ouvre.
4. Sur la page **Général**, vérifiez que le contenu affiché correspond bien au contenu que vous voulez distribuer, indiquez si vous voulez que Configuration Manager détecte les dépendances de contenu associées au contenu sélectionné et ajoutez les dépendances à la distribution avant de cliquer sur **Suivant**.

   > **NOTE**
   > Vous pouvez configurer le paramètre **Détecter les dépendances de contenu associées et les ajouter à cette distribution** pour le type de contenu d'application uniquement. Configuration Manager configure automatiquement ce paramètre pour les séquences de tâches et il ne peut pas être modifié.

5. Dans l'onglet **Contenu** , s'il s'affiche, vérifiez que le contenu répertorié correspond au contenu que vous voulez distribuer, puis cliquez sur **Suivant**.

   > **NOTE**
   > La page **Contenu** s'affiche uniquement lorsque le paramètre **Détecter les dépendances de contenu associées et les ajouter à cette distribution** est sélectionné sur la page **Général** de l'Assistant.

6. Sur la page **Destination du contenu** , cliquez sur **Ajouter**, choisissez l'une des opérations suivantes, puis suivez l'étape associée :
   - **Regroupements**: sélectionnez **Regroupements d'utilisateurs** ou **Regroupements d'appareils**, cliquez sur le regroupement associé à un ou plusieurs groupes de points de distribution, puis sur **OK**.

> **NOTE**
> Seuls les regroupements qui sont associés à un groupe de points de distribution sont affichés. Pour plus d'informations sur l'association des regroupements et des groupes de points de distribution, consultez Gérer les groupes de points de distribution dans la rubrique Installer et configurer des points de distribution pour System Center Configuration Manager.

- **Point de distribution**: sélectionnez un point de distribution existant, puis cliquez sur **OK**. Les points de distribution ayant précédemment reçu le contenu ne sont pas affichés.
- **Groupe de points de distribution**: sélectionnez un groupe de points de distribution existant, puis cliquez sur **OK**. Les groupes de points de distribution ayant précédemment reçu le contenu ne sont pas affichés.

Lorsque vous avez terminé d'ajouter des destinations de contenu, cliquez sur **Suivant**.

7. Sur la page **Résumé** , vérifiez les paramètres de la distribution avant de continuer. Pour distribuer le contenu vers les destinations sélectionnées, cliquez sur **Suivant**.
8. La page **Progression** affiche la progression de la distribution.
9. La page **Confirmation** affiche si le contenu a été bien attribué avec succès aux points de distribution. Pour surveiller la distribution de contenu, consultez Surveiller le contenu que vous avez distribué avec System Center Configuration Manager.

## Utiliser le contenu préparé

Vous pouvez préparer des fichiers de contenu pour les applications et les types de packages :

- Dans la console Configuration Manager, vous sélectionnez le contenu dont vous avez besoin, puis utilisez l'**Assistant Création du fichier de contenu préparé** pour créer un fichier de contenu préparé compressé qui contient les fichiers et les métadonnées associées pour le contenu que vous avez sélectionné.
- Vous pouvez ensuite importer manuellement le contenu au niveau d'un serveur de site, d'un site secondaire ou d'un point de distribution.
- Lorsque vous importez le fichier de contenu préparé sur un serveur de site, les fichiers de contenu sont ajoutés à la bibliothèque de contenu sur le serveur de site, puis enregistrés dans la base de données du serveur de site.
- Lorsque vous importez le fichier de contenu préparé sur un point de distribution, les fichiers de contenu sont ajoutés à la bibliothèque de contenu sur le point de distribution, et un message d'état est envoyé au serveur de site qui informe le site que le contenu est disponible sur le point de distribution.

**Limitations et éléments à prendre en compte pour le contenu préparé :**

- **Si le point de distribution est situé sur le serveur de site**, n'activez pas le point de distribution pour le contenu préparé. Au lieu de cela, procédez comme indiqué dans Guide pratique pour préparer du contenu sur un point de distribution situé sur un serveur de site.
- **Si le point de distribution est configuré en tant que point de distribution d'extraction**, n'activez pas le point de distribution pour le contenu préparé. La configuration de contenu préparé pour un point de distribution se substitue à la configuration du point de distribution d'extraction. Un point de distribution d'extraction configuré pour du contenu préparé n'extrait pas de contenu auprès d'un point de distribution source et ne reçoit pas de contenu du serveur de site.
- **Vous devez créer la bibliothèque de contenu sur le point de distribution avant de préparer le**

**contenu pour ce point de distribution**. Distribuez le contenu sur le réseau au moins une fois avant de préparer le contenu vers le point de distribution.

- **Lorsque vous préparez du contenu pour un package dont le chemin source est particulièrement long** (plus de 140 caractères, par exemple), l'outil en ligne de commande d'extraction de contenu risque de ne pas réussir à extraire le contenu de ce package vers la bibliothèque de contenu.

Pour plus d'informations sur le moment propice à la préparation des fichiers de contenu, consultez *Contenu préparé* dans la rubrique Gérer la bande passante du réseau pour la gestion de contenu.

Utilisez les sections suivantes pour préparer du contenu.

**Étape 1 : Créer un fichier de contenu préparé**

Vous pouvez créer un fichier de contenu préparé et compressé qui contient les fichiers et les métadonnées associées pour le contenu que vous sélectionnez dans la console Configuration Manager. Pour créer un fichier de contenu préparé, procédez comme suit.

Pour créer un fichier de contenu préparé

1. Dans la console Configuration Manager, cliquez sur **Bibliothèque de logiciels**.
2. Dans l'espace de travail **Bibliothèque de logiciels** , sélectionnez l'une des étapes suivantes pour le type de contenu que vous souhaitez préparer :
   - **Applications**: développez **Gestion d'applications**, cliquez sur **Applications**, puis sélectionnez les applications que vous souhaitez préparer.
   - **Packages**: développez **Gestion d'applications**, cliquez sur **Packages**, puis sélectionnez les packages que vous souhaitez préparer.
   - **Packages de pilotes**: développez **Systèmes d'exploitation**, cliquez sur **Packages de pilotes**, puis sélectionnez les packages de pilotes que vous souhaitez préparer.
   - **Images du système d'exploitation**: développez **Systèmes d'exploitation**, cliquez sur **Images du système d'exploitation**, puis sélectionnez les images du système d'exploitation que vous souhaitez préparer.
   - **Programmes d'installation de système d'exploitation**: développez **Systèmes d'exploitation**, cliquez sur **Programmes d'installation de système d'exploitation**, puis sélectionnez les programmes d'installation de système d'exploitation que vous souhaitez préparer.
   - **Images de démarrage**: développez **Systèmes d'exploitation**, cliquez sur **Images de démarrage**, puis sélectionnez les images de démarrage que vous souhaitez préparer.
   - **Séquences de tâches**: Développez **Systèmes d'exploitation**, cliquez sur **Séquences de tâches**, puis sélectionnez les séquences de tâches que vous souhaitez préparer.
3. Dans l'onglet **Accueil** , dans le groupe **Déploiement** , cliquez sur **Créer un fichier de contenu préparé**. L'Assistant Création du fichier de contenu préparé s'ouvre.

   > **NOTE**
   >
   > **Pour les applications :** Sous l'onglet **Accueil**, dans le groupe **Application**, cliquez sur **Créer un fichier de contenu préparé**.
   >
   > **Pour les packages :** Sous l'onglet **Accueil**, dans le groupe <*nom_package*>, cliquez sur **Créer un fichier de contenu préparé**.

4. Sur la page **Général** , cliquez sur **Parcourir**, choisissez l'emplacement pour le fichier de contenu préparé, spécifiez un nom pour le fichier, puis cliquez sur **Enregistrer**. Vous utilisez ce fichier de contenu préparé sur

des serveurs de site principaux, des serveurs de site secondaires ou des points de distribution afin d'importer le contenu et les métadonnées.

5. Pour les applications, sélectionnez **Exporter toutes les dépendances** afin que Configuration Manager détecte et ajoute les dépendances associées à l'application au fichier de contenu préparé. Ce paramètre est activé par défaut.

6. Dans **Commentaires de l'administrateur**, saisissez des commentaires facultatifs concernant le fichier de contenu préparé, puis cliquez sur **Suivant**.

7. Sur la page **Contenu** , vérifiez que le contenu répertorié correspond au contenu que vous souhaitez ajouter au fichier de contenu préparé, puis cliquez sur **Suivant**.

8. Sur la page **Emplacements du contenu** , spécifiez les points de distribution à partir desquels vous souhaitez récupérer les fichiers de contenu pour le fichier de contenu préparé. Vous pouvez sélectionner plusieurs points de distribution pour récupérer le contenu. Les points de distribution sont répertoriés dans la section Emplacements du contenu. La colonne **Contenu** affiche le nombre de packages ou applications sélectionnés disponibles sur chaque point de distribution. Configuration Manager commence par le premier point de distribution de la liste pour récupérer le contenu sélectionné, puis descend dans la liste afin de récupérer le contenu restant requis pour le fichier de contenu préparé. Cliquez sur **Monter** ou **Descendre** pour modifier l'ordre de priorité des points de distribution. Si les points de distribution de la liste ne contiennent pas tout le contenu sélectionné, vous devez ajouter des points de distribution à la liste contenant le contenu ou fermer l'Assistant, distribuer le contenu à un point de distribution au moins, puis redémarrer l'Assistant.

9. Sur la page **Résumé** , vérifiez les détails. Vous pouvez revenir aux pages précédentes et apporter des modifications. Cliquez sur **Suivant** pour créer le fichier de contenu préparé.

10. La page **Progression** affiche le contenu qui est ajouté au fichier de contenu préparé.

11. Sur la page **Dernière étape** , vérifiez que le fichier de contenu préparé a été créé correctement, puis cliquez sur **Fermer**.

### Étape 2 : Affecter le contenu aux points de distribution

Après avoir préparé le fichier de contenu, attribuez le contenu aux points de distribution.

> **NOTE**
> Si vous utilisez un fichier de contenu préparé pour récupérer la bibliothèque de contenu sur un serveur de site et n'êtes pas obligé de préparer les fichiers de contenu sur un point de distribution, vous pouvez ignorer cette procédure.

Pour affecter le contenu du fichier de contenu préparé aux points de distribution, procédez comme suit.

> **IMPORTANT**
> Vérifiez que les points de distribution que vous souhaitez préparer sont configurés comme des points de distribution préparés ou que le contenu est distribué aux points de distribution via le réseau.

#### Pour affecter le contenu aux points de distribution

1. Dans la console Configuration Manager, cliquez sur **Bibliothèque de logiciels**.

2. Dans l'espace de travail **Bibliothèque de logiciels** , sélectionnez l'une des étapes suivantes pour le type de contenu que vous avez sélectionné lorsque vous avez créé le fichier de contenu préparé :

   - **Applications**: développez **Gestion d'applications**, cliquez sur **Applications**, puis sélectionnez les applications que vous avez préparées.

- **Packages**: développez **Gestion d'applications**, cliquez sur **Packages**, puis sélectionnez les Packages que vous avez préparés.
- **Packages de déploiement**: développez **Mises à jour logicielles**, cliquez sur **Packages de déploiement**, puis sélectionnez les packages de déploiement que vous avez préparés.
- **Packages de pilotes**: développez **Systèmes d'exploitation**, cliquez sur **Packages de pilotes**, puis sélectionnez les packages de pilotes que vous avez préparés.
- **Images du système d'exploitation**: développez **Systèmes d'exploitation**, cliquez sur **Images du système d'exploitation**, puis sélectionnez les images du système d'exploitation que vous avez préparées.
- **Programmes d'installation de système d'exploitation**: développez **Systèmes d'exploitation**, cliquez sur **Programmes d'installation de système d'exploitation**, puis sélectionnez les programmes d'installation de système d'exploitation que vous avez préparés.
- **Images de démarrage**: développez **Systèmes d'exploitation**, cliquez sur **Images de démarrage**, puis sélectionnez les images de démarrage que vous avez préparées.

3. Dans l'onglet **Accueil** , dans le groupe **Déploiement** , cliquez sur **Distribuer du contenu**. L'Assistant Distribuer du contenu s'ouvre.
4. Sur la page **Général** , vérifiez que le contenu affiché correspond bien au contenu que vous avez préparé, indiquez si vous voulez que Configuration Manager détecte les dépendances de contenu associées au contenu sélectionné et ajoutez les dépendances à la distribution avant de cliquer sur **Suivant**.

   > **NOTE**
   > Vous pouvez configurer le paramètre **Détecter les dépendances de contenu associées et les ajouter à cette distribution** pour le type de contenu d'application uniquement. Configuration Manager configure automatiquement ce paramètre pour les séquences de tâches et il ne peut pas être modifié.

5. Sur la page **Contenu** , si elle s'affiche, vérifiez que le contenu répertorié correspond au contenu que vous voulez distribuer, puis cliquez sur **Suivant**.

   > **NOTE**
   > La page **Contenu** s'affiche uniquement lorsque le paramètre **Détecter les dépendances de contenu associées et les ajouter à cette distribution** est sélectionné sur la page **Général** de l'Assistant.

6. Sur la page **Destination du contenu** , cliquez sur **Ajouter**, choisissez l'une des opérations suivantes qui inclut les points de distribution à préinstaller, puis suivez l'étape associée :

   - **Regroupements**: sélectionnez **Regroupements d'utilisateurs** ou **Regroupements d'appareils**, cliquez sur le regroupement associé à un ou plusieurs groupes de points de distribution, puis sur **OK**.

     > **NOTE**
     > Seuls les regroupements qui sont associés à un groupe de points de distribution sont affichés. Pour plus d'informations, consultez Gérer les groupes de points de distribution dans la rubrique Installer et configurer des points de distribution pour System Center Configuration Manager.

   - **Point de distribution**: sélectionnez un point de distribution existant, puis cliquez sur **OK**. Les points de distribution ayant précédemment reçu le contenu ne sont pas affichés.

- **Groupe de points de distribution**: sélectionnez un groupe de points de distribution existant, puis cliquez sur **OK**. Les groupes de points de distribution ayant précédemment reçu le contenu ne sont pas affichés.

Lorsque vous avez terminé d'ajouter des destinations de contenu, cliquez sur **Suivant**.

7. Sur la page **Résumé** , vérifiez les paramètres de la distribution avant de continuer. Pour distribuer le contenu vers les destinations sélectionnées, cliquez sur **Suivant**.
8. La page **Progression** affiche la progression de la distribution.
9. La page **Confirmation** affiche si le contenu a été bien attribué avec succès aux points de distribution. Pour surveiller la distribution de contenu, consultez Surveiller le contenu que vous avez distribué avec System Center Configuration Manager.

**Étape 3 : Extraire le contenu du fichier de contenu préparé**

Une fois que vous avez créé le fichier de contenu préparé et que vous avez attribué le contenu aux points de distribution, vous pouvez extraire les fichiers de contenu vers la bibliothèque de contenu d'un serveur de site ou d'un point de distribution. Généralement, vous avez copié le fichier de contenu préparé vers un lecteur portable, tel qu'un lecteur USB, ou gravé le contenu sur un support, tel qu'un DVD, puis vous l'avez mis à disposition à l'emplacement du serveur de site ou du point de distribution qui demande le contenu.

Pour exporter manuellement les fichiers de contenu à partir du fichier de contenu préparé à l'aide de l'outil de ligne de commande Extraire le contenu, procédez comme suit.

> **IMPORTANT**
> Lorsque vous exécutez l'outil d'extraction de contenu en ligne de commande, l'outil crée un fichier temporaire lors de la création du fichier de contenu préparé. Le fichier est ensuite copié dans le dossier de destination, puis supprimé. Vous devez disposer de suffisamment d'espace disque pour stocker ce fichier temporaire. Sinon, le processus échoue. Le fichier temporaire est créé à l'emplacement suivant :
>
> - Le fichier temporaire est créé dans le même dossier que celui spécifié comme dossier de destination du fichier de contenu préparé.

> **IMPORTANT**
> L'utilisateur qui exécute l'outil en ligne de commande d'extraction de contenu doit disposer de droits d'**administrateur** sur l'ordinateur à partir duquel vous extrayez le contenu préparé.

**Pour extraire les fichiers de contenu du fichier de contenu préparé**

1. Copiez le fichier de contenu préparé à l'ordinateur à partir duquel vous souhaitez extraire le contenu.
2. Copiez l'outil en ligne de commande d'extraction de contenu depuis *<chemin_installation_Configuration_Manager>*\bin*<plateforme>* sur l'ordinateur à partir duquel vous souhaitez extraire le fichier de contenu préparé.
3. Ouvrez l'invite de commandes et accédez à l'emplacement du dossier du fichier de contenu préparé et l'outil Extraire le contenu.

   > **NOTE**
   > Vous pouvez extraire un ou plusieurs fichiers de contenu préparé sur un serveur de site, un serveur de site secondaire ou un point de distribution.

4. Tapez **extractcontent /P:***<emplacement_fichier_préparé>******<nom_fichier_préparé>* **/S** pour importer un

seul fichier.

Tapez **extractcontent /P:**<*emplacement_fichier_préparé*> **/S** pour importer tous les fichiers préparés dans le dossier spécifié.

Par exemple, tapez **extractcontent /P:D:\PrestagedFiles\MyPrestagedFile.pkgx /S** où `D:\PrestagedFiles\` est l'emplacement du fichier préparé, `MyPrestagedFile.pkgx` est le nom du fichier préparé et `/S` informe Configuration Manager d'extraire uniquement les fichiers de contenu qui sont plus récents que ce qui se trouve actuellement sur le point de distribution.

Lorsque vous extrayez le fichier de contenu préparé sur un serveur de site, les fichiers de contenu sont ajoutés à la bibliothèque de contenu sur le serveur de site, puis la disponibilité du contenu est enregistrée dans la base de données du serveur de site. Lorsque vous exportez le fichier de contenu préparé sur un point de distribution, les fichiers de contenu sont ajoutés à la bibliothèque de contenu sur le point de distribution, ce dernier envoie un message d'état au serveur de site principal parent, puis la disponibilité du contenu est enregistrée dans la base de données du site.

> **IMPORTANT**
> Dans le scénario suivant, vous devez mettre à jour le contenu que vous avez extrait à partir d'un fichier de contenu préparé lorsque le contenu est mis à jour vers une nouvelle version :
>
> 1. Vous créez un fichier de contenu préparé pour la version 1 d'un package.
> 2. Vous mettez à jour les fichiers sources pour le package avec la version 2.
> 3. Vous extrayez le fichier de contenu préparé (version 1 du package) sur un point de distribution.
>
> Configuration Manager ne distribue pas automatiquement le package version 2 vers le point de distribution. Vous devez créer un nouveau fichier de contenu préparé contenant la nouvelle version du fichier, puis extraire le contenu, mettre à jour le point de distribution pour distribuer les fichiers qui ont été modifiés ou redistribuer tous les fichiers du package.

**Guide pratique pour préparer du contenu sur un point de distribution situé sur un serveur de site**

Lorsqu'un point de distribution est installé sur un serveur de site, vous devez suivre la procédure suivante pour préparer correctement le contenu. Cela est dû au fait que les fichiers de contenu se trouvent déjà dans la bibliothèque de contenu.

Lorsqu'un point de distribution n'est pas activé pour préparer le contenu ou lorsque le point de distribution ne se trouve pas sur un serveur de site, consultez la section Utilisation de contenu préparé dans cette rubrique.

###### Pour préparer du contenu sur des points de distribution situés sur un serveur de site

1. Utilisez les étapes suivantes pour vérifier que le point de distribution n'est pas activé pour le contenu préparé.
   a. Dans la console Configuration Manager, cliquez sur **Administration**.
   b. Dans l'espace de travail **Administration** , cliquez sur **Points de distribution**et sélectionnez le point de distribution situé sur le serveur de site.
   c. Dans l'onglet **Accueil** , dans le groupe **Propriétés** , cliquez sur **Propriétés**.
   d. Dans l'onglet **Général** , vérifiez que la case **Activer ce point de distribution pour le contenu préparé** est décochée.
2. Créez le fichier de contenu préparé en suivant la section Étape 1 : Créer un fichier de contenu préparé dans cette rubrique.
3. Affectez le contenu au point de distribution en suivant la section Étape 2 : Affecter le contenu aux points de distribution dans cette rubrique.

4. Sur le serveur de site, extrayez le contenu du fichier de contenu préparé en suivant la section Étape 3 : Extraire le contenu du fichier de contenu préparé dans cette rubrique.

> **NOTE**
> Lorsque le point de distribution est situé sur un site secondaire, patientez au moins 10 minutes, puis utilisez une console Configuration Manager connectée au site principal parent pour affecter le contenu au point de distribution sur le site secondaire.

## Gérer le contenu que vous avez distribué

Vous disposez des options suivantes pour gérer le contenu :

- Mettre à jour le contenu
- Redistribuer le contenu
- Supprimer le contenu
- Valider le contenu

### Mettre à jour le contenu

Si l'emplacement du fichier source d'un déploiement est mis à jour par l'ajout de nouveaux fichiers ou le remplacement de fichiers existants par d'autres plus récents, vous pouvez mettre à jour les fichiers de contenu sur les points de distribution à l'aide de l'action **Mettre à jour les points de distribution** ou **Mettre à jour le contenu** :

- Les fichiers de contenu sont copiés du chemin source vers la bibliothèque de contenu sur le site propriétaire de la source du contenu du package.
- La version du package est incrémentée.
- Chaque instance de la bibliothèque de contenu sur les serveurs de site et sur les points de distribution est mise à jour uniquement avec les fichiers qui ont été modifiés.

> **WARNING**
> La version du package pour les applications est toujours 1. Quand vous mettez à jour le contenu pour un type de déploiement d'application, Configuration Manager crée un ID de contenu pour le type de déploiement, et le package fait référence à ce nouvel ID de contenu.

#### Pour mettre à jour du contenu sur les points de distribution

1. Dans la console Configuration Manager, cliquez sur **Bibliothèque de logiciels**.
2. Dans l'espace de travail **Bibliothèque de logiciels** , sélectionnez l'une des étapes suivantes pour le type de contenu que vous souhaitez distribuer :
   - **Applications** : Développez **Gestion d'applications** > **Applications**, puis sélectionnez les applications à distribuer. Cliquez sur l'onglet **Types de déploiement** , puis sélectionnez le type de déploiement à mettre à jour.
   - **Packages** : Développez **Gestion d'applications** > **Packages**, puis sélectionnez les packages à mettre à jour.
   - **Packages de déploiement** : Développez **Mises à jour logicielles** > **Packages de déploiement**, puis sélectionnez les packages de déploiement à mettre à jour.
   - **Packages de pilotes** : Développez **Systèmes d'exploitation** > **Packages de pilotes**, puis sélectionnez les packages de pilotes à mettre à jour.

- **Images de système d'exploitation** : Développez **Systèmes d'exploitation** > **Images du système d'exploitation**, puis sélectionnez les images de système d'exploitation à mettre à jour.
- **Programmes de système d'exploitation** : Développez **Systèmes d'exploitation** > **Programmes d'installation de système d'exploitation**, puis sélectionnez les programmes d'installation de système d'exploitation à mettre à jour.
- **Images de démarrage** : Développez **Systèmes d'exploitation** > **Images de démarrage**, puis sélectionnez les images de démarrage à mettre à jour.

3. Dans l'onglet **Accueil** , cliquez sur le groupe **Déploiement** , cliquez sur **Mettre à jour les points de distribution**, puis cliquez sur **OK** pour confirmer la mise à jour du contenu.

> **NOTE**
> Pour mettre à jour le contenu pour les applications, cliquez sur l'onglet **Types de déploiement** , cliquez avec le bouton droit sur le type de déploiement, cliquez sur **Mettre à jour le contenu**, puis cliquez sur **OK** pour confirmer l'actualisation du contenu.

> **NOTE**
> Lorsque vous mettez à jour du contenu pour les images de démarrage, l'Assistant Gestion des points de distribution s'ouvre. Vérifiez les informations sur la **Résumé** , puis effectuez toutes les étapes de l'Assistant pour mettre à jour le contenu.

**Redistribuer le contenu**

Vous pouvez redistribuer un package pour copier tous les fichiers de contenu dans le package vers des points de distribution ou des groupes de points de distribution, et remplacer les fichiers existants.

Utilisez cette option pour réparer les fichiers de contenu dans le package ou pour renvoyer le contenu après un échec de la distribution initiale. Vous pouvez redistribuer un package à partir des propriétés suivantes :

- Propriétés du package
- Propriétés du point de distribution
- Propriétés du groupe de points de distribution

**Pour redistribuer du contenu à partir des propriétés de package**

1. Dans la console Configuration Manager, cliquez sur **Bibliothèque de logiciels**.
2. Dans l'espace de travail **Bibliothèque de logiciels** , sélectionnez l'une des étapes suivantes pour le type de contenu que vous souhaitez distribuer :
   - **Applications** : Développez **Gestion d'applications** > **Applications**, puis sélectionnez l'application à redistribuer.
   - **Packages** : Développez **Gestion d'applications** > **Packages**, puis sélectionnez le package à redistribuer.
   - **Packages de déploiement** : Développez **Mises à jour logicielles** > **Packages de déploiement**, puis sélectionnez le package de déploiement à redistribuer.
   - **Packages de pilotes** : Développez **Systèmes d'exploitation** > **Packages de pilotes**, puis sélectionnez le package de pilote à redistribuer.
   - **Images de système d'exploitation** : Développez **Systèmes d'exploitation** > **Images du système d'exploitation**, puis sélectionnez l'image du système d'exploitation à redistribuer.

- **Programmes de système d'exploitation** : Développez **Systèmes d'exploitation** > **Programmes d'installation de système d'exploitation**, puis sélectionnez le programme d'installation de système d'exploitation à redistribuer.
- **Images de démarrage** : Développez **Systèmes d'exploitation** > **Images de démarrage**, puis sélectionnez l'image de démarrage à redistribuer.

3. Dans l'onglet **Accueil** , dans le groupe **Propriétés** , cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Emplacements du contenu** , sélectionnez le point de distribution ou le groupe de points de distribution dans lequel vous souhaitez redistribuer le contenu, cliquez sur **Redistribuer**, puis cliquez sur **OK**.

#### Pour redistribuer du contenu à partir des propriétés de package de point de distribution

1. Dans la console Configuration Manager, cliquez sur **Administration**.
2. Dans l'espace de travail **Administration** , cliquez sur **Points de distribution**, puis sélectionnez le point de distribution dans lequel vous souhaitez redistribuer du contenu.
3. Dans l'onglet **Accueil** , dans le groupe **Propriétés** , cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Contenu** , sélectionnez le contenu à redistribuer, cliquez sur **Redistribuer**, puis cliquez sur **OK**.

#### Pour redistribuer du contenu des propriétés du groupe de points de distribution

1. Dans la console Configuration Manager, cliquez sur **Administration**.
2. Dans l'espace de travail **Administration** , cliquez sur **Groupes de points de distribution**, puis sélectionnez le groupe de points de distribution dont vous souhaitez redistribuer du contenu.
3. Dans l'onglet **Accueil** , dans le groupe **Propriétés** , cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Contenu** , sélectionnez le contenu à redistribuer, cliquez sur **Redistribuer**, puis cliquez sur **OK**.

> **IMPORTANT**
> Le contenu du package est redistribué à tous les points de distribution du groupe de points de distribution.

#### Utiliser le SDK pour forcer la réplication de contenu

Vous pouvez utiliser la méthode de classe WMI (Windows Management Instrumentation) **RetryContentReplication** à partir du SDK Configuration Manager pour forcer le gestionnaire de distribution à copier le contenu de l'emplacement source vers la bibliothèque de contenu.

Utilisez uniquement cette méthode pour forcer la réplication quand vous devez redistribuer le contenu après avoir rencontré des problèmes lors de la réplication normale de contenu (généralement validée à l'aide du nœud Surveillance de la console).

Pour plus d'informations sur cette option SDK, consultez RetryContentReplication Method in Class SMS_CM_UpdatePackages (Méthode RetryContentReplication dans la classe SMS_CM_UpdatePackages) sur MSDN.Microsoft.com.

### Supprimer le contenu

Si vous n'avez plus besoin de contenu sur vos points de distribution, vous pouvez supprimer les fichiers de contenu sur le point de distribution.

- Propriétés du package
- Propriétés du point de distribution

- Propriétés du groupe de points de distribution

Cependant, si le contenu est associé à un autre package qui a été distribué au même point de distribution, vous ne pouvez pas le supprimer.

#### Pour supprimer les fichiers de contenu de package de points de distribution

1. Dans la console Configuration Manager, cliquez sur **Bibliothèque de logiciels**.
2. Dans l'espace de travail **Bibliothèque de logiciels** , sélectionnez l'une de ces étapes pour le type de contenu que vous souhaitez supprimer :
   - **Applications** : Développez **Gestion d'applications** > **Applications**, puis sélectionnez l'application à supprimer.
   - **Packages** : Développez **Gestion d'applications** > **Packages**, puis sélectionnez le package à supprimer.
   - **Packages de déploiement** : Développez **Mises à jour logicielles** > **Packages de déploiement**, puis sélectionnez le package de déploiement à supprimer.
   - **Packages de pilotes** : Développez **Systèmes d'exploitation** > **Packages de pilotes**, puis sélectionnez le package de pilotes à supprimer.
   - **Images de système d'exploitation** : Développez **Systèmes d'exploitation** > **Images du système d'exploitation**, puis sélectionnez l'image du système d'exploitation à supprimer.
   - **Programmes de système d'exploitation** : Développez **Systèmes d'exploitation** > **Programmes d'installation de système d'exploitation**, puis sélectionnez le programme d'installation de système d'exploitation à supprimer.
   - **Images de démarrage** : Développez **Systèmes d'exploitation** > **Images de démarrage**, puis sélectionnez l'image de démarrage à supprimer.
3. Dans l'onglet **Accueil** , dans le groupe **Propriétés** , cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Emplacements du contenu** , sélectionnez le point de distribution ou le groupe de points de distribution à partir duquel vous souhaitez supprimer le contenu, cliquez sur **Supprimer**, puis cliquez sur **OK**.

#### Pour supprimer le contenu du package des propriétés du point de distribution

1. Dans la console Configuration Manager, cliquez sur **Administration**.
2. Dans l'espace de travail **Administration** , cliquez sur **Points de distribution**, puis sélectionnez le point de distribution dans lequel vous souhaitez supprimer le contenu.
3. Dans l'onglet **Accueil** , dans le groupe **Propriétés** , cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Contenu** , sélectionnez le contenu à supprimer, cliquez sur **Supprimer**, puis cliquez sur **OK**.

#### Pour supprimer du contenu des propriétés du groupe de points de distribution

1. Dans la console Configuration Manager, cliquez sur **Administration**.
2. Dans l'espace de travail **Administration** , cliquez sur **Groupes de points de distribution**, puis sélectionnez le groupe de points de distribution dans lequel vous souhaitez supprimer du contenu.
3. Dans l'onglet **Accueil** , dans le groupe **Propriétés** , cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Contenu** , sélectionnez le contenu à supprimer, cliquez sur **Supprimer**, puis cliquez sur **OK**.

### Valider le contenu

Le processus de validation du contenu vérifie l'intégrité des fichiers de contenu sur les points de distribution. Vous pouvez activer la validation du contenu selon une planification, ou vous pouvez démarrer manuellement la validation du contenu à partir des propriétés des points de distribution et des packages.

Lors du démarrage du processus de validation du contenu, Configuration Manager vérifie les fichiers de contenu sur les points de distribution et si le hachage du fichier est inattendu pour les fichiers du point de distribution, Configuration Manager crée un message d'état que vous pouvez consulter dans l'espace de travail **Surveillance**.

Pour plus d'informations sur la configuration de la planification de la validation du contenu, consultez Configurations des points de distribution dans la rubrique Installer et configurer des points de distribution pour System Center Configuration Manager.

#### Pour initier la validation du contenu de tout le contenu d'un point de distribution

1. Dans la console Configuration Manager, cliquez sur **Administration**.
2. Dans l'espace de travail **Administration** , cliquez sur **Points de distribution**, puis sélectionnez le point de distribution dont vous voulez valider le contenu.
3. Dans l'onglet **Accueil** , dans le groupe **Propriétés** , cliquez sur **Propriétés**.
4. Dans l'onglet **Accueil** , sélectionnez le package dans lequel vous souhaitez valider le contenu, cliquez sur **Valider**, sur **OK**, puis de nouveau sur **OK**. Le processus de validation du contenu démarre pour le package sur le point de distribution.
5. Pour afficher les résultats du processus de validation du contenu, dans l'espace de travail **Surveillance** , développez **État de distribution**, puis cliquez sur le nœud **État du contenu** . Le contenu de chaque type de package (par exemple, application, package de mises à jour logicielles et image de démarrage) s'affiche. Pour plus d'informations sur la surveillance de l'état du contenu, consultez Surveiller le contenu que vous avez distribué avec System Center Configuration Manager.

#### Pour initier la validation du contenu d'un package

1. Dans la console Configuration Manager, cliquez sur **Bibliothèque de logiciels**.
2. Dans l'espace de travail **Bibliothèque de logiciels** , sélectionnez l'une de ces étapes pour le type de contenu que vous souhaitez valider :
   - **Applications** : Développez **Gestion d'applications** > **Applications**, puis sélectionnez l'application à valider.
   - **Packages** : Développez **Gestion d'applications** > **Packages**, puis sélectionnez le package à valider.
   - **Packages de déploiement** : Développez **Mises à jour logicielles** > **Packages de déploiement**, puis sélectionnez le package de déploiement à valider.
   - **Packages de pilotes** : Développez **Systèmes d'exploitation** > **Packages de pilotes**, puis sélectionnez le package de pilotes à valider.
   - **Images de système d'exploitation** : Développez **Systèmes d'exploitation** > **Images du système d'exploitation**, puis sélectionnez l'image du système d'exploitation à valider.
   - **Programmes de système d'exploitation** : Développez **Systèmes d'exploitation** > **Programmes d'installation de système d'exploitation**, puis sélectionnez le programme d'installation de système d'exploitation à valider.
   - **Images de démarrage** : Développez **Systèmes d'exploitation** > **Images de démarrage**, puis sélectionnez l'image de démarrage à préparer.
3. Dans l'onglet **Accueil** , dans le groupe **Propriétés** , cliquez sur **Propriétés**.

4. Dans l'onglet **Emplacements du contenu** , sélectionnez le point de distribution ou le groupe de points de distribution dans lequel vous souhaitez valider le contenu, cliquez sur **Valider**, sur **OK**, puis de nouveau sur **OK**. Le processus de validation du contenu démarre pour le contenu situé sur le point de distribution ou le groupe de points de distribution sélectionné.

5. Pour afficher les résultats du processus de validation du contenu, dans l'espace de travail **Surveillance** , développez **État de distribution**, puis cliquez sur le nœud **État du contenu** . Le contenu de chaque type de package (par exemple, application, package de mises à jour logicielles et image de démarrage) s'affiche. Pour plus d'informations sur la surveillance de l'état du contenu, consultez Surveiller le contenu que vous avez distribué avec System Center Configuration Manager.

# Surveiller le contenu que vous avez distribué avec System Center Configuration Manager

22/06/2018 • 14 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez la console System Center Configuration Manager pour surveiller le contenu distribué, à savoir :

- État de tous les types de package liés aux points de distribution associés.
- État de la validation du contenu d'un package.
- État du contenu attribué à un groupe de points de distribution spécifique.
- État du contenu attribué à un point de distribution.
- État des fonctionnalités facultatives pour chaque point de distribution (validation du contenu, PXE et multidiffusion).

> **NOTE**
> Configuration Manager surveille uniquement le contenu d'un point de distribution situé dans la bibliothèque de contenu. Le contenu stocké sur le point de distribution au sein de packages ou de partages personnalisés n'est pas surveillé.

## Surveillance de l'état du contenu

Le nœud **État du contenu** dans l'espace de travail **Surveillance** fournit des informations sur les packages de contenu. Dans la console Configuration Manager, vous pouvez examiner les informations suivantes :

- Nom du package.
- Type.
- Nombre de points de distribution ayant reçu un package.
- Niveau de compatibilité.
- Date de création du package.
- ID du package.
- Version source.

Vous y trouverez également des informations d'état détaillées pour chaque package, ainsi que l'état de distribution du package :

- Nombre d'échecs.
- Distributions en attente.
- Nombre d'installations.

Vous pouvez aussi gérer les distributions qui sont toujours en cours de cheminement vers un point de distribution ou celles qui n'ont pas pu distribuer correctement le contenu à un point de distribution :

- L'option pour annuler ou redistribuer du contenu est disponible quand vous affichez le message d'état du déploiement d'une tâche de distribution sur un point de distribution dans le volet **Détails du bien**. Ce volet se trouve sous l'onglet **En cours** ou sous l'onglet **Erreur** du nœud **État du contenu**.
- De plus, les détails de la tâche affichent le pourcentage de la tâche qui est terminé quand vous affichez les détails d'une tâche sous l'onglet **En cours**. Les détails du travail affichent également le nombre de nouvelles tentatives restantes pour une tâche, ainsi que la durée restante avant la nouvelle tentative suivante quand

vous affichez les détails d'une tâche disponible à partir de l'onglet **Erreur**.

Quand vous annulez un déploiement qui n'est pas encore terminé, la tâche de distribution pour transférer ce contenu s'arrête :

- L'état du déploiement est ensuite mis à jour pour indiquer que la distribution a échoué et a été annulée par une action de l'utilisateur.
- Ce nouvel état s'affiche dans l'onglet **Erreur** .

> **TIP**
> Lorsqu'un déploiement est presque terminé, il est possible que l'action visant à annuler cette distribution ne s'exécute pas avant la fin de la distribution vers le point de distribution. Lorsque cela se produit, l'action visant à annuler le déploiement est ignorée et l'état du déploiement s'affiche comme réussi.

> **NOTE**
> Bien que vous puissiez sélectionner l'option visant à annuler une distribution vers un point de distribution situé sur un serveur de site, cela n'a aucun effet. Cela est dû au fait que le serveur de site et le point de distribution sur un serveur de site partagent le même magasin de contenu d'instances uniques. Il n'existe aucune tâche réelle de distribution à annuler.

Quand vous redistribuez du contenu dont le transfert sur un point de distribution a précédemment échoué, Configuration Manager relance immédiatement le redéploiement de ce contenu sur le point de distribution. Configuration Manager met à jour l'état du déploiement pour refléter l'état actuel de ce redéploiement.

Procédez comme suit pour afficher l'état du contenu et gérer les distributions qui sont toujours en cours ou qui ont échoué.

**Pour surveiller l'état du contenu**

1. Dans la console Configuration Manager, cliquez sur **Surveillance**.
2. Dans l'espace de travail **Surveillance** , développez **État de distribution**, puis cliquez sur **État du contenu**. Les packages sont affichés.
3. Sélectionnez le package pour lequel vous souhaitez obtenir des informations d'état détaillées.
4. Dans l'onglet **Accueil** , cliquez sur **Afficher l'état**. Des informations d'état détaillées pour le package sont affichées.

**Pour annuler une distribution qui est toujours en cours**

1. Dans la console Configuration Manager, cliquez sur **Surveillance**.
2. Dans l'espace de travail **Surveillance** , développez **État de distribution**, puis cliquez sur **État du contenu**. Les packages sont affichés.
3. Sélectionnez le package que vous souhaitez gérer, puis dans le volet des détails, cliquez sur **Afficher l'état**.
4. Dans le volet **Détails du bien** de l'onglet **En cours**, cliquez avec le bouton droit sur l'entrée correspondant à la distribution que vous souhaitez annuler, puis sélectionnez **Annuler**.
5. Cliquez sur **Oui** pour confirmer l'action et d'annuler la tâche de distribution pour ce point de distribution.

**Pour redistribuer le contenu qui n'a pas pu être distribué**

1. Dans la console Configuration Manager, cliquez sur **Surveillance**.
2. Dans l'espace de travail **Surveillance** , développez **État de distribution**, puis cliquez sur **État du**

**contenu**. Les packages sont affichés.

3. Sélectionnez le package que vous souhaitez gérer, puis dans le volet des détails, cliquez sur **Afficher l'état**.
4. Dans le volet **Détails du bien** sous l'onglet **Erreur**, cliquez avec le bouton droit sur l'entrée correspondant à la distribution que vous souhaitez redistribuer, puis sélectionnez **Redistribuer**.
5. Cliquez sur **Oui** pour confirmer l'action et démarrer le processus de redistribution sur ce point de distribution.

## État du groupe de points de distribution

Le nœud **État du groupe de points de distribution** dans l'espace de travail **Surveillance** fournit des informations sur les groupes de points de distribution. Vous pouvez notamment consulter les informations suivantes :

- Nom du groupe de points de distribution.
- Description.
- Nombre de points de distribution appartenant au groupe de points de distribution.
- Nombre de packages attribués au groupe.
- État du groupe de points de distribution.
- Niveau de compatibilité.

Vous pouvez également consulter les informations d'état détaillées suivantes :

- Erreurs liées au groupe de points de distribution.
- Nombre de distributions en cours.
- Nombre de distributions correctement effectuées.

**Pour surveiller l'état du groupe de points de distribution**

1. Dans la console Configuration Manager, cliquez sur **Surveillance**.
2. Dans l'espace de travail **Surveillance** , développez **État de distribution**, puis cliquez sur **État du groupe de points de distribution**. Les groupes de points de distribution sont affichés.
3. Sélectionnez le groupe de points de distribution pour lequel vous souhaitez obtenir des informations d'état détaillées.
4. Dans l'onglet **Accueil** , cliquez sur **Afficher l'état**. Des informations d'état détaillées pour le groupe de points de distribution sont affichées.

## État de configuration du point de distribution

Le nœud **État de configuration du point de distribution** dans l'espace de travail **Surveillance** fournit des informations sur le point de distribution. Vous pouvez vérifier quels attributs sont activés pour le point de distribution, notamment le PXE, la multidiffusion, la validation du contenu et l'état de distribution pour le point de distribution. Vous pouvez également afficher des informations d'état détaillées pour le point de distribution.

> **WARNING**
> L'état de la configuration du point de distribution concerne les dernières 24 heures. Si le point de distribution présente une erreur et que celle-ci est résolue, l'état d'erreur peut s'afficher jusqu'à 24 heures après la restauration du point de distribution.

Pour afficher l'état de configuration du point de distribution, procédez comme suit.

**Pour surveiller l'état de configuration du point de distribution**

1. Dans la console Configuration Manager, cliquez sur **Surveillance**.
2. Dans l'espace de travail **Surveillance** , développez **État de distribution**, puis cliquez sur **État de la configuration du point de distribution**. Les points de distribution sont affichés.
3. Sélectionnez le point de distribution pour lequel vous souhaitez obtenir des informations d'état du point de distribution.
4. Dans le volet des résultats, cliquez sur l'onglet **Détails** . Des informations d'état pour le point de distribution sont affichées.

## Tableau de bord Sources de données du client

À compter de la version 1610, vous pouvez utiliser le tableau de bord **Sources de données du client** pour comprendre l'utilisation du Cache d'homologue dans votre environnement. Le tableau de bord commencera à afficher des données une fois que les clients auront téléchargé du contenu, et signalera ces informations au site. Cette opération peut prendre jusqu'à 24 heures.

> **TIP**
> Le **Cache d'homologue client** et le tableau de bord **Sources de données de clients** sont des fonctionnalités en préversion présentées dans la version 1610. À compter de la version 1710, ces fonctionnalités ne sont plus des fonctionnalités en préversion. Vous devez activer le cache d'homologue client pour que le tableau de bord Sources de données de clients devienne visible dans la console.

Dans la console, accédez à **Surveillance** > **État de distribution** > **Sources de données du client**. Vous pouvez sélectionner ici une période à appliquer au tableau de bord. Ensuite, dans l'affichage, vous pouvez sélectionner le groupe de limites ou le package sur lesquels vous souhaitez afficher des informations. Lors de la consultation de celles-ci, vous pouvez pointer le curseur de la souris sur la surface pour afficher plus de détails sur les différentes sources de contenu ou de stratégie.

Ces détails incluent :

- **Sources de contenu pour les clients** : affiche les sources à partir desquelles les clients ont obtenu du contenu.
- **Points de distribution** : affiche le nombre de points de distribution qui font partie du groupe de limites sélectionné.
- **Clients ayant utilisé un point de distribution** : affiche le nombre de clients membres du groupe de limites sélectionné qui ont utilisé un point de distribution pour obtenir du contenu.
- **Sources de mise en cache d'homologue** : pour le groupe de limites sélectionné, affiche le nombre de sources de mise en cache d'homologue qui ont fourni un historique de téléchargement.
- **Clients ayant utilisé un homologue** : affiche le nombre de clients membres du groupe de limites sélectionné qui ont utilisé une source de mise en cache d'homologue pour obtenir du contenu.

Vous pouvez également utiliser un nouveau rapport, **Sources de données du client - Résumé**, pour afficher une synthèse des sources de données du client pour chaque groupe de limites.

# Exécuter la découverte pour System Center Configuration Manager

22/06/2018 • 8 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous utilisez une ou plusieurs méthodes de découverte dans System Center Configuration Manager pour trouver les ressources d'appareils et d'utilisateurs que vous pouvez gérer. Vous pouvez également utiliser la découverte pour identifier l'infrastructure réseau de votre environnement. Vous disposez de diverses méthodes permettant de découvrir différents éléments. Chaque méthode a ses propres configurations et limitations.

## Vue d'ensemble de la découverte

La découverte est le processus par lequel Configuration Manager apprend quels élément vous pouvez gérer. Les méthodes de découverte disponibles sont les suivantes :

- Découverte de forêts Active Directory
- Découverte de groupes Active Directory
- Découverte de systèmes Active Directory
- Découverte d'utilisateurs Active Directory
- Découverte par pulsations d'inventaire
- Découverte du réseau
- Découverte de serveurs

> **TIP**
> Vous pouvez en savoir plus sur chaque méthode de découverte dans About discovery methods for System Center Configuration Manager (À propos des méthodes de découverte pour System Center Configuration Manager).
>
> Pour savoir quelle méthode privilégier et quel site de votre hiérarchie choisir, consultez Sélectionner des méthodes de découverte à utiliser pour System Center Configuration Manager.

Pour utiliser la plupart des méthodes de découverte, vous devez les activer sur un site et les configurer pour qu'elles effectuent une recherche sur un réseau ou à des emplacements Active Directory spécifiques. Lorsqu'une méthode de découverte est exécutée, elle interroge l'emplacement spécifié afin de recueillir des informations sur les appareils ou utilisateurs que Configuration Manager peut gérer. Quand une méthode de découverte trouve des informations sur une ressource, elle place ces informations dans un fichier appelé enregistrement de données de découverte (DDR, Discovery Data Record). Ce fichier est ensuite traité par un site principal ou un site d'administration centrale. Le traitement d'un fichier DDR génère un nouvel enregistrement dans la base de données du site pour les nouvelles ressources découvertes, ou met à jour des enregistrements existants avec les nouvelles informations.

Certaines méthodes de découverte peuvent générer un volume important de trafic réseau, et les fichiers DDR produits peuvent entraîner une utilisation intensive des ressources du processeur au cours du traitement. Par conséquent, prévoyez d'utiliser uniquement les méthodes de découverte dont vous avez besoin pour atteindre vos objectifs. Vous pouvez commencer par n'utiliser qu'une ou deux méthodes de découverte, avant

d'éventuellement en activer d'autres de manière contrôlée par la suite pour étendre le niveau de découverte dans votre environnement.

Une fois les informations de découverte ajoutées à la base de données du site, elles sont répliquées sur chaque site dans la hiérarchie, indépendamment du site sur lequel les informations ont été découvertes ou traitées. Par conséquent, si vous pouvez configurer des planifications et des paramètres différents pour les méthodes de découverte sur différents sites, vous ne pouvez exécuter une méthode de découverte spécifique que sur un seul site. Cela permet de réduire l'utilisation de la bande passante réseau par le biais d'actions de détection de doublons, et de réduire le traitement de données de découverte redondantes sur plusieurs sites.

Vous pouvez utiliser les données de découverte pour créer des regroupements et des requêtes personnalisés qui regroupent logiquement des ressources pour les tâches de gestion suivantes. Par exemple :

- Effectuer une installation Push du client ou une mise à niveau.
- Déployer du contenu sur des utilisateurs ou appareils.
- Déployer des paramètres client et les configurations associées.

## À propos des enregistrements de données de découverte

Les DDR sont des fichiers créés par une méthode de découverte. Ils contiennent des informations sur une ressource que vous pouvez gérer dans Configuration Manager, comme des ordinateurs, des utilisateurs et, dans certains cas, l'infrastructure réseau. Ils sont traités au niveau des sites principaux ou des sites d'administration centrale. Une fois que les informations sur la ressource contenues dans le DDR ont été entrées dans la base de données, le DDR est supprimé et ces informations sont répliquées sous forme de données globales sur tous les sites de la hiérarchie.

Le site où un DDR est traité dépend des informations qu'il contient :

- Les DDR des ressources nouvellement découvertes, qui ne sont pas dans la base de données, sont traités sur le site de niveau supérieur de la hiérarchie. Le site de niveau supérieur crée un nouvel enregistrement de ressource dans la base de données et lui attribue un identifiant unique. Les DDR sont transférés par réplication basée sur les fichiers, jusqu'à ce qu'ils atteignent le site de niveau supérieur.
- Les DDR d'objets précédemment découverts sont traités au niveau des sites principaux. Les sites enfants principaux ne transfèrent pas de DDR au site d'administration centrale lorsque le DDR contient des informations sur une ressource qui est déjà dans la base de données.
- Les sites secondaires ne traitent pas les DDR, mais les transfèrent toujours par une réplication basée sur les fichiers sur leur site principal parent.

Les fichiers DDR sont identifiés par l'extension .ddr et ont généralement une taille standard d'environ 1 Ko.

## Prise en main de la découverte :

Avant d'utiliser la console Configuration Manager pour configurer la découverte, vous devez comprendre les différences entre les méthodes, les opérations possibles et, pour certaines d'entre elles, leurs limites.

Les rubriques suivantes peuvent vous aider à utiliser correctement les méthodes de découverte :

- À propos des méthodes de découverte pour System Center Configuration Manager
- Sélectionner les méthodes de découverte à utiliser pour System Center Configuration Manager

Dès lors que vous avez déterminé quelles méthodes utiliser, vous pouvez les configurer en vous aidant des conseils fournis dans Configurer les méthodes de découverte pour System Center Configuration Manager.

# À propos des méthodes de découverte pour System Center Configuration Manager

22/06/2018 • 53 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les méthodes de découverte de Configuration Manager permettent de rechercher différents appareils sur votre réseau, des appareils et des utilisateurs dans Active Directory, ou des utilisateurs dans Azure AD (Azure Active Directory). Pour utiliser efficacement une méthode de découverte, vous devez en comprendre les configurations disponibles et les limitations.

## Découverte de forêts Active Directory

**Configurable :** Oui

**Activée par défaut :** Non

**Comptes** que vous pouvez utiliser pour exécuter cette méthode :

- **Compte de découverte de forêts Active Directory** (défini par l'utilisateur)
- **Compte d'ordinateur** du serveur de site

À la différence des autres méthodes de découverte Active Directory, la découverte de forêts Active Directory ne découvre pas des ressources que vous pouvez gérer. Au lieu de cela, cette méthode découvre les emplacements réseau qui sont configurés dans Active Directory. Elle peut convertir ces emplacements en limites à utiliser dans votre hiérarchie.

Quand cette méthode est exécutée, elle effectue une recherche dans la forêt Active Directory locale, chaque forêt approuvée et chaque forêt supplémentaire que vous configurez dans le nœud **Forêts Active Directory** de la console Configuration Manager.

Utilisez la découverte de forêts Active Directory pour :

- Découvrir les sites et sous-réseaux Active Directory, puis créer les limites de Configuration Manager en fonction de ces emplacements réseau.
- Identifier les sur-réseaux qui sont affectés à un site Active Directory. Convertir chaque sur-réseau en limite de plage d'adresses IP.
- Publier sur AD DS (Active Directory Domain Services) dans une forêt quand la publication est activée pour cette forêt. Le compte de forêt Active Directory spécifié doit disposer d'autorisations sur cette forêt.

Vous pouvez gérer la découverte de forêts Active Directory dans la console Active Directory. Accédez à l'espace de travail **Administration** et développez **Configuration de la hiérarchie**.

- **Méthodes de découverte** : Activez la découverte de forêts Active Directory pour l'exécution sur le site de niveau supérieur de votre hiérarchie. Vous pouvez également spécifier un calendrier simple pour exécuter la découverte. Configurez-la pour créer automatiquement des limites à partir des sous-réseaux IP et des sites Active Directory qui sont découverts. La découverte de forêts Active Directory ne peut pas s'exécuter sur un site principal enfant ou un site secondaire.
- **Forêts Active Directory** : Configurez les forêts supplémentaires à découvrir, spécifiez chaque compte de forêt Active Directory et configurez la publication de chaque forêt. Surveillez le processus de découverte.

Ajoutez des sous-réseaux IP ainsi que des sites Active Directory à Configuration Manager en tant que limites et membres des groupes de limites.

Pour configurer la publication pour les forêts Active Directory pour chaque site de votre hiérarchie, connectez votre console Configuration Manager au site de niveau supérieur de votre hiérarchie. L'onglet **Publication** dans la boîte de dialogue **Propriétés** d'un site Active Directory peut uniquement afficher le site actuel et ses sites enfants. Quand la publication est activée pour une forêt et que le schéma de cette forêt est étendu pour Configuration Manager, les informations suivantes sont publiées pour chaque site autorisé à publier dans cette forêt Active Directory :

- **SMS-Site-<code_site>**
- **SMS-MP-<<code_site>-<nom_serveur_de_site>**
- **SMS-SLP-<<code_site>-<nom_serveur_de_site>**
- **SMS-<code_site>-<nom_site_Active_Directory_ou sous-réseau>**

> **NOTE**
> Les sites secondaires utilisent toujours le compte d'ordinateur du serveur de site secondaire pour publier dans Active Directory. Si vous voulez que les sites secondaires publient dans Active Directory, vérifiez que le compte d'ordinateur du serveur de site secondaire dispose d'autorisations de publication dans Active Directory. Un site secondaire ne peut pas publier de données dans une forêt non approuvée.

Caution
Si vous décochez l'option de publication d'un site sur une forêt Active Directory, toutes les informations publiées précédemment pour ce site, notamment des rôles de systèmes de site disponibles, sont supprimées d'Active Directory.

Les actions de la découverte de forêts Active Directory sont enregistrées dans les journaux suivants :

- Toutes les actions, à l'exception des actions liées à la publication, sont enregistrées dans le fichier **ADForestDisc.Log** du dossier **<Chemin_installation>\Logs** sur le serveur de site.
- Les actions de publication de la découverte de forêts Active Directory sont enregistrées dans les fichiers **hman.log** et **sitecomp.log** du dossier **<Chemin_installation>\Logs** sur le serveur de site.

Pour plus d'informations sur la configuration de cette méthode de découverte, consultez Configurer les méthodes de découverte.

## Découverte de groupes Active Directory

**Configurable :** Oui

**Activée par défaut :** Non

**Comptes** que vous pouvez utiliser pour exécuter cette méthode :

- **Compte de découverte de groupes Active Directory** (défini par l'utilisateur)
- **Compte d'ordinateur** du serveur de site

> **TIP**
> Pour plus d'informations,voir la section Fonctionnalités communes de la découverte de groupes, de systèmes et d'utilisateurs Active Directory.

Utilisez cette méthode pour effectuer une recherche dans Active Directory Domain Services et identifier ce qui suit :

- Groupes de sécurité local, global et universel.
- Appartenance aux groupes.
- Informations limitées sur les ordinateurs des membres d'un groupe et les utilisateurs, notamment quand une autre méthode de découverte n'a pas encore découvert ces ordinateurs et utilisateurs.

Cette méthode de découverte est prévue pour identifier les groupes et les relations du groupe des membres des groupes. Par défaut, seuls les groupes de sécurité sont découverts. Si vous voulez également découvrir l'appartenance aux groupes de distribution, vous devez cocher la case de l'option **Découvrir l'appartenance aux groupes de distribution** sous l'onglet **Option** de la boîte de dialogue des **propriétés de découverte de groupes Active Directory**.

La découverte de groupes Active Directory ne prend pas en charge les attributs Active Directory étendus qui peuvent être identifiés à l'aide de la découverte de systèmes Active Directory ou de la découverte d'utilisateurs Active Directory. Puisque cette méthode de découverte n'est pas optimisée pour la découverte des ressources d'ordinateur et d'utilisateur, envisagez de l'exécuter après avoir exécuté la découverte de systèmes Active Directory et la découverte d'utilisateurs Active Directory. En effet, cette méthode crée un enregistrement de données de découverte (DDR) complet pour les groupes, mais seulement un DDR limité pour les ordinateurs et les utilisateurs qui appartiennent à des groupes.

Vous pouvez configurer les étendues de découverte suivantes, qui contrôlent la manière dont cette méthode recherche des informations :

- **Emplacement**: Utilisez un emplacement si vous souhaitez rechercher un ou plusieurs conteneurs Active Directory. Cette option d'étendue prend en charge une recherche récursive des conteneurs Active Directory spécifiés. Ce processus recherche également dans chaque conteneur enfant sous le conteneur que vous spécifiez. Il continue jusqu'à ne plus trouver de conteneur enfant.
- **Groupes**: Utilisez les groupes si vous souhaitez rechercher un ou plusieurs groupes Active Directory spécifiques. Vous pouvez configurer **Domaine Active Directory** de manière à utiliser le domaine et la forêt par défaut ou limiter la recherche à un contrôleur de domaine individuel. En outre, vous pouvez spécifier un ou plusieurs groupes à rechercher. Si vous ne spécifiez pas au moins un groupe, tous les groupes trouvés à l'emplacement **Domaine Active Directory** spécifié sont recherchés.

Caution

Quand vous configurez une étendue de découverte, choisissez uniquement les groupes que vous devez découvrir. En effet, la découverte de groupes Active Directory tente de découvrir chaque membre de chaque groupe dans l'étendue de découverte. La découverte de grands groupes peut demander l'utilisation extensive de bande passante et de ressources Active Directory.

> **NOTE**
>
> Pour créer des regroupements basés sur des attributs Active Directory étendus (et assurer des résultats de découverte précis pour les ordinateurs et les utilisateurs), exécutez la découverte de systèmes Active Directory ou la découverte d'utilisateurs Active Directory, en fonction de ce que vous voulez découvrir.

Les actions de la découverte de groupes Active Directory sont enregistrées dans le fichier **adsgdis.log** du dossier **<Chemin_installation>\LOGS** sur le serveur de site.

Pour plus d'informations sur la configuration de cette méthode de découverte, consultez Configurer les méthodes de découverte.

# Découverte de systèmes Active Directory

**Configurable :** Oui

**Activée par défaut :** Non

**Comptes** que vous pouvez utiliser pour exécuter cette méthode :

- **Compte de découverte de systèmes Active Directory** (défini par l'utilisateur)
- **Compte d'ordinateur** du serveur de site

> **TIP**
> Pour plus d'informations,voir la section Fonctionnalités communes de la découverte de groupes, de systèmes et d'utilisateurs Active Directory.

Utilisez cette méthode de découverte pour rechercher dans les emplacements Active Directory Domain Services spécifiés des ressources d'ordinateurs pouvant être utilisées pour créer des regroupements et des requêtes. Vous pouvez également installer le client Configuration Manager sur un appareil détecté à l'aide de l'installation Push du client.

Par défaut, cette méthode découvre des informations de base sur l'ordinateur, notamment les attributs suivants :

- Nom de l'ordinateur
- Système d'exploitation et version
- nom du conteneur Active Directory.
- Adresse IP
- Site Active Directory
- Horodateur de la dernière ouverture de session

Pour réussir la création d'un DDR pour un ordinateur, la découverte de systèmes Active Directory doit pouvoir identifier le compte d'ordinateur, puis traduire correctement le nom de l'ordinateur en une adresse IP.

Dans la boîte de dialogue **Propriétés de la découverte de systèmes Active Directory**, sous l'onglet **Attributs Active Directory**, vous pouvez afficher la liste complète des attributs d'objets par défaut découverts. Vous pouvez également configurer cette méthode pour découvrir des attributs supplémentaires (étendus).

Les actions de la découverte de systèmes Active Directory sont enregistrées dans le fichier **adsysdis.log** du dossier **<Chemin_installation>\LOGS** sur le serveur de site.

Pour plus d'informations sur la configuration de cette méthode de découverte, consultez Configurer les méthodes de découverte.

# Découverte d'utilisateurs Active Directory

**Configurable :** Oui

**Activée par défaut :** Non

**Comptes** que vous pouvez utiliser pour exécuter cette méthode :

- **Compte de découverte d'utilisateurs Active Directory** (défini par l'utilisateur)
- **Compte d'ordinateur** du serveur de site

> **TIP**
> Pour plus d'informations,voir la section Fonctionnalités communes de la découverte de groupes, de systèmes et d'utilisateurs Active Directory.

Utilisez cette méthode de découverte pour rechercher dans Active Directory Domain Services des comptes d'utilisateur et les attributs associés. Par défaut, cette méthode découvre des informations de base sur le compte d'utilisateur, notamment les attributs suivants :

- Nom d'utilisateur
- Nom d'utilisateur unique (y compris le nom de domaine)
- Domaine
- Noms de conteneurs Active Directory

Dans la boîte de dialogue **Propriétés de la découverte d'utilisateurs Active Directory**, sous l'onglet **Attributs Active Directory**, vous pouvez afficher la liste par défaut complète des attributs d'objets découverts. Vous pouvez également configurer cette méthode pour découvrir des attributs supplémentaires (étendus).

Les actions de la découverte d'utilisateurs Active Directory sont enregistrées dans le fichier **adusrdis.log** du dossier **<Chemin_installation>\LOGS** sur le serveur de site.

Pour plus d'informations sur la configuration de cette méthode de découverte, consultez Configurer les méthodes de découverte.

## Découverte des utilisateurs Azure Active Directory

Utilisez la découverte d'utilisateurs Azure AD (Azure Active Directory) pour rechercher dans votre abonnement Azure AD les utilisateurs avec une identité de cloud moderne. La découverte d'utilisateurs Azure AD peut trouver les attributs suivants :

- objectId
- displayName
- messagerie
- mailNickname
- onPremisesSecurityIdentifier
- userPrincipalName
- AAD tenantID

Cette méthode prend en charge une synchronisation complète et une synchronisation delta des attributs utilisateur à partir d'Azure AD. Vous pouvez ensuite utiliser ces informations avec les données de découverte que vous collectez par le biais des autres méthodes de découverte.

Les actions de la découverte d'utilisateurs Azure AD sont enregistrées dans le fichier **SMS_AZUREAD_DISCOVERY_AGENT.log** sur le serveur de site de niveau supérieur de la hiérarchie.

Pour configurer la découverte d'utilisateurs Azure AD, consultez Configurer les services Azure pour la gestion cloud. Pour plus d'informations sur la configuration de cette méthode de découverte, consultez Configurer la découverte des utilisateurs Azure AD.

## Découverte par pulsations d'inventaire

**Configurable :** Oui

**Activée par défaut :** Oui

**Comptes** que vous pouvez utiliser pour exécuter cette méthode :

- **Compte d'ordinateur** du serveur de site

La découverte par pulsations d'inventaire diffère des autres méthodes de découverte de Configuration Manager. Elle est activée par défaut et s'exécute sur chaque client de l'ordinateur (et non sur un serveur de site) pour créer un DDR. Pour les clients d'appareils mobiles, ce DDR est créé par le point de gestion qui est utilisé par le client de l'appareil mobile. Pour permettre la tenue à jour de l'enregistrement de base de données des clients Configuration Manager, ne désactivez pas la découverte par pulsations d'inventaire. Par ailleurs, cette méthode peut forcer la découverte d'un ordinateur en tant que nouvel enregistrement de ressource. Elle peut également de nouveau remplir l'enregistrement de base de données d'un ordinateur qui a été supprimé de la base de données.

La découverte par pulsations d'inventaire est exécutée selon un calendrier configuré pour tous les clients de la hiérarchie. Le calendrier par défaut pour la découverte par pulsations d'inventaire est défini sur tous les sept jours. Si vous modifiez l'intervalle de découverte par pulsations d'inventaire, vérifiez qu'elle est exécutée plus fréquemment que la tâche de maintenance de site **Supprimer les données de découverte anciennes**. Cette tâche supprime les enregistrements de clients inactifs de la base de données du site. Vous pouvez configurer la tâche **Supprimer les données de découverte anciennes** uniquement pour les sites principaux.

Vous pouvez également appeler manuellement la découverte par pulsations d'inventaire sur un client spécifique. Exécutez le **Cycle de collecte de données de découverte** sous l'onglet **Action** du panneau de configuration Configuration Manager d'un client.

Durant son exécution, la découverte par pulsations d'inventaire crée un DDR comprenant les informations actuelles du client. Le client copie ensuite ce petit fichier (d'environ 1 Ko) sur un point de gestion pour qu'un site principal puisse le traiter. Le fichier comprend les informations suivantes :

- Emplacement réseau
- Nom NetBIOS
- Version de l'agent client
- Détails sur l'état opérationnel

La découverte par pulsations d'inventaire est la seule méthode de découverte qui fournit des détails sur l'état de l'installation du client. Pour cela, elle met à jour l'attribut du client de la ressource système avec une valeur égale à **Oui**.

> **NOTE**
> Même lorsque la découverte par pulsations d'inventaire est désactivée, les enregistrements de découverte de données sont toujours créés et soumis pour les clients d'appareils mobiles actifs. Ce comportement garantit que la tâche **Supprimer les données de découverte anciennes** n'affecte pas les appareils mobiles actifs. Quand la tâche **Supprimer les données de découverte anciennes** supprime un enregistrement de base de données pour un appareil mobile, elle révoque également le certificat de l'appareil. Cette action empêche l'appareil mobile de se connecter aux points de gestion.

Les actions de la découverte par pulsations d'inventaire sont consignées aux emplacements suivants :

- Pour les ordinateurs clients, les actions de la découverte par pulsations d'inventaire sont enregistrées sur le client dans le fichier **InventoryAgent.log** du dossier *%Windir%\CCM\Logs*.
- Pour les clients d'appareils mobiles, les actions de découverte par pulsations d'inventaire sont enregistrées dans le fichier **DMPRP.log** du dossier *%Program Files%\CCM\Logs* du point de gestion que le client d'appareil mobile utilise.

Pour plus d'informations sur la configuration de cette méthode de découverte, consultez Configurer les méthodes de découverte.

## Découverte du réseau

**Configurable :** Oui

**Activée par défaut :** Non

**Comptes** que vous pouvez utiliser pour exécuter cette méthode :

- **Compte d'ordinateur** du serveur de site

Utilisez cette méthode pour découvrir la topologie de votre réseau et les appareils de votre réseau qui ont une adresse IP. La découverte du réseau cherche sur votre réseau des ressources sur lesquelles IP est activé en interrogeant les entités suivantes :

- Serveurs qui exécutent une implémentation Microsoft de DHCP
- Caches ARP (Address Resolution Protocol) dans les routeurs réseau
- périphériques SNMP
- Domaines Active Directory

Pour utiliser la découverte du réseau, vous devez spécifier le *niveau* de découverte à exécuter. Vous configurez également un ou plusieurs mécanismes de découverte qui permettent à la découverte du réseau d'interroger des segments ou périphériques réseau. Vous pouvez également configurer des paramètres qui permettent de contrôler des actions de découverte sur le réseau. Enfin, vous définissez un ou plusieurs calendriers d'exécution de la découverte du réseau.

Pour que cette méthode découvre une ressource, elle doit identifier l'adresse IP et le masque de sous-réseau de la ressource. Les méthodes suivantes sont utilisées pour identifier le masque de sous-réseau d'un objet :

- **Mémoire cache ARP de routeur :** La découverte du réseau interroge la mémoire cache ARP d'un routeur pour rechercher des informations de sous-réseau. En règle générale, les données situées dans la mémoire cache ARP d'un routeur ont une courte durée de vie. Par conséquent, quand la découverte du réseau interroge la mémoire cache ARP, celle-ci peut ne plus avoir d'informations sur l'objet demandé.
- **DHCP :** La découverte du réseau interroge chaque serveur DHCP que vous spécifiez pour découvrir les appareils pour lesquels le serveur DHCP a fourni un bail. La découverte du réseau prend en charge uniquement les serveurs DHCP qui exécutent l'implémentation Microsoft du protocole DHCP.
- **Unité SNMP :** La découverte du réseau peut interroger directement une unité SNMP. Pour que la découverte du réseau puisse interroger un périphérique, celui-ci doit avoir un agent SNMP local installé. Configurez également la découverte du réseau pour utiliser le nom de communauté utilisé par l'agent SNMP.

Quand la découverte identifie un objet IP et peut déterminer le masque de sous-réseau des objets, elle crée un DDR pour cet objet. Étant donné que différents types d'appareils se connectent au réseau, la découverte du réseau découvre des ressources qui ne prennent pas en charge le client Configuration Manager. Par exemple, parmi les périphériques qui peuvent être découverts mais qui ne peuvent pas être gérés, citons les imprimantes et les routeurs.

La découverte du réseau peut retourner plusieurs attributs dans le cadre de l'enregistrement de découverte qu'elle crée, Parmi ces attributs, citons notamment :

- Nom NetBIOS
- Adresses IP

- Domaine de la ressource
- Rôles de système
- Nom de communauté SNMP
- Adresses MAC

L'activité de la découverte du réseau est enregistrée dans le fichier **Netdisc.log** dans *<Chemin_installation>\Logs* sur le serveur de site qui exécute la découverte.

Pour plus d'informations sur la configuration de cette méthode de découverte, consultez Configurer les méthodes de découverte.

> **NOTE**
> Les réseaux complexes et les connexions à faible bande passante peuvent ralentir la découverte du réseau et générer un important trafic réseau. Comme meilleure pratique, exécutez la découverte du réseau uniquement lorsque les autres méthodes de découverte ne peuvent pas trouver les ressources que vous devez découvrir. Par exemple, utilisez la découverte du réseau si vous devez découvrir des ordinateurs du groupe de travail. D'autres méthodes de découverte ne découvrent pas les ordinateurs du groupe de travail.

**Niveaux de découverte du réseau**

Lorsque vous configurez la découverte du réseau, vous spécifiez l'un des trois niveaux de découverte :

| NIVEAU DE DÉCOUVERTE | DÉTAILS |
|---|---|
| Topologie | Ce niveau découvre des routeurs et des sous-réseaux mais n'identifie pas un masque de sous-réseau pour les objets. |
| Topologie et client ; | En plus de la topologie, ce niveau découvre des clients potentiels, comme des ordinateurs, et des ressources, comme des imprimantes et des routeurs. Ce niveau de découverte tente d'identifier le masque de sous-réseau des objets qu'il trouve. |
| Topologie, client et système d'exploitation. | Outre la topologie et les clients potentiels, ce niveau tente de découvrir le nom et la version du système d'exploitation de l'ordinateur. Ce niveau utilise l'Explorateur Windows et les appels de gestion de réseau Windows. |

Avec chaque niveau incrémentiel, la découverte du réseau augmente son activité et l'utilisation de la bande passante du réseau. Tenez compte du trafic réseau qui peut être généré avant d'activer tous les aspects de la découverte du réseau.

Par exemple, lorsque vous utilisez la découverte du réseau pour la première fois, vous pouvez commencer avec le niveau de topologie uniquement pour identifier votre infrastructure réseau. Ensuite, reconfigurez la découverte du réseau pour découvrir des objets et les systèmes d'exploitation de leur appareil. Vous pouvez également configurer des paramètres qui limitent la découverte du réseau à une plage spécifique de segments de réseau. De cette façon, vous découvrez des objets à des emplacements réseau dont vous avez besoin et évitez tout trafic réseau inutile. Ce processus vous permet également de découvrir des objets à partir de routeurs de périphérie ou à l'extérieur de votre réseau.

**Options de découverte du réseau**

Pour permettre à la découverte du réseau de rechercher des appareils avec adresse IP, configurez une ou plusieurs des options suivantes.

> **NOTE**
> La découverte du réseau est exécutée dans le contexte du compte d'ordinateur du serveur de site qui exécute la découverte. Si le compte d'ordinateur ne dispose pas d'autorisation sur un domaine non approuvé, les configurations du domaine et du serveur DHCP peuvent ne pas réussir à découvrir des ressources.

#### DHCP

Spécifiez chaque serveur DHCP que la découverte du réseau devra interroger. (La découverte du réseau prend en charge uniquement les serveurs DHCP qui exécutent l'implémentation Microsoft du protocole DHCP.)

- La découverte du réseau récupère les informations en émettant des appels de procédure distante vers la base de données sur le serveur DHCP.
- La découverte du réseau peut interroger des serveurs DHCP 32 bits et 64 bits pour une liste de périphériques qui sont enregistrés avec chaque serveur.
- Pour que la découverte du réseau interroge avec succès un serveur DHCP, le compte d'ordinateur du serveur qui exécute la découverte doit être membre du groupe d'utilisateurs DHCP sur le serveur DHCP. Par exemple, ce niveau d'accès existe quand l'une des affirmations suivantes est vraie :
  - Le serveur DHCP spécifié est le serveur DHCP du serveur qui exécute la découverte.
  - L'ordinateur qui exécute la découverte et le serveur DHCP se trouvent dans le même domaine.
  - Il existe une relation d'approbation bidirectionnelle entre l'ordinateur qui exécute la découverte et le serveur DHCP.
  - Le serveur de site est membre du groupe d'utilisateurs DHCP.
- Lorsque la découverte du réseau énumère un serveur DHCP, elle ne découvre pas toujours des adresses IP statiques. La découverte du réseau ne trouve pas d'adresses IP appartenant à une plage exclue d'adresses IP sur le serveur DHCP. Par ailleurs, elle ne découvre pas d'adresses IP réservées à l'attribution manuelle.

#### Domaines

Spécifiez chaque domaine que la découverte du réseau devra interroger.

- Le compte d'ordinateur du serveur de site qui exécute la découverte doit disposer d'autorisations pour lire les contrôleurs de domaine dans chaque domaine spécifié.
- Pour découvrir les ordinateurs du domaine local, vous devez activer le service du navigateur d'ordinateur sur au moins un ordinateur. Cet ordinateur doit se trouver sur le même sous-réseau que le serveur de site qui exécute la découverte du réseau.
- La découverte du réseau peut découvrir n'importe quel ordinateur que vous pouvez consulter à partir de votre serveur de site lorsque vous parcourez le réseau.
- La découverte du réseau récupère l'adresse IP. Elle utilise ensuite une demande d'écho ICMP (Internet Control Message Protocol) pour effectuer un test ping sur chaque appareil qu'elle trouve. La commande **ping** permet de déterminer quels ordinateurs sont actuellement actifs.

#### Unités SNMP

Spécifiez chaque unité SNMP que la découverte du réseau devra interroger.

- La découverte du réseau récupère la valeur ipNetToMediaTable depuis toute unité SNMP qui répond à la requête. Cette valeur retourne des groupes d'adresses IP qui sont des ordinateurs clients ou autres ressources, comme des imprimantes, des routeurs ou d'autres périphériques IP.
- Pour interroger un périphérique, vous devez spécifier l'adresse IP ou le nom NetBIOS du périphérique.

- Configurez la découverte du réseau de sorte qu'elle utilise le nom de communauté de l'appareil ; dans le cas contraire, l'appareil rejette la requête basée sur SNMP.

**Limitation de la découverte du réseau**

Quand la découverte du réseau interroge un appareil SNMP sur le bord de votre réseau, elle peut identifier des informations sur les sous-réseaux et les appareils SNMP qui sont en dehors de votre réseau immédiat. Utilisez les informations suivantes pour limiter la découverte du réseau en configurant les unités SNMP avec lesquelles la découverte peut communiquer et en spécifiant les segments réseau à interroger.

#### Sous-réseaux

Configurez les sous-réseaux que la découverte du réseau interroge lorsqu'elle utilise les options DHCP et SNMP. Ces deux options cherchent uniquement les sous-réseaux activés.

Par exemple, une requête DHCP peut renvoyer des périphériques à partir d'emplacements situés dans l'ensemble de votre réseau. Si vous souhaitez découvrir uniquement des périphériques situés sur un sous-réseau spécifique, spécifiez et activez ce sous-réseau spécifique sous l'onglet **Sous-réseaux** de la boîte de dialogue **Propriétés de la découverte du réseau**. Quand vous spécifiez et activez des sous-réseaux, vous limitez les futures tâches de découverte DHCP et SNMP à ces sous-réseaux.

> **NOTE**
> Les configurations de sous-réseau ne limitent pas les objets que l'option de découverte **Domaines** découvre.

#### Noms de communautés SNMP

Pour permettre à la découverte du réseau d'interroger avec succès un appareil SNMP, configurez la découverte du réseau avec le nom de communauté de l'appareil. Si la découverte du réseau n'est pas configurée à l'aide du nom de communauté du périphérique SNMP, le périphérique rejette la requête.

#### Nombre maximal de sauts

Lorsque vous configurez le nombre maximal de sauts de routeur, vous limitez le nombre de segments réseau et de routeurs que la découverte du réseau peut interroger à l'aide du protocole SNMP.

Le nombre de sauts que vous configurez limite le nombre de périphériques supplémentaires et de segments réseau que la découverte du réseau peut interroger.

Par exemple, une découverte pour la topologie uniquement avec **0** (zéro) saut de routeur découvre le sous-réseau sur lequel réside le serveur d'origine. Elle inclut tous les routeurs de ce sous-réseau.

Le diagramme suivant illustre le résultat d'une requête de découverte du réseau pour la topologie, uniquement quand elle est exécutée sur le serveur 1 avec 0 saut de routeur spécifié : sous-réseau D et routeur 1.

Le diagramme suivant illustre le résultat d'une requête de découverte du réseau pour la topologie et le client, quand elle est exécutée sur le serveur 1 avec 0 saut de routeur spécifié : sous-réseau D et routeur 1, ainsi que tous les clients potentiels du sous-réseau D.

Pour mieux comprendre comment les sauts de routeur supplémentaires peuvent augmenter la quantité de ressources réseau découvertes, prenez l'exemple de réseau suivant :

L'exécution d'une découverte du réseau pour la topologie uniquement à partir du serveur 1 avec un saut de routeur permet de découvrir les entités suivantes :

- Routeur 1 et sous-réseau 10.1.10.0 (détectés avec zéro saut)

- Sous-réseaux 10.1.20.0 et 10.1.30.0, sous-réseau A et routeur 2 (détectés sur le premier saut)

> **WARNING**
> Chaque augmentation du nombre de sauts de routeur peut considérablement augmenter le nombre de ressources à découvrir et augmenter la bande passante réseau utilisée par la découverte du réseau.

## Découverte de serveurs

**Configurable :** Non

Outre ces méthodes de découverte pouvant être configurées par l'utilisateur, Configuration Manager utilise un processus appelé **découverte de serveurs** (SMS_WINNT_SERVER_DISCOVERY_AGENT). Cette méthode de découverte crée des enregistrements de ressources pour les ordinateurs qui sont des systèmes de site, par exemple un ordinateur configuré comme point de gestion.

## Fonctionnalités communes de la découverte de groupes, de systèmes et d'utilisateurs Active Directory

Cette section fournit des informations sur les fonctionnalités qui sont communes aux méthodes de découverte suivantes :

- Découverte de groupes Active Directory
- Découverte de systèmes Active Directory
- Découverte d'utilisateurs Active Directory

> **NOTE**
> Les informations dans cette section ne s'appliquent pas à la découverte de forêts Active Directory.

Ces trois méthodes de découverte sont similaires au niveau de la configuration et du fonctionnement. Elles peuvent découvrir des ordinateurs, des utilisateurs et des informations sur les appartenances aux groupes des ressources qui sont stockées dans Active Directory Domain Services. Le processus de découverte est géré par un agent de découverte. L'agent s'exécute sur le serveur de site sur chaque site où l'exécution de la découverte est configurée. Vous pouvez configurer chacune de ces méthodes de découverte pour rechercher un ou plusieurs emplacements Active Directory en tant qu'instances d'emplacement dans la forêt locale ou dans les forêts distantes.

Lorsque la découverte recherche des ressources dans une forêt non approuvée, l'agent de découverte doit être en mesure de résoudre les éléments suivants pour fonctionner correctement :

- Pour découvrir une ressource d'ordinateur à l'aide de la découverte de systèmes Active Directory, l'agent de découverte doit pouvoir résoudre le nom de domaine complet de la ressource. Dans le cas contraire, il tente ensuite de résoudre la ressource par son nom NetBIOS.
- Pour découvrir une ressource d'utilisateur ou de groupe à l'aide de la découverte d'utilisateurs Active Directory ou de la découverte de groupes Active Directory, l'agent de découverte doit pouvoir résoudre le nom de domaine complet du contrôleur de domaine spécifié pour l'emplacement Active Directory.

Pour chaque emplacement que vous spécifiez, vous pouvez configurer des options de recherche individuelles, comme l'activation d'une recherche récursive des emplacements de conteneurs enfants Active Directory. Vous pouvez également configurer un compte unique à utiliser lors de la recherche de cet emplacement. Vous bénéficiez ainsi de flexibilité dans la configuration d'une méthode de découverte sur un site pour chercher à

plusieurs emplacements Active Directory dans plusieurs forêts. Vous n'avez pas à configurer un compte unique avec des autorisations sur tous les emplacements.

Quand l'une de ces trois méthodes de découverte s'exécute sur un site spécifique, le serveur de site Configuration Manager sur le site contacte le contrôleur de domaine le plus proche dans la forêt Active Directory spécifiée pour localiser les ressources Active Directory. Le domaine et la forêt peuvent être dans n'importe quel mode Active Directory pris en charge. Le compte que vous attribuez à chaque instance d'emplacement doit disposer de l'autorisation d'accès **Lecture** aux emplacements Active Directory spécifiés.

La découverte recherche des objets aux emplacements spécifiés, puis tente de recueillir des informations sur ces objets. Lorsque suffisamment d'informations sur une ressource sont identifiées, un enregistrement de données de découverte est créé. Les informations requises varient en fonction de la méthode de découverte utilisée.

Si vous configurez l'exécution d'une même méthode de découverte dans différents sites Configuration Manager pour tirer profit de l'interrogation des serveurs Active Directory locaux, vous pouvez configurer chaque site à l'aide d'un ensemble unique d'options de découverte. Étant donné que les données de découverte sont partagées avec chaque site de la hiérarchie, évitez la superposition entre ces configurations pour découvrir de manière efficace chaque ressource une seule fois.

Dans les environnements plus petits, envisagez d'exécuter chaque méthode de découverte sur un seul site dans votre hiérarchie. Cette configuration réduit les charges administratives supplémentaires et la possibilité de multiples actions de découverte redécouvrant les mêmes ressources. Quand vous limitez le nombre de sites exécutant des découvertes, vous réduisez la bande passante réseau globale utilisée par la découverte. Vous pouvez également réduire le nombre global de DDR qui sont créés et qui doivent être traités par vos serveurs de site.

De nombreuses configurations de méthode de découverte sont intuitives. Utilisez les sections suivantes pour en savoir plus sur les options de découverte qui requièrent plus d'informations préalables à la configuration.

Les options suivantes peuvent être utilisées avec plusieurs méthodes de découverte Active Directory :

- Découverte delta
- Filtrer les enregistrements d'ordinateurs obsolètes par connexion au domaine
- Filtrer les enregistrements obsolètes par mot de passe de l'ordinateur
- Rechercher les attributs Active Directory personnalisés

**Découverte delta**

Disponible pour :

- Découverte de groupes Active Directory
- Découverte de systèmes Active Directory
- Découverte d'utilisateurs Active Directory

La découverte delta n'est pas une méthode de découverte indépendante, mais une option disponible pour les méthodes de découverte applicables. La découverte delta recherche dans des attributs Active Directory spécifiques des modifications qui ont été apportées depuis le dernier cycle de découverte complète de la méthode de détection applicable. Les modifications d'attributs sont soumises à la base de données Configuration Manager pour mettre à jour l'enregistrement de découverte de la ressource.

Par défaut, la découverte delta s'exécute sur un cycle de cinq minutes. Autrement dit, elle a lieu beaucoup plus fréquemment qu'un cycle complet de découverte. Cette fréquence est possible car la découverte delta utilise moins de ressources de serveur de site et de ressources réseau qu'un cycle de découverte complète. Lorsque vous utilisez la découverte delta, vous pouvez réduire la fréquence du cycle de découverte complète pour cette méthode de découverte.

Les modifications les plus courantes détectées par la découverte delta sont les suivantes :

- Ajout de nouveaux ordinateurs ou utilisateurs à Active Directory
- Modifications des informations de base de l'ordinateur et de l'utilisateur
- Ajout de nouveaux ordinateurs ou utilisateurs à un groupe
- Suppression d'ordinateurs ou d'utilisateurs d'un groupe
- Modifications apportées aux objets de groupes de systèmes

Bien que la découverte delta puisse détecter de nouvelles ressources et des modifications de l'appartenance à un groupe, elle ne peut pas détecter qu'une ressource a été supprimée d'Active Directory. Les enregistrements de données de découverte (DDR) créés par la découverte delta sont traités de la même manière que les DDR qui sont créés par un cycle de découverte complète.

Vous configurez la découverte delta à partir de l'onglet **Calendrier d'interrogation** dans les propriétés de chaque méthode de découverte.

**Filtrer les enregistrements d'ordinateurs obsolètes par connexion au domaine**

Disponible pour :

- Découverte de groupes Active Directory
- Découverte de systèmes Active Directory

Vous pouvez configurer la découverte de manière à exclure les ordinateurs ayant un enregistrement d'ordinateur obsolète. Cette exclusion est basée sur la dernière connexion de l'ordinateur au domaine. Quand cette option est activée, la découverte de systèmes Active Directory évalue chaque ordinateur identifié. La découverte de groupes Active Directory évalue chaque ordinateur membre d'un groupe qui est découvert.

Pour utiliser cette option :

- Les ordinateurs doivent être configurés pour mettre à jour l'attribut **lastLogonTimeStamp** dans les services de domaine Active Directory.
- Le niveau fonctionnel du domaine Active Directory doit être défini sur Windows Server 2003 ou version ultérieure.

Quand vous configurez le délai entre la dernière connexion et l'utilisation de ce paramètre, prenez en compte l'intervalle de réplication entre les contrôleurs de domaine.

Configurez le filtrage sous l'onglet **Option** dans les boîtes de dialogue des **propriétés de découverte des systèmes Active Directory** et des **propriétés de découverte de groupes Active Directory**. Choisissez l'option **Découvrir uniquement les ordinateurs qui se sont connectés à un domaine pendant une période donnée**.

> **WARNING**
> Quand vous configurez ce filtre et **Filtrer les enregistrements obsolètes par mot de passe de l'ordinateur**, les ordinateurs qui répondent aux critères de l'un des filtres sont exclus de la découverte.

**Filtrer les enregistrements obsolètes par mot de passe de l'ordinateur**

Disponible pour :

- Découverte de groupes Active Directory
- Découverte de systèmes Active Directory

Vous pouvez configurer la découverte de manière à exclure les ordinateurs ayant un enregistrement d'ordinateur obsolète. Cette exclusion est basée sur la dernière mise à jour du mot de passe du compte d'ordinateur par l'ordinateur. Quand cette option est activée, la découverte de systèmes Active Directory évalue chaque ordinateur identifié. La découverte de groupes Active Directory évalue chaque ordinateur membre d'un groupe qui est découvert.

Pour utiliser cette option :

- Les ordinateurs doivent être configurés pour mettre à jour l'attribut **pwdLastSet** dans les services de domaine Active Directory.

Quand vous configurez cette option, prenez en compte l'intervalle pour les mises à jour de cet attribut en plus de l'intervalle de réplication entre les contrôleurs de domaine.

Configurez le filtrage sous l'onglet **Option** dans les boîtes de dialogue des **propriétés de découverte des systèmes Active Directory** et des **propriétés de découverte de groupes Active Directory**. Choisissez l'option **Découvrir uniquement les ordinateurs qui ont mis à jour le mot de passe de leur compte d'ordinateur pendant une période donnée**.

> **WARNING**
> Quand vous configurez ce filtre et **Filtrer les enregistrements obsolètes par connexion au domaine**, les ordinateurs qui répondent aux critères de l'un des filtres sont exclus de la découverte.

**Rechercher les attributs Active Directory personnalisés**

Disponible pour :

- Découverte de systèmes Active Directory
- Découverte d'utilisateurs Active Directory

Chaque méthode de découverte prend en charge une liste unique d'attributs Active Directory pouvant être découverts.

Vous pouvez afficher et configurer les liste des attributs personnalisés sous l'onglet **Attributs Active Directory** des boîtes de dialogue des **propriétés de découverte des systèmes Active Directory** et des **propriétés de découverte d'utilisateurs Active Directory**.

# Sélectionner des méthodes de découverte à utiliser pour System Center Configuration Manager

22/06/2018 • 20 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Pour utiliser correctement et efficacement la découverte pour System Center Configuration Manager, vous devez prendre en compte les méthodes à utiliser et les sites sur lesquels les exécuter.

La découverte peut générer un volume de trafic réseau considérable, et les enregistrements de données de découverte obtenus peuvent utiliser beaucoup de ressources du processeur pendant le traitement. Vous devez donc limiter l'utilisation des méthodes de découverte à celles qui sont nécessaires pour répondre à vos objectifs. Vous pouvez commencer par n'utiliser qu'une ou deux méthodes de découverte, avant d'éventuellement en activer d'autres de manière contrôlée par la suite pour étendre le niveau de découverte dans votre environnement. Les informations fournies dans cette rubrique peuvent vous aider à prendre des décisions éclairées.

Pour plus d'informations sur les différentes méthodes de découverte, consultez À propos des méthodes de découverte pour System Center Configuration Manager.

## Sélectionner des méthodes pour découvrir des choses différentes

Pour découvrir des ordinateurs clients Configuration Manager potentiels ou des ressources utilisateur, vous devez activer les méthodes de découverte appropriées. Vous pouvez utiliser différentes combinaisons de méthodes de découverte pour localiser différentes ressources et découvrir des informations supplémentaires sur ces ressources. Les méthodes employées déterminent le type de ressources découvertes, ainsi que les services et agents Configuration Manager utilisés dans le processus de découverte. Elles déterminent également le type d'informations concernant les ressources que vous pouvez découvrir.

**Détecter les ordinateurs**

Quand vous voulez découvrir des ordinateurs, vous pouvez utiliser la **Découverte de systèmes Active Directory** ou la **Découverte du réseau**.

Par exemple, si vous souhaitez découvrir des ressources qui peuvent installer le client Configuration Manager avant d'utiliser l'installation Push du client, vous pouvez exécuter la découverte de systèmes Active Directory. À l'aide de cette méthode, vous découvrez non seulement la ressource, mais aussi des informations de base, et même des informations étendues à partir des services de domaine Active Directory. Ces informations peuvent être utiles pour créer des requêtes et des regroupements complexes à utiliser dans l'attribution de paramètres de client ou le déploiement de contenu.

En guise d'alternative, vous pouvez exécuter la découverte du réseau et utiliser ses options pour découvrir le système d'exploitation des ressources (nécessaire pour utiliser l'installation Push du client ultérieurement). La découverte du réseau fournit des informations sur la topologie de votre réseau que vous ne pouvez pas obtenir avec d'autres méthodes de découverte. Toutefois, cette méthode ne fournit aucune information sur votre environnement Active Directory.

Il existe également une méthode appelée **Découverte par pulsations d'inventaire**. Il est possible d'utiliser uniquement la découverte par pulsations d'inventaire pour forcer la découverte des clients que vous avez installés à l'aide de méthodes autres que l'installation Push du client. Cependant, contrairement aux autres méthodes de découverte, la découverte par pulsations d'inventaire ne peut pas découvrir des ordinateurs qui ne disposent pas d'un client Configuration Manager actif. Elle retourne un ensemble limité d'informations, destinées à tenir à jour un enregistrement de base de données existant plutôt que la base de cet enregistrement. Les informations

soumises par la découverte par pulsations d'inventaire peuvent ne pas suffire à construire des requêtes ou des regroupements complexes.

Si vous utilisez la **découverte de groupes Active Directory** pour découvrir l'appartenance d'un groupe spécifique, vous pouvez découvrir des informations limitées sur le système ou l'ordinateur. Cela ne remplace pas une découverte complète des ordinateurs, mais peut fournir des informations de base. Ces informations sont insuffisantes pour l'installation Push du client.

**Découvrir des utilisateurs**

Quand vous voulez découvrir des informations sur les utilisateurs, utilisez la **Découverte d'utilisateurs Active Directory**. Comme pour la découverte de systèmes Active Directory, cette méthode découvre des utilisateurs d'Active Directory. Cela comprend les informations de base, en plus des informations étendues Active Directory. Vous pouvez utiliser ces informations pour générer des requêtes et des regroupements complexes similaires à ceux des ordinateurs.

**Découvrir des informations de groupe**

Quand vous voulez découvrir des informations sur les groupes et les appartenances aux groupes, utilisez la **Découverte de groupes Active Directory**. Cette méthode de découverte crée des enregistrements de ressources pour les groupes de sécurité.

Vous pouvez utiliser cette méthode pour rechercher un groupe spécifique d'Active Directory afin d'identifier les membres de ce groupe, ainsi que les groupes imbriqués dans ce groupe. Cette méthode permet également de rechercher des groupes dans un emplacement Active Directory et de rechercher, de manière récursive, chaque conteneur enfant de cet emplacement dans les services de domaine Active Directory.

Cette méthode de découverte peut également rechercher l'appartenance des groupes de distribution. Elle permet également d'identifier les relations de groupe des utilisateurs et des ordinateurs.

Lorsque vous découvrez un groupe, vous pouvez également découvrir des informations limitées sur ses membres. Toutefois, cela ne remplace pas les méthodes de découverte de systèmes ou d'utilisateurs Active Directory. Cela ne suffit généralement pas pour créer des requêtes et des regroupements complexes, ou pour servir de base d'une installation Push du client.

**Découvrir l'infrastructure**

Vous pouvez appliquer deux méthodes pour découvrir l'infrastructure réseau : la **Découverte de forêts Active Directory** et la **Découverte du réseau**.

Utilisez la découverte de forêts Active Directory pour rechercher des informations sur les sous-réseaux et les configurations de site Active Directory dans une forêt Active Directory. Ces configurations peuvent ensuite être automatiquement entrées dans Configuration Manager en tant qu'emplacements limites.

Lorsque vous souhaitez découvrir la topologie de votre réseau, utilisez la découverte du réseau. Les autres méthodes de découverte retournent des informations liées aux services de domaine Active Directory et peuvent identifier l'emplacement réseau actuel d'un client, mais elles ne peuvent pas fournir d'informations d'infrastructure basées sur la topologie des sous-réseaux ou du routeur de votre réseau.

## Les données de découverte sont partagées entre les sites

Une fois que Configuration Manager a ajouté des données de découverte à une base de données, elles sont rapidement partagées parmi tous les sites de la hiérarchie. Comme il n'y a généralement pas d'avantage à découvrir les mêmes informations sur plusieurs sites de votre hiérarchie, il peut être judicieux de configurer une seule instance de chaque méthode de découverte que vous utilisez, pour qu'elle s'exécute sur un seul site. Cela vaut mieux que d'exécuter plusieurs instances d'une seule méthode sur différents sites.

Il peut toutefois être utile, pour certains environnements, d'attribuer la même méthode de découverte à plusieurs sites, avec une configuration et une planification distinctes à chaque fois. Par exemple, quand vous utilisez la

découverte du réseau, vous souhaiterez peut-être diriger chaque site pour découvrir son réseau local, au lieu d'essayer de découvrir tous les emplacements réseau sur un réseau WAN.

Si vous configurez plusieurs instances des mêmes méthodes de découverte pour qu'elles s'exécutent sur différents sites, planifiez soigneusement la configuration de chaque site. Il faut éviter que plusieurs sites découvrent les mêmes ressources de votre réseau ou d'Active Directory. Cela peut consommer de la bande passante réseau supplémentaire et créer des enregistrements DDR en double.

Le tableau suivant identifie sur quels sites vous pouvez configurer les différentes méthodes de découverte.

| MÉTHODE DE DÉCOUVERTE | EMPLACEMENTS PRIS EN CHARGE |
|---|---|
| Découverte de forêts Active Directory | Site d'administration centrale<br><br>Site principal |
| Découverte de groupes Active Directory | Site principal |
| Découverte de systèmes Active Directory | Site principal |
| Découverte d'utilisateurs Active Directory | Site principal |
| Découverte par pulsations d'inventaire[1] | Site principal |
| Découverte du réseau | Site principal<br><br>Site secondaire |

[1] Les sites secondaires ne peuvent pas configurer la découverte par pulsations d'inventaire, mais peuvent recevoir l'enregistrement de données de découverte par pulsation de la part d'un client.

Lorsque des sites secondaires exécutent la découverte du réseau, ou reçoivent des DDR de découverte par pulsations d'inventaire, ils transfèrent le DDR par réplication basée sur les fichiers vers leur site principal parent. Ceci est dû au fait que seuls les sites principaux et les sites d'administration centrale peuvent traiter les enregistrements de données de découverte. Pour plus d'informations sur le traitement des enregistrements de données de découverte, consultez À propos des enregistrements de données de découverte.

## Éléments à prendre en compte pour différentes méthodes de découverte

Chaque environnement réseau et de serveur de site étant différent, il est préférable de limiter vos configurations initiales pour la découverte. Ensuite, surveillez attentivement la capacité de chaque serveur de site à traiter les données de découverte générées.

Quand vous utilisez une méthode de découverte **Active Directory** pour les systèmes, les utilisateurs ou les groupes :

- Exécutez la découverte sur un site qui dispose d'une connexion réseau rapide pour vos contrôleurs de domaine.
- Pensez à la topologie de réplication Active Directory pour vous assurer que la découverte peut accéder aux informations les plus récentes.
- Pensez à l'étendue de la configuration de la découverte et limitez la découverte aux emplacements et groupes Active Directory que vous souhaitez découvrir.

Si vous utilisez la **Découverte du réseau** :

- Utilisez une configuration initiale limitée pour identifier votre topographie réseau.
- Après avoir identifié votre topographie réseau, configurez la découverte du réseau pour qu'elle s'exécute sur des sites spécifiques, qui jouent un rôle central pour les zones du réseau que vous souhaitez découvrir plus en détail.

Dans la mesure où la **Découverte par pulsations d'inventaire** ne s'exécute pas sur un site spécifique, vous n'avez pas besoin de prendre en compte le lieu de l'exécution dans la planification générale.

## Bonnes pratiques pour la découverte

Pour obtenir de meilleurs résultats avec la découverte, nous vous recommandons d'effectuer les opérations suivantes :

- **Réalisez une découverte de systèmes Active Directory et une découverte d'utilisateurs Active Directory avant de procéder à une découverte de groupes Active Directory.**

  Lorsqu'une découverte de groupes Active Directory identifie en tant que membre d'un groupe un ordinateur ou un utilisateur jusqu'alors inconnu, elle tente de découvrir les détails de base concernant cet utilisateur ou cet ordinateur. La découverte de groupes Active Directory n'étant pas optimisée pour ce type de découverte, ce processus peut provoquer un ralentissement de son exécution. Par ailleurs, la découverte de groupes Active Directory identifie uniquement les informations de base sur les utilisateurs et les ordinateurs, et ne crée pas d'enregistrement complet de découverte d'utilisateurs ou d'ordinateurs. Quand vous procédez à une découverte de systèmes Active Directory et à une découverte d'utilisateurs Active Directory, les attributs Active Directory supplémentaires de chaque type d'objet sont disponibles. Ainsi, la découverte de groupes Active Directory est plus performante.

- **Quand vous configurez la découverte de groupes Active Directory, spécifiez uniquement les groupes que vous utilisez avec Configuration Manager.**

  Pour mieux contrôler les ressources utilisées par le processus de découverte de groupes Active Directory, spécifiez uniquement les groupes que vous utilisez avec Configuration Manager. En effet, la découverte de groupes Active Directory recherche de manière récursive les utilisateurs, les ordinateurs et les groupes imbriqués dans chaque groupe qu'elle découvre. La recherche dans chaque groupe imbriqué peut élargir l'étendue de la découverte de groupes Active Directory et réduire les performances. En outre, quand vous configurez la découverte delta pour la découverte de groupes Active Directory, la méthode de découverte surveille les modifications apportées à chaque groupe. Les performances sont ainsi d'autant plus ralenties lorsque la méthode doit rechercher des groupes qui ne sont pas nécessaires.

- **Configurez les méthodes de découverte de telle sorte que l'intervalle entre les découvertes complètes soit plus long et que les découvertes delta soient plus fréquentes.**

  La découverte delta consomme moins de ressources qu'un cycle de découverte complète et peut identifier les ressources nouvelles ou modifiées dans Active Directory. Ainsi, vous pouvez réduire la fréquence des cycles de découverte complète à un par semaine (ou moins). La découverte delta de la découverte de systèmes Active Directory, de la découverte d'utilisateurs Active Directory et de la découverte de groupes Active Directory identifie presque toutes les modifications apportées aux objets Active Directory, et peut conserver des données de découverte exactes concernant les ressources.

- **Exécutez les méthodes de découverte Active Directory sur le site principal dont l'emplacement réseau est le plus proche de votre contrôleur de domaine Active Directory.**

  Pour améliorer les performances de la découverte Active Directory, nous vous recommandons de l'exécuter sur un site principal connecté aux contrôleurs de domaine via une connexion réseau rapide. Si vous exécutez la même méthode de découverte Active Directory sur plusieurs sites, configurez chaque méthode de découverte pour éviter les chevauchements. Contrairement aux versions antérieures de Configuration

Manager, les données de découverte sont partagées parmi les sites. Ainsi, il n'est pas nécessaire de procéder à la découverte des mêmes informations sur plusieurs sites. Pour plus d'informations, consultez Les données de découverte sont partagées entre les sites.

- **Procédez à une découverte de forêts Active Directory sur un seul site quand vous envisagez de créer automatiquement des limites à partir des données de découverte.**

  Si vous effectuez une découverte de forêts Active Directory sur plusieurs sites d'une hiérarchie, nous vous recommandons d'activer les options permettant de créer automatiquement des limites uniquement sur un site. En effet, lorsqu'une découverte de forêts Active Directory est réalisée sur chaque site et crée des limites, Configuration Manager ne peut pas fusionner ces limites en un objet de limite unique. Si vous configurez la découverte de forêts Active Directory de façon à ce qu'elle crée automatiquement des limites sur plusieurs sites, vous risquez de créer des objets de limite en double dans la console Configuration Manager.

# Configurer les méthodes de découverte pour System Center Configuration Manager

22/06/2018 • 45 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Configurez des méthodes de découverte pour trouver des ressources à gérer à partir de votre réseau, d'Active Directory et d'Azure Active Directory (Azure AD). Commencez par activer et configurer chaque méthode à utiliser pour explorer votre environnement. Vous pouvez aussi désactiver une méthode en suivant la même procédure que pour l'activer. La découverte par pulsations d'inventaire et la découverte de serveurs constituent les seules exceptions à ce processus :

- Par défaut, la **découverte par pulsations d'inventaire** est déjà activée au moment où vous installez un site principal Configuration Manager. Elle est configurée pour s'exécuter selon une planification de base. Maintenez la découverte par pulsations d'inventaire activée, car cette méthode garantit que les enregistrements de données de découverte (DDR) pour les appareils sont à jour. Pour plus d'informations sur la découverte par pulsations d'inventaire, consultez Découverte par pulsations d'inventaire.
- La **découverte de serveurs** est une méthode de découverte automatique. Elle recherche les ordinateurs que vous utilisez comme systèmes de site. Elle n'est ni configurable ni désactivable.

**Activer une méthode de découverte configurable**

> **NOTE**
> Les informations suivantes ne s'appliquent pas à la découverte d'utilisateurs Azure AD. Consultez plutôt Configurer la découverte d'utilisateurs Azure AD plus loin dans cet article.

1. Dans la console Configuration Manager, accédez à l'espace de travail **Administration**, développez **Configuration de la hiérarchie**, puis sélectionnez **Méthodes de découverte**.
2. Sélectionnez la méthode de découverte pour le site sur lequel vous voulez activer la découverte.
3. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**. Ensuite, sous l'onglet **Général**, cochez la case **Enable <discovery method>** (Activer la méthode de découverte).

   Si cette case à cocher est déjà activée, vous pouvez la désélectionner pour désactiver la méthode de découverte.
4. Choisissez **OK** pour enregistrer la configuration.

## Configurer la découverte de forêts Active Directory

Pour finaliser la configuration de la découverte des forêts Active Directory, vous devez configurer des paramètres dans deux emplacements :

- Dans le nœud **Méthodes de découverte**, vous pouvez :
  - Activer cette méthode de découverte.
  - Définir un calendrier d'interrogation.
  - Indiquez si la découverte doit créer automatiquement des limites pour les sites Active Directory et les sous-réseaux qui sont découverts.

- Dans le nœud **Forêts Active Directory**, vous pouvez :
  - Ajouter les forêts à découvrir.
  - Activer la découverte des sites et sous-réseaux Active Directory dans cette forêt.
  - Configurer les paramètres permettant aux sites Configuration Manager de publier leurs informations de site dans la forêt.
  - Attribuer un compte à utiliser comme compte de forêt Active Directory pour chaque forêt.

Utilisez les procédures suivantes pour activer la découverte de forêts Active Directory et configurer chaque forêt à utiliser avec la découverte de forêts Active Directory.

**Pour activer la découverte de forêts Active Directory**

1. Dans la console Configuration Manager, choisissez **Administration** > **Configuration de la hiérarchie**, puis **Méthodes de découverte**.
2. Sélectionnez la méthode Découverte de forêts Active Directory pour le site sur lequel vous voulez configurer la découverte.
3. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
4. Dans l'onglet **Général**, activez la case à cocher pour activer la découverte. Vous pouvez aussi configurer la découverte maintenant et l'activer ultérieurement.
5. Spécifiez les options nécessaires pour créer des limites de site des emplacements découverts.
6. Spécifiez une planification du moment d'exécution de la découverte.
7. Après avoir terminé la configuration de la découverte de forêts Active Directory pour ce site, choisissez **OK** pour enregistrer la configuration.

**Pour configurer une forêt pour la découverte de forêts Active Directory**

1. Dans l'espace de travail **Administration**, choisissez **Forêts Active Directory**. Si la découverte de forêts Active Directory a été exécutée précédemment, vous pouvez voir chaque forêt découverte dans le volet des résultats. La forêt locale et toutes les forêts approuvées sont découvertes lorsque la Découverte de forêts Active Directory s'exécute. Seules les forêts non approuvées doivent être ajoutées manuellement.
   - Pour configurer une forêt déjà découverte, sélectionnez-la dans le volet de résultats. Ensuite, dans l'onglet **Accueil** et dans le groupe **Propriétés**, choisissez **Propriétés** pour ouvrir les propriétés de la forêt. Passez à l'étape 3.
   - Pour configurer une nouvelle forêt non répertoriée, dans l'onglet **Accueil** et dans le groupe **Créer**, choisissez **Ajouter une forêt** pour ouvrir la boîte de dialogue **Ajouter une forêt**. Passez à l'étape 3.
2. Dans l'onglet **Général**, finalisez la configuration de forêt que vous souhaitez découvrir et spécifiez le **Compte de forêt Active Directory**.

   > **NOTE**
   > La découverte de forêts Active Directory requiert un compte global pour découvrir et publier les forêts non approuvées. Si vous n'utilisez pas le compte d'ordinateur du serveur de site, vous ne pouvez sélectionner qu'un compte global.

3. Si vous prévoyez d'autoriser des sites à publier des données de site dans cette forêt, dans l'onglet **Publication**, terminez la configuration de la publication dans cette forêt.

> **NOTE**
> Si vous autorisez les sites à publier dans une forêt, vous devez étendre le schéma Active Directory de cette forêt à Configuration Manager. Le compte de forêt Active Directory doit avoir des autorisations Contrôle total sur le conteneur système dans cette forêt.

4. Lorsque vous terminez la configuration de cette forêt à utiliser avec la Découverte de forêts Active Directory, choisissez **OK** pour enregistrer la configuration.

## Configurer la découverte Active Directory pour les ordinateurs, les utilisateurs ou les groupes

Pour configurer la découverte des ordinateurs, utilisateurs ou groupes, utilisez les informations de ces sections pour les méthodes de découverte ci-après :

- Découverte de groupes Active Directory
- Découverte de systèmes Active Directory
- Découverte d'utilisateurs Active Directory

> **NOTE**
> Les informations dans cette section ne s'appliquent pas à la découverte de forêts Active Directory.

Bien qu'indépendantes, ces méthodes de découverte partagent des options similaires. Pour plus d'informations sur ces options de configuration, consultez Options partagées pour la découverte des groupes, systèmes et utilisateurs.

> **WARNING**
> Le processus d'interrogation Active Directory par chacune de ces méthodes de découverte peut entraîner un trafic réseau important. Pensez à planifier l'exécution de chaque méthode de découverte à des moments où ce trafic ne risque pas de nuire à l'usage commercial de votre réseau.

**Pour configurer la découverte de groupes Active Directory**

1. Dans la console Configuration Manager, choisissez **Administration** > **Configuration de la hiérarchie**, puis **Méthodes de découverte**.
2. Sélectionnez la méthode **Découverte de groupes Active Directory** pour le site sur lequel vous voulez configurer la découverte.
3. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
4. Dans l'onglet **Général**, activez la case à cocher pour activer la découverte. Vous pouvez aussi configurer la découverte maintenant et l'activer ultérieurement.
5. Choisissez **Ajouter** pour configurer une étendue de découverte, sélectionnez **Groupes** ou **Emplacement**, puis terminez les configurations suivantes dans la boîte de dialogue **Ajouter des groupes** ou **Ajouter un emplacement Active Directory** :
   a. Spécifiez un **Nom** pour cette étendue de découverte.
   b. Spécifiez un **Domaine Active Directory** ou un **Emplacement** à rechercher :
      - Si vous avez choisi **Groupes**, spécifiez un ou plusieurs groupes Active Directory à découvrir.

- Si vous avez choisi **Emplacement**, spécifiez un conteneur Active Directory comme emplacement à découvrir. Vous pouvez également activer une recherche récursive des conteneurs enfants Active Directory pour cet emplacement.

c. Spécifiez le **Compte de découverte de groupes Active Directory** utilisé pour rechercher cette étendue de découverte.

d. Choisissez **OK** pour enregistrer la configuration de l'étendue de découverte.

6. Répétez l'étape 6 pour chaque étendue de découverte supplémentaire à définir.

7. Dans l'onglet **Calendrier d'interrogation** , configurez le calendrier d'interrogation de découverte complet et la découverte delta.

8. Le cas échéant, sous l'onglet **Option**, configurez des options pour filtrer ou exclure les enregistrements d'ordinateur obsolètes de la découverte. Configurez également la découverte de l'appartenance des groupes de distribution.

> **NOTE**
> Par défaut, le processus de découverte de groupes Active Directory ne découvre que l'appartenance aux groupes de sécurité.

9. Après avoir terminé la configuration de la découverte des groupes Active Directory, choisissez **OK** pour enregistrer la configuration.

**Pour configurer la découverte de systèmes Active Directory**

1. Dans la console Configuration Manager, choisissez **Administration** > **Configuration de la hiérarchie**, puis **Méthodes de découverte**.

2. Sélectionnez la méthode pour le site sur lequel vous voulez configurer la découverte.

3. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.

4. Dans l'onglet **Général**, activez la case à cocher pour activer la découverte. Vous pouvez aussi configurer la découverte maintenant et l'activer ultérieurement.

5. Choisissez l'icône **Nouveau** pour spécifier un nouveau conteneur Active Directory. Dans la boîte de dialogue **Conteneur Active Directory**, finalisez les configurations suivantes :

a. Spécifiez un ou plusieurs emplacements à rechercher.

b. Pour chaque emplacement, spécifiez les options qui modifient le comportement de la recherche.

c. Pour chaque emplacement, spécifiez le compte à utiliser en tant que **Compte de découverte Active Directory**.

> **TIP**
> Pour chaque emplacement spécifié, vous pouvez configurer un ensemble d'options de découverte et un compte de découverte Active Directory unique.

d. Choisissez **OK** pour enregistrer la configuration du conteneur Active Directory.

6. Dans l'onglet **Calendrier d'interrogation** , configurez le calendrier d'interrogation de découverte complet et la découverte delta.

7. Le cas échéant, dans l'onglet **Attributs Active Directory** , vous pouvez configurer des attributs Active

Directory supplémentaires pour les ordinateurs à découvrir. Les attributs d'objets par défaut sont également répertoriés.

> **TIP**
> Par exemple, votre organisation utilise l'attribut **Description** sur le compte d'ordinateur dans Active Directory. Cliquez sur **Personnalisé**et ajoutez `Description` comme attribut personnalisé. Une fois que cette méthode de découverte s'exécute, cet attribut s'affiche sous l'onglet Propriétés de l'appareil dans la console Configuration Manager.

8. Le cas échéant, dans l'onglet **Option**, vous pouvez configurer des options pour filtrer ou exclure les enregistrements d'ordinateur obsolètes de la découverte.
9. Après avoir terminé la configuration de la découverte de systèmes Active Directory pour ce site, choisissez **OK** pour enregistrer la configuration.

**Pour configurer la découverte d'utilisateurs Active Directory**

1. Dans la console Configuration Manager, choisissez **Administration** > **Configuration de la hiérarchie**, puis **Méthodes de découverte**.
2. Choisissez la méthode **Découverte d'utilisateurs Active Directory** pour le site sur lequel vous voulez configurer la découverte.
3. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
4. Dans l'onglet **Général**, activez la case à cocher pour activer la découverte. Vous pouvez aussi configurer la découverte maintenant et l'activer ultérieurement.
5. Choisissez l'icône **Nouveau** pour spécifier un nouveau conteneur Active Directory. Dans la boîte de dialogue **Conteneur Active Directory**, finalisez les configurations suivantes :
   a. Spécifiez un ou plusieurs emplacements à rechercher.
   b. Pour chaque emplacement, spécifiez les options qui modifient le comportement de la recherche.
   c. Pour chaque emplacement, spécifiez le compte à utiliser en tant que **Compte de découverte Active Directory**.

      > **NOTE**
      > Pour chaque emplacement spécifié, vous pouvez configurer un ensemble d'options de découverte et un compte de découverte Active Directory uniques.

   d. Choisissez **OK** pour enregistrer la configuration du conteneur Active Directory.
6. Dans l'onglet **Calendrier d'interrogation** , configurez le calendrier d'interrogation de découverte complet et la découverte delta.
7. Le cas échéant, dans l'onglet **Attributs Active Directory** , vous pouvez configurer des attributs Active Directory supplémentaires pour les ordinateurs à découvrir. Les attributs d'objets par défaut sont également répertoriés.
8. Après avoir terminé la configuration de la découverte d'utilisateurs Active Directory, choisissez **OK** pour enregistrer la configuration.

## Configurer la découverte des utilisateurs Azure AD

La découverte d'utilisateurs Azure AD n'est pas activée ni configurée de la même façon que d'autres méthodes de

découverte. Configurez-la quand vous intégrez le site Configuration Manager à Azure AD. Quand vous configurez les services Azure pour la **gestion cloud**, vous pouvez également activer et configurer cette méthode de découverte.

Lors de la configuration du service Azure de **gestion cloud** :

- Dans la page **Découverte** de l'Assistant, cliquez sur **Activer la découverte d'utilisateurs Azure Active Directory**.
- Cliquez sur **Paramètres**.
- Dans la boîte de dialogue Paramètres de découverte d'utilisateurs Azure AD, configurez une planification pour déterminer quand la découverte survient. Vous pouvez également activer la découverte delta, qui vérifie uniquement les comptes nouveaux ou modifiés dans Azure AD.

Pour plus d'informations, consultez Découverte d'utilisateurs Azure AD.

> **IMPORTANT**
> Avant *d'importer* l'application Azure AD dans Configuration Manager, vous devez accorder l'autorisation d'application serveur pour lire les données d'annuaire Azure AD.
>
> - Dans le portail Azure, accédez au panneau **Azure Active Directory**.
> - Cliquez sur **Inscriptions des applications**, puis basculez vers **Toutes les applications** si nécessaire.
> - Sélectionnez l'application serveur de type *Application/API web*, puis cliquez sur **Paramètres**.
> - Cliquez sur **Autorisations nécessaires**, puis sur **Accorder des autorisations**.
>
> Si vous *créez* l'application serveur à partir de Configuration Manager, Azure AD crée automatiquement les autorisations avec l'application. Vous devez néanmoins donner votre consentement à l'application dans le portail Azure.

> **NOTE**
> Si l'utilisateur est une identité fédérée ou synchronisée, vous devez utiliser la découverte d'utilisateurs Active Directory de Configuration Manager ainsi que la découverte d'utilisateurs Azure AD. Pour plus d'informations sur les identités hybrides, consultez Définir une stratégie d'adoption des identités hybrides.

## Configurer la découverte par pulsations d'inventaire

Par défaut, la découverte par pulsations d'inventaire est activée au moment où vous installez un site principal Configuration Manager. Par conséquent, il vous suffit de configurer la fréquence selon laquelle les clients envoient l'enregistrement des données de la découverte par pulsations d'inventaire à un point de gestion, si vous ne voulez pas utiliser la valeur par défaut (tous les sept jours).

> **NOTE**
> Si la tâche d'installation poussée du client et la tâche de maintenance de site pour **Remettre à zéro l'indicateur d'installation** sont activées sur le même site, définissez la planification de la découverte par pulsations d'inventaire à une valeur inférieure à la **Période de redécouverte client** de la tâche de maintenance de site **Remettre à zéro l'indicateur d'installation** . Pour plus d'informations sur les tâches de maintenance de site, consultez Tâches de maintenance pour System Center Configuration Manager.

**Pour configurer la planification de découverte par pulsations d'inventaire**

1. Dans la console Configuration Manager, choisissez **Administration** > **Configuration de la hiérarchie**, puis **Méthodes de découverte**.
2. Sélectionnez **Découverte par pulsations d'inventaire** pour le site sur lequel vous souhaitez exécuter la

découverte par pulsations d'inventaire.

3. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
4. Configurez la fréquence de l'envoi d'un enregistrement de données de découverte par pulsations d'inventaire par les clients, puis choisissez **OK** pour enregistrer la configuration.

# Configurer la découverte du réseau

Pour configurer la découverte du réseau, utilisez les informations dans les sections suivantes.

### À propos de la configuration de la découverte du réseau

Avant de configurer la découverte du réseau, vous devez comprendre les sujets suivants :

- Niveaux disponibles de découverte du réseau
- Options disponibles de découverte du réseau
- Limitation de la découverte du réseau sur le réseau

Pour plus d'informations, consultez la section Découverte du réseau.

Les sections suivantes fournissent des informations sur les configurations courantes pour la découverte du réseau. Vous pouvez configurer une ou plusieurs de ces configurations pour l'utilisation pendant la même exécution de la découverte. Si vous utilisez plusieurs configurations, vous devez tenir compte des interactions pouvant affecter les résultats de la découverte.

Vous pouvez, par exemple, vouloir découvrir tous les appareils SNMP (Simple Network Management Protocol) qui utilisent un nom de communauté SNMP spécifique. De plus, vous pouvez désactiver la découverte sur un sous-réseau spécifique pour la même exécution de la découverte. Lors de l'exécution de la découverte, la découverte du réseau ne découvre pas les unités SNMP avec le nom de communauté spécifié sur le sous-réseau que vous avez désactivé.

#### Déterminer la topologie de votre réseau

La découverte pour la topologie uniquement vous permet de mapper votre réseau. Ce type de découverte ne découvre pas les clients potentiels. La découverte du réseau pour la topologie uniquement s'appuie sur SNMP.

Lors du mappage de la topologie de votre réseau, vous devez configurer le **Nombre maximal de sauts** dans l'onglet **SNMP** de la boîte de dialogue **Propriétés de la découverte du réseau**. Quelques sauts permettent de contrôler la bande passante du réseau utilisée lors de l'exécution de la découverte. À mesure que vous découvrez votre réseau, vous pouvez augmenter le nombre de sauts pour mieux comprendre la topologie de votre réseau.

Une fois que vous avez compris la topologie de votre réseau, vous pouvez configurer des propriétés supplémentaires permettant à la découverte du réseau de découvrir des clients potentiels et leurs systèmes d'exploitation, pendant que vous utilisez les configurations disponibles pour limiter le nombre de segments réseau dans lesquels la découverte du réseau peut effectuer des recherches.

#### Limiter les recherches en utilisant des sous-réseaux

Vous pouvez configurer la découverte du réseau pour rechercher des sous-réseaux spécifiques au cours d'une opération de découverte. Par défaut, la découverte du réseau recherche le sous-réseau du serveur qui exécute la découverte. Tous les sous-réseaux supplémentaires que vous configurez et activez ne s'appliquent qu'aux options de recherche SNMP et DHCP (Dynamic Host Configuration Protocol). Quand la découverte du réseau effectue des recherches dans des domaines, elle n'est pas limitée par les configurations des sous-réseaux.

Si vous spécifiez un ou plusieurs sous-réseaux dans l'onglet **Sous-réseaux** de la boîte de dialogue **Propriétés de la découverte du réseau** , la recherche s'applique uniquement aux sous-réseaux marqués **Activé** .

Quand vous désactivez un sous-réseau, il est exclu de la découverte, et les conditions suivantes s'appliquent :

- Les requêtes SNMP ne s'exécutent pas sur le sous-réseau.
- Les serveurs DHCP ne renvoient pas une liste des ressources situées sur le sous-réseau.
- Les requêtes basées sur le domaine peuvent découvrir des ressources situées sur le sous-réseau.

#### Rechercher dans un domaine spécifique

La découverte du réseau peut être configurée pour rechercher dans un domaine spécifique ou dans plusieurs domaines au cours d'une opération de découverte. Par défaut, la découverte du réseau recherche dans le domaine local du serveur qui exécute la découverte.

Si vous spécifiez un ou plusieurs domaines sous l'onglet **Domaines** de la boîte de dialogue **Propriétés de la découverte du réseau**, la recherche s'applique uniquement aux domaines marqués **Activé**.

Quand vous désactivez un domaine, il est exclu de la découverte, et les conditions suivantes s'appliquent :

- La découverte du réseau n'interroge pas les contrôleurs de domaine situés dans ce domaine.
- Les requêtes SNMP s'exécutent sur les sous-réseaux du domaine.
- Les serveurs DHCP renvoient toujours une liste des ressources situées dans le domaine.

#### Limiter les recherches en utilisant des noms de communautés SNMP

La découverte du réseau peut être configurée pour rechercher une communauté SNMP spécifique ou plusieurs communautés au cours d'une opération de découverte. Par défaut, le nom de communauté dit **Public** est configuré pour l'utilisation.

La fonction de découverte du réseau utilise des noms de communautés pour accéder à des routeurs qui constituent des périphériques SNMP. Un routeur permet d'informer le service de découverte du réseau sur les autres routeurs et les sous-réseaux liés au premier routeur.

> **NOTE**
> Les noms de communautés SNMP sont semblables aux mots de passe. Le service de découverte du réseau peut uniquement obtenir des informations d'une unité SNMP pour laquelle vous avez spécifié un nom de communauté. Chaque périphérique SNMP peut disposer de son propre nom de communauté mais souvent, plusieurs périphériques partagent le même nom de communauté. En outre, la plupart des périphériques SNMP disposent d'un nom de communauté par défaut dit **Public**. Toutefois, certaines organisations suppriment le nom de communauté **Public** de leurs appareils pour des raisons de sécurité.

Si plusieurs communautés SNMP s'affichent sous l'onglet **SNMP** de la boîte de dialogue **Propriétés de la découverte du réseau**, les recherches effectuées par la découverte du réseau s'effectuent dans l'ordre d'affichage des communautés. Afin de réduire l'impact sur le trafic réseau généré par les tentatives de contact avec un périphérique en utilisant différents noms, assurez-vous que les noms les plus fréquemment utilisés sont en haut de la liste.

> **NOTE**
> Outre le nom de communauté SNMP, vous pouvez spécifier l'adresse IP ou le nom pouvant être résolu d'une unité SNMP. Pour ce faire, utilisez l'onglet **Unités SNMP** de la boîte de dialogue **Propriétés de la découverte du réseau**.

#### Rechercher sur un serveur DHCP spécifique

La découverte du réseau peut être configurée pour utiliser un serveur DHCP spécifique ou plusieurs serveurs en vue de découvrir des clients DHCP au cours d'une opération de découverte.

La découverte du réseau recherche sur chaque serveur DHCP que vous spécifiez sous l'onglet **DHCP** de la boîte de dialogue **Propriétés de la découverte du réseau**. Si le serveur qui exécute la découverte loue son adresse IP à un serveur DHCP, vous pouvez configurer la découverte pour qu'elle effectue la recherche sur ce serveur DHCP

en activant la case à cocher **Inclure le serveur DHCP pour lequel le serveur de site est configuré**.

> **NOTE**
> Pour configurer avec succès un serveur DHCP dans la découverte du réseau, votre environnement doit prendre en charge IPv4. Vous ne pouvez pas configurer la découverte du réseau de sorte qu'elle utilise un serveur DHCP dans un environnement IPv6 natif.

### Guide pratique pour configurer la découverte du réseau

Procédez comme suit pour d'abord découvrir uniquement la topologie de votre réseau, puis configurer la découverte du réseau afin de découvrir des clients potentiels à l'aide de l'une ou de plusieurs options disponibles de découverte du réseau.

#### Pour déterminer la topologie de votre réseau

1. Dans la console Configuration Manager, choisissez **Administration** > **Configuration de la hiérarchie**, puis **Méthodes de découverte**.
2. Choisissez **Découverte du réseau** pour le site sur lequel vous souhaitez exécuter la découverte du réseau.
3. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
   - Dans l'onglet **Général**, activez la case à cocher **Activer la découverte du réseau**, puis choisissez **Topologie** dans **Type de découverte**.
   - Dans l'onglet **Sous-réseaux**, activez la case à cocher **Rechercher les sous-réseaux locaux**.

     > **TIP**
     > Si vous connaissez les sous-réseaux qui constituent votre réseau, décochez la case **Rechercher les sous-réseaux locaux**. Utilisez ensuite l'icône **Nouveau** pour ajouter les sous-réseaux dans lesquels effectuer des recherches. Pour les réseaux de grande taille, il est souvent préférable d'effectuer la recherche uniquement dans un ou deux sous-réseaux à la fois, afin de minimiser l'utilisation de la bande passante du réseau.

   - Dans l'onglet **Domaines**, activez la case à cocher **Rechercher dans le domaine local**.
   - Dans l'onglet **SNMP** , utilisez la liste déroulante **Nombre maximal de sauts** pour déterminer le nombre de sauts de routeur que la découverte du réseau doit effectuer lors du mappage de votre topologie.

     > **TIP**
     > Lorsque vous mappez la topologie de votre réseau pour la première fois, configurez quelques sauts de routeur pour réduire l'utilisation de la bande passante du réseau.

4. Dans l'onglet **Calendrier**, choisissez l'icône **Nouveau** pour définir le calendrier d'exécution de la découverte du réseau.

   > **NOTE**
   > Vous ne pouvez pas attribuer une configuration de découverte différente à des planifications de découverte du réseau distinctes. La découverte du réseau utilise la configuration de découverte en cours à chaque exécution.

5. Choisissez **OK** pour accepter la configuration. La découverte du réseau s'exécute à l'heure planifiée.

#### Pour configurer la découverte du réseau

1. Dans la console Configuration Manager, choisissez **Administration** > **Configuration de la hiérarchie**, puis **Méthodes de découverte**.
2. Choisissez **Découverte du réseau** pour le site sur lequel vous souhaitez exécuter la découverte du réseau.
3. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
4. Dans l'onglet **Général**, activez la case à cocher **Activer la découverte du réseau**, puis sélectionnez le type de découverte à exécuter dans **Type de découverte**.
5. Pour configurer la découverte afin de rechercher les sous-réseaux, cliquez sur l'onglet **Sous-réseaux**, puis configurez une ou plusieurs des options suivantes :
   - Pour lancer la découverte sur les sous-réseaux locaux de l'ordinateur exécutant la découverte, activez la case à cocher **Rechercher les sous-réseaux locaux**.
   - Pour rechercher un sous-réseau spécifique, celui-ci doit figurer dans la liste **Sous-réseaux à rechercher** et son paramètre **Rechercher** doit avoir pour valeur **Activé** :
     a. Si le sous-réseau ne figure pas dans la liste, choisissez l'icône **Nouveau**  . Dans la boîte de dialogue **Nouvelle attribution de sous-réseau**, renseignez les champs **Sous-réseau** et **Masque**, puis choisissez **OK**. Par défaut, un nouveau sous-réseau est activé pour la recherche.
     b. Pour modifier la valeur **Rechercher** d'un sous-réseau figurant dans la liste, sélectionnez-le, puis choisissez l'icône **Basculer** afin de remplacer la valeur **Désactivé** par la valeur **Activé** (ou inversement).
6. Pour configurer la découverte et rechercher les domaines, cliquez sur l'onglet **Domaines**, puis configurez une ou plusieurs des options suivantes :
   - Pour lancer la découverte sur le domaine de l'ordinateur exécutant la découverte, activez la case à cocher **Rechercher dans le domaine local**.
   - Pour rechercher un domaine spécifique, vérifiez que celui-ci figure dans la liste **Domaines** et que son paramètre **Rechercher** a pour valeur **Activé** :
     a. Si le domaine ne figure pas dans la liste, choisissez l'icône **Nouveau**  . Dans la boîte de dialogue **Propriétés de domaine**, renseignez le champ **Domaine**, puis choisissez **OK**. Par défaut, un nouveau domaine est activé pour la recherche.
     b. Pour modifier la valeur **Rechercher** d'un domaine figurant dans la liste, sélectionnez le domaine, puis choisissez l'icône **Basculer** afin de remplacer la valeur **Désactivé** par la valeur **Activé** (ou inversement).
7. Pour configurer la découverte afin de rechercher des noms de communautés SNMP, choisissez l'onglet **SNMP**, puis configurez une ou plusieurs des options suivantes :
   - Pour ajouter un nom de communauté SNMP dans la liste **Noms de communautés SNMP**, choisissez l'icône **Nouveau**  . Dans la boîte de dialogue **Nouveau nom de communauté SNMP**, indiquez le **Nom** de la communauté SNMP, puis choisissez **OK**.
   - Pour supprimer un nom de communauté SNMP, sélectionnez-le, puis choisissez l'icône **Supprimer**  .
   - Pour modifier l'ordre de recherche des noms de communautés SNMP, sélectionnez un nom de communauté, puis choisissez l'icône **Déplacer l'élément vers le haut**  ou **Déplacer l'élément vers le bas**  . Lors de l'exécution de la découverte, la recherche des noms de

communauté est effectuée dans un ordre de haut en bas. Gardez à l'esprit les points suivants.

> **NOTE**
> Le service de découverte du réseau utilise les noms des communautés SNMP pour accéder à des routeurs correspondant à des périphériques SNMP. Un routeur permet d'informer le service de découverte du réseau sur les autres routeurs et les sous-réseaux liés au premier routeur.

- Les noms de communautés SNMP sont semblables aux mots de passe.
- Le service de découverte du réseau peut uniquement obtenir des informations d'un périphérique SNMP pour lequel vous avez spécifié un nom de communauté.
- Chaque périphérique SNMP peut disposer de son propre nom de communauté mais souvent, plusieurs périphériques partagent le même nom de communauté.
- La plupart des périphériques SNMP ont un nom de communauté par défaut, qui est **Public**. Vous pouvez l'utiliser si vous n'en connaissez pas d'autres. Toutefois, certaines organisations suppriment le nom de communauté **Public** de leurs périphériques pour des raisons de sécurité.

8. Pour configurer le nombre maximal de sauts de routeur pour les recherches SNMP, choisissez l'onglet **SNMP**, puis sélectionnez le nombre maximal de sauts dans la liste déroulante **Nombre maximal de sauts**.
9. Pour configurer un périphérique SNMP, choisissez l'onglet **Périphériques SNMP**. Si le périphérique ne figure pas dans la liste, choisissez l'icône **Nouveau**  . Dans la boîte de dialogue **Nouvelle unité SNMP**, tapez l'adresse IP ou le nom du périphérique SNMP, puis choisissez **OK**.

   > **NOTE**
   > Si vous spécifiez un nom de périphérique, Configuration Manager doit pouvoir résoudre le nom NetBIOS en adresse IP.

10. Pour configurer la découverte afin d'interroger certains serveurs DHCP de clients DHCP, choisissez l'onglet **DHCP**, puis configurez une ou plusieurs des options suivantes :

    - Pour interroger le serveur DHCP sur l'ordinateur exécutant la découverte, choisissez de **toujours utiliser le serveur DHCP du serveur de site**.

      > **NOTE**
      > Pour utiliser cette option, le serveur doit louer son adresse IP à un serveur DHCP, et il ne peut pas utiliser une adresse IP statique.

    - Pour interroger un serveur DHCP spécifique, choisissez l'icône **Nouveau**  . Dans la boîte de dialogue **Nouveau serveur DHCP**, entrez l'adresse IP ou le nom du serveur DHCP, puis choisissez **OK**.

      > **NOTE**
      > Si vous spécifiez un nom de serveur, Configuration Manager doit pouvoir résoudre le nom NetBIOS en adresse IP.

11. Pour configurer à quel moment la découverte s'exécute, cliquez sur l'onglet **Calendrier**, puis choisissez l'icône **Nouveau** afin de définir le calendrier d'exécution de la découverte du réseau.

    Vous pouvez configurer plusieurs calendriers récurrents et plusieurs calendriers non récurrents.

    > **NOTE**
    > Si plusieurs calendriers s'affichent dans l'onglet **Calendrier**, tous exécutent la découverte du réseau à l'heure indiquée. Ce comportement s'applique également aux planifications périodiques.

12. Choisissez **OK** pour enregistrer vos configurations.

**Guide pratique pour vérifier que la découverte du réseau est terminée**

La durée d'exécution de la découverte du réseau peut varier selon un ou plusieurs des facteurs suivants :

- Taille de votre réseau
- Topologie de votre réseau
- Nombre maximal de sauts configurés pour la recherche de routeurs sur le réseau
- Type de découverte en cours d'exécution

Comme la découverte du réseau ne génère pas de message d'alerte signalant qu'elle est terminée, vous devez donc le vérifier à l'aide de la procédure suivante.

#### Pour vérifier qu'une découverte du réseau est terminée

1. Dans la console Configuration Manager, choisissez **Surveillance**.
2. Dans l'espace de travail **Surveillance**, développez **État du système**, puis choisissez **Requêtes sur les messages d'état**.
3. Choisissez **All Status Messages (Tous les messages d'état)**.
4. Dans l'onglet **Accueil** puis dans le groupe **Requêtes sur les messages d'état**, choisissez **Afficher les messages**.
5. Dans la liste déroulante **Sélectionner la date et l'heure**, sélectionnez une valeur indiquant depuis combien de temps a démarré la découverte, puis choisissez **OK** pour ouvrir la boîte de dialogue **Afficheur des messages d'état de Configuration Manager**.

    > **TIP**
    > Vous pouvez également utiliser l'option **Spécifier la date et l'heure** pour sélectionner la date et l'heure auxquelles vous avez exécuté la découverte. Cette option s'avère utile si vous avez exécuté une découverte du réseau à une date donnée et que vous voulez récupérer uniquement les messages ayant été générés à cette date.

6. Pour valider que la découverte du réseau est terminée, recherchez un message d'état contenant les détails suivants :

    - ID de message : **502**
    - Composant : **SMS_NETWORK_DISCOVERY**
    - Description : **Ce composant s'est arrêté.**

    Si ce message d'état ne s'affiche pas, la découverte de réseau n'est pas terminée.

7. Pour valider le moment de démarrage de la découverte du réseau, recherchez un message d'état contenant

les détails suivants :

- ID de message : **500**
- Composant : **SMS_NETWORK_DISCOVERY**
- Description : **Ce composant a démarré.**

Ces informations vérifient que la découverte du réseau a démarré. Si ces informations ne s'affichent pas, replanifiez une découverte du réseau.

# Définir des limites de site et les groupes de limites pour System Center Configuration Manager

22/06/2018 • 5 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les limites pour System Center Configuration Manager définissent les emplacements réseau sur votre intranet pouvant contenir des appareils que vous souhaitez gérer. Les groupes de limites sont des groupes logiques de limites que vous configurez.

Une hiérarchie peut inclure n'importe quel nombre de groupes de limites, et chaque groupe de limites peut contenir n'importe quelle combinaison des types de limites suivants :

- Sous-réseau IP
- Nom de site Active Directory
- Préfixe IPv6
- Plage d'adresses IP

Les clients intranet évaluent leur emplacement réseau actuel, puis utilisent ces informations pour identifier les groupes de limites auxquels ils appartiennent.

Les clients utilisent des groupes de limites pour :

- **Trouver un site attribué** : les groupes de limites permettent aux clients de trouver un site principal pour l'attribution du client (attribution automatique de site).
- **Trouver des rôles de système de site spécifiques disponibles** : quand vous associez un groupe de limites à certains rôles de système de site, le groupe de limites fournit aux clients la liste des systèmes de site à utiliser pour l'emplacement du contenu et en tant que points de gestion préférés.

Les clients Internet ou les clients configurés en tant que clients Internet uniquement n'utilisent pas les informations sur les limites. Ces clients ne peuvent pas utiliser l'attribution automatique de site. Ils peuvent toujours télécharger le contenu de n'importe quel point de distribution sur leur site attribué quand le point de distribution est configuré pour autoriser les connexions clientes depuis Internet.

**Pour bien démarrer :**

- Tout d'abord, définissez les emplacements réseau en tant que limites.
- Puis, poursuivez en configurant des groupes de limites pour associer les clients dans ces limites aux serveurs de système de site qu'ils peuvent utiliser.

## Meilleures pratiques en matière de limites et de groupes de limites

- **Utilisez une combinaison du plus petit nombre de limites qui répondent à vos besoins :**
  Dans le passé, nous vous avons conseillé d'utiliser certains types de limites plus que d'autres. Compte-tenu des modifications apportées pour améliorer les performances, nous vous conseillons dorénavant d'utiliser le ou les types de votre choix qui fonctionnent dans votre environnement et qui vous permettent d'utiliser le plus petit nombre de limites possible pour simplifier vos tâches de gestion.

- **Éviter le chevauchement des limites pour l'attribution automatique de site :**
  Chaque groupe de limites prend en charge les configurations d'attribution de site et d'emplacement du contenu, mais il est recommandé de créer un ensemble de groupes de limites à utiliser uniquement pour

l'attribution de site. Cela signifie que vous devez vérifier qu'aucune limite d'un groupe de limites n'est membre d'un autre groupe de limites ayant une attribution de site différente. La raison est la suivante :

- Une limite peut être incluse dans plusieurs groupes de limites.
- Chaque groupe de limites peut être associé à un site principal différent pour l'attribution de site.
- Un client sur une limite qui est membre de deux groupes de limites ayant des attributions de site différentes sélectionne au hasard un site auquel se joindre, site qui n'est pas nécessairement le site que vous avez prévu à cet effet. Cette configuration est appelée chevauchement des limites.

  Le chevauchement des limites n'est pas un problème pour l'emplacement du contenu. Il s'agit souvent d'une configuration souhaitée qui fournit aux clients des ressources ou emplacements de contenu supplémentaires qu'ils peuvent utiliser.

# Définir des emplacements réseau comme limites pour System Center Configuration Manager

22/06/2018 • 7 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les limites de Configuration Manager sont des emplacements sur votre réseau contenant des appareils que vous souhaitez gérer. La limite sur laquelle se trouve un appareil est équivalente au site Active Directory ou à l'adresse IP réseau identifiée par le client Configuration Manager installé sur l'appareil.

- Vous pouvez créer manuellement des limites individuelles. Cependant, Configuration Manager ne prend pas en charge l'entrée directe d'un sur-réseau en tant que limite. À la place, utilisez le type de limite de la plage d'adresses IP.
- Vous pouvez configurer la méthode de découverte de forêts Active Directory afin de détecter automatiquement et de créer des limites pour chaque sous-réseau IP et site Active Directory ainsi découverts. Lorsque la fonctionnalité de découverte de forêts Active Directory identifie un sur-réseau attribué à un site Active Directory, Configuration Manager convertit le sur-réseau en limite de plage d'adresses IP.

Il n'est pas rare qu'un appareil utilise une adresse IP dont l'administrateur Configuration Manager n'a pas connaissance. En cas de doute sur l'emplacement réseau d'un appareil, confirmez l'emplacement signalé par l'appareil en exécutant la commande **IPCONFIG** sur l'appareil.

Quand vous créez une limite, elle reçoit automatiquement un nom basé sur son type et son étendue. Ce nom ne peut pas être modifié. Au lieu de cela, vous pouvez spécifier une description permettant de l'identifier dans la console Configuration Manager.

Chaque limite est utilisable par tous les sites de votre hiérarchie. Après avoir créé une limite, vous pouvez modifier ses propriétés pour effectuer les opérations suivantes :

- Ajouter la limite à un ou plusieurs groupes de limites.
- Changer le type ou la portée de la limite.
- Afficher l'onglet **Systèmes de site** des limites pour savoir quels serveurs de système de site (points de distribution, points de migration d'état et points de gestion) sont associés à la limite.

## Pour créer une limite

1. Dans la console Configuration Manager, cliquez sur **Administration** > **Configuration de la hiérarchie** > **Limites**
2. Dans l'onglet **Accueil** , dans le groupe **Créer** , cliquez sur **Créer Boundary.**
3. Dans l'onglet **Général** de la boîte de dialogue Créer une limite, vous pouvez spécifier une **Description** pour identifier une limite par un nom convivial ou une référence.
4. Sélectionnez un **Type** pour cette limite :
   - Si vous sélectionnez **Sous-réseau IP**, vous devez spécifier un **ID de sous-réseau** pour cette limite.

> **TIP**
> Vous pouvez spécifier le **Réseau** et le **Masque de sous-réseau** pour que l' **ID de sous-réseau** soit automatiquement spécifié. Lorsque vous enregistrez la limite, seule la valeur d'ID de sous-réseau est enregistrée.

- Si vous sélectionnez **Site Active Directory**, vous devez spécifier ou **Parcourir** vers un site Active Directory dans la forêt locale du serveur de site.

  > **IMPORTANT**
  > Lorsque vous spécifiez un site Active Directory pour une limite, la limite inclut chaque sous-réseau IP membre de ce site Active Directory. Si la configuration du site Active Directory est modifiée dans Active Directory, les emplacements réseau inclus dans cette limite sont également modifiés.

- Si vous sélectionnez **Préfixe IPv6**, vous devez spécifier un **Préfixe** au format de préfixe IPv6.
- Si vous sélectionnez **Plage d'adresses IP**, vous devez spécifier une **Adresse IP de début** et une **Adresse IP de fin** qui inclut la partie d'un sous-réseau IP ou inclut plusieurs sous-réseaux IP.

5. Cliquez sur **OK** pour enregistrer la nouvelle limite.

## Pour configurer une limite

1. Dans la console Configuration Manager, cliquez sur **Administration** > **Configuration de la hiérarchie** > **Limites**
2. Sélectionnez la limite à modifier.
3. Dans l'onglet **Accueil** , dans le groupe **Propriétés** , cliquez sur **Propriétés**.
4. Dans la boîte de dialogue **Propriétés** de la limite, sélectionnez l'onglet **Général** pour modifier la **Description** ou le **Type** de la limite. Vous pouvez également modifier l'étendue d'une limite en modifiant les emplacements réseau pour la limite. Par exemple, pour une limite de site Active Directory, vous pouvez spécifier un nouveau nom de site Active Directory.
5. Sélectionnez l'onglet **Systèmes de site** pour afficher les systèmes de site associés à cette limite. Vous ne pouvez pas modifier cette configuration à partir des propriétés d'une limite.

   > **TIP**
   > Pour qu'un serveur de système de site soit référencé comme système de site pour une limite, il faut que le serveur de système de site soit associé en tant que serveur de système de site pour au moins un groupe de limites comportant cette limite. Vous pouvez configurer cela sous l'onglet **Références** d'un groupe de limites.

6. Sélectionnez l'onglet **Groupes de limites** pour modifier l'appartenance au groupe de limites pour cette limite :
   - Pour ajouter cette limite à un ou plusieurs groupes de limites, cliquez sur **Ajouter**, cochez la case d'un ou plusieurs groupes de limites, puis cliquez sur **OK**.
   - Pour supprimer cette limite d'un groupe de limites, sélectionnez le groupe de limites, puis cliquez sur **Supprimer**.
7. Cliquez sur **OK** pour fermer les propriétés de la limite et enregistrer la configuration.

# Configurer les groupes de limites pour System Center Configuration Manager

22/06/2018 • 60 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez des groupes de limites dans Configuration Manager afin d'organiser de façon logique des emplacements réseau associés (limites) pour faciliter la gestion de votre infrastructure. Attribuez des limites aux groupes de limites avant d'utiliser le groupe de limites.

Par défaut, Configuration Manager crée un groupe de limites de site par défaut sur chaque site.

Pour configurer des groupes de limites, associez des limites (emplacements réseau) et des rôles de système de site, comme les points de distribution, au groupe de limites. Cette configuration permet d'associer les clients aux serveurs de système de site tels que les points de distribution qui se trouvent près des clients sur le réseau.

Pour augmenter la disponibilité des serveurs de systèmes de site, tels que les points de distribution, sur un plus large éventail d'emplacements réseau, affectez la même limite et le même serveur à plusieurs groupes de limites.

Les clients utilisent un groupe de limites pour les applications suivantes :

- Attribution automatique du site
- Recherche d'un serveur de système de site capable de fournir un service, notamment :
  - Points de distribution pour l'emplacement du contenu
  - Points de mise à jour logicielle
  - Points de migration de l'état
  - Points de gestion préférés (Si vous utilisez des points de gestion préférés, vous devez activer cette option pour la hiérarchie et non pas à partir de la configuration du groupe de limites. Consultez la section Activer l'utilisation des points de gestion préférés de cette rubrique.)

## Relations et groupes de limites

Pour chaque groupe de limites de votre hiérarchie, vous pouvez affecter :

- Une ou plusieurs limites. Le groupe de limites **actif** d'un client correspond à un emplacement réseau défini comme limite affectée à un groupe de limites donné. Un client peut avoir plusieurs groupes de limites actifs.
- Un ou plusieurs rôles de système de site. Les clients peuvent toujours utiliser des rôles de système de site associés à leur groupe de limites actif. En fonction des configurations supplémentaires, ils peuvent dans certains cas utiliser les rôles de système de site dans les groupes de limites supplémentaires.

Pour chaque groupe de limites créé, vous pouvez configurer un lien à sens unique vers un autre groupe de limites. Ce lien est appelé **relation**. Les groupes de limites vers lequel pointent ces liens sont appelés groupes de limites **voisins**. Un groupe de limites peut avoir plusieurs relations, chacune avec un groupe de limites voisin spécifique.

Quand un client ne parvient pas à trouver un serveur de système de site disponible dans son groupe de limites actif, la configuration de chaque relation détermine le moment où il commence à effectuer des recherches dans un groupe de limites voisin. Cette recherche dans des groupes supplémentaires est appelée **secours**.

## Secours

Pour éviter des problèmes quand les clients ne trouvent pas de système de site disponible dans leur groupe de

limites actif, définissez la relation entre les groupes de limites pour le comportement de secours. Le secours permet à un client d'étendre sa recherche à des groupes de limites supplémentaires pour trouver un système de site disponible.

Les relations sont configurées dans l'onglet **Relations** des propriétés du groupe de limites. Lorsque vous configurez une relation, vous définissez un lien vers un groupe de limites voisin. Pour chaque type de rôle de système de site pris en charge, configurez des paramètres indépendants pour le recours au groupe de limites voisin. Par exemple, quand vous configurez une relation vers un groupe de limites donné, définissez le déclenchement du secours après 20 minutes au lieu des 120 minutes par défaut pour les points de distribution. Pour obtenir un exemple plus complet, consultez Exemple d'utilisation des groupes de limites.

Si un client ne trouve pas un rôle de système de site disponible dans son groupe de limites actif, il utilise le délai de secours en minutes. Ce délai détermine le moment où le client commence à rechercher un système de site disponible associé au groupe de limites voisin.

Quand un client ne peut pas trouver de système de site disponible et commence à effectuer des recherches à des emplacements de groupes de limites voisins, il augmente le pool de systèmes de site disponibles. La configuration des groupes de limites et de leurs relations définit l'utilisation de ce pool par le client.

- Un groupe de limites peut avoir plusieurs relations. Avec plusieurs relations, vous pouvez configurer l'intervention de la solution de secours pour chaque type de système de site sur différents voisins après différents délais.
- Les clients utilisent uniquement en secours un groupe de limites qui est un voisin direct de leur groupe de limites actuel.
- Quand un client est membre de plusieurs groupes de limites, le groupe de limites actif est défini en tant qu'union de tous les groupes de limites du client. Le client peut ensuite recourir à des voisins de n'importe lequel de ces groupes de limites d'origine.

**Le groupe de limites de site par défaut**

Outre les groupes de limites que vous créez, chaque site possède un groupe de limites de site par défaut créé par Configuration Manager. Ce groupe est nommé ***Default-Site-Boundary-Group<sitecode>***. Par exemple, le groupe du site ABC s'appellerait *Default-Site-Boundary-Group<ABC>*.

Pour chaque groupe de limites que vous créez, Configuration Manager crée automatiquement un lien implicite vers chacun des groupes de limites de site par défaut de la hiérarchie.

- Le lien implicite est une option de secours par défaut d'un groupe de limites actif vers le groupe de limites de site par défaut, qui a un délai de secours par défaut de 120 minutes.
- Pour les clients qui ne sont pas sur une limite associée à un groupe de limites : pour identifier les rôles de système de site valides, ils doivent utiliser le groupe de limites par défaut du site qui leur a été affecté.

Pour gérer le recours au groupe de limites de site par défaut :

- Ouvrez les propriétés du groupe de limites par défaut du site et modifiez les valeurs de l'onglet **Comportement par défaut**. Les modifications apportées ici s'appliquent à *tous* les liens implicites vers ce groupe de limites. Ces paramètres peuvent être remplacés lorsque vous configurez le lien explicite vers ce groupe de limites de site par défaut à partir d'un autre groupe de limites.
- Ouvrez les propriétés d'un groupe de limites personnalisé. Modifiez les valeurs du lien explicite vers un groupe de limites de site par défaut. Lorsque vous définissez un nouveau délai de secours ou de secours en bloc en minutes, cette modification affecte uniquement le lien que vous configurez. La configuration du lien explicite remplace les paramètres de l'onglet **Comportement par défaut** d'un groupe de limites de site par défaut.

## Attribution de site

Vous pouvez configurer chaque groupe de limites avec un site attribué pour les clients.

- Quand un client récemment installé utilise l'attribution automatique de site, il rejoint le site attribué d'un groupe de limites qui englobe l'emplacement réseau actuel du client.
- Après avoir été attribué à un site, un client ne modifie pas son attribution de site quand il change d'emplacement réseau. Par exemple, si le client est en itinérance vers un nouvel emplacement réseau représenté par une limite dans un groupe de limites disposant d'une attribution de site différente, le site attribué au client n'est pas modifié.
- Lorsque la découverte de systèmes Active Directory détecte une nouvelle ressource, les informations sur le réseau de la ressource découverte sont évaluées en fonction des limites dans les groupes de limites. Ce processus associe la nouvelle ressource à un site attribué pour une utilisation par la méthode d'installation poussée du client.
- Quand une limite est membre de plusieurs groupes de limites auxquels différents sites sont attribués, les clients sélectionnent l'un des sites de manière aléatoire.
- Les modifications apportées à un site attribué à des groupes de limites s'appliquent uniquement aux nouvelles actions d'attribution de site. Les clients déjà attribués à un site ne réévaluent pas leur attribution à un site en fonction des changements apportés à la configuration d'un groupe de limites (ou à leur emplacement réseau).

Pour plus d'informations sur l'attribution de site client, consultez Utilisation de l'attribution automatique de site pour les ordinateurs dans Guide pratique pour affecter des clients à un site dans System Center Configuration Manager.

## Points de distribution

Quand un client demande l'emplacement d'un point de distribution, Configuration Manager lui envoie une liste des systèmes de site. Ces systèmes de site sont du type approprié associé à chaque groupe de limites qui inclut l'emplacement réseau actuel du client :

- **Lors de la distribution de logiciels**, les clients demandent un emplacement pour le contenu de déploiement disponible à partir d'un point de distribution, ou une autre source de contenu valide (par exemple, un client configuré pour le cache d'homologue).
- **Durant le déploiement de système d'exploitation**, les clients demandent un emplacement où envoyer ou recevoir des informations sur la migration de leur état.

Lors du déploiement de contenu, si un client demande du contenu qui n'est pas disponible à partir d'une source de son groupe de limites actif, le client continue de demander ce contenu. Il essaie différentes sources de contenu dans son groupe de limites actif, jusqu'à ce que la période de secours d'un groupe de limites voisin ou du groupe de limites de site par défaut soit atteinte. Si le client n'a pas encore trouvé de contenu, il étend ensuite sa recherche de sources de contenu aux groupes de limites voisins.

Si le contenu est distribué à la demande, mais qu'il n'est pas disponible sur un point de distribution quand il est demandé par un client, le processus de transfert du contenu vers ce point de distribution commence. Il est possible que le client trouve ce serveur comme source de contenu avant d'utiliser un groupe de limites voisin en secours.

## Points de mise à jour logicielle

Les clients utilisent des groupes de limites pour rechercher un nouveau point de mise à jour logicielle. Pour contrôler les serveurs qu'un client peut trouver, ajoutez des points de mise à jour logicielle individuels à différents groupes de limites.

Si vous effectuez la mise à jour à partir d'une version antérieure à la version 1702, chaque site ajoute tous les points de mise à jour logicielle existants au groupe de limites de site par défaut. Ce comportement de mise à jour du site garde le comportement du client précédent pour sélectionner un point de mise à jour logicielle dans le pool de serveurs disponibles. Ce comportement est conservé tant que vous ne choisissez pas d'ajouter des points de mise à jour logicielle propres à chaque groupe de limites pour une sélection contrôlée et un comportement de

secours.

Si vous installez un nouveau site, des points de mise à jour logicielle ne sont pas ajoutés au groupe de limites de site par défaut. Attribuez des points de mise à jour logicielle à un groupe de limites afin que les clients puissent les trouver et les utiliser.

**Action de secours pour les points de mise à jour logicielle**

Pour les points de mise à jour logicielle, le secours est configuré comme les autres rôles de système de site, mais avec les restrictions suivantes :

- **Les nouveaux clients utilisent des groupes de limites pour sélectionner les points de mise à jour logicielle.** Les nouveaux clients installés sélectionnent un point de mise à jour logicielle parmi les serveurs associés aux groupes de limites que vous configurez. Ce comportement vient remplacer celui qui consistait, pour les clients, à sélectionner un point de mise à jour logicielle de manière aléatoire dans une liste des serveurs partageant la forêt du client.
- **Les clients continuent d'utiliser un dernier point de mise à jour logicielle correct connu jusqu'à ce qu'ils en recherchent un nouveau une fois l'action de secours lancée.** Les clients qui disposent déjà d'un point de mise à jour logicielle continuent de l'utiliser jusqu'à ce qu'il ne soit plus accessible. Ce comportement comprend la poursuite de l'utilisation d'un point de mise à jour logicielle non associé au groupe de limites actif du client.

  Le fait qu'un point de mise à jour logicielle existant soit utilisé même si ce serveur ne se trouve pas dans le groupe de limites actif du client est intentionnel. Quand le point de mise à jour logicielle change, le client synchronise ses données avec le nouveau serveur, ce qui peut entraîner une utilisation importante du réseau. Si tous les clients basculent vers un nouveau serveur en même temps, le délai de transition peut permettre d'éviter la saturation du réseau.
- **Un client tente toujours d'atteindre son dernier point de mise à jour logicielle correct connu pendant 120 minutes avant de démarrer l'action de secours.** Après 120 minutes, si le client n'a pas établi de contact, il démarre l'action de secours. Quand l'action de secours démarre, le client reçoit la liste de tous les points de mise à jour logicielle à partir de son groupe de limites actif. Des points de mise à jour logicielle supplémentaires à partir de groupes de limites voisins et de site par défaut sont disponibles en fonction des configurations de secours.

**Configurations de l'action de secours pour les points de mise à jour logicielle**

**Depuis la version 1706**

Vous pouvez configurer des **durées avant repli (en minutes)** inférieures à 120 minutes pour les points de mise à jour logicielle. Toutefois, le client tente toujours d'atteindre son point de mise à jour logicielle d'origine pendant 120 minutes. Il étend ensuite sa recherche à des serveurs supplémentaires. Les délais de secours des groupes de limites démarrent dès que le client ne parvient pas à atteindre le serveur d'origine. Quand le client étend sa recherche, le site fournit tous les groupes de limites configurés depuis moins de 120 minutes.

Pour bloquer l'action de secours pour un point de mise à jour logicielle vers un groupe de limites voisin, affectez au paramètre la valeur **Jamais d'action de secours**.

Après avoir échoué pendant deux heures à atteindre le serveur d'origine, le client utilise un cycle plus court pour établir une connexion à un nouveau point de mise à jour logicielle. Ce comportement permet au client d'explorer rapidement la liste croissante des points de mise à jour logicielle potentiels.

- **Exemple d'action de secours :**
  Le groupe de limites actif d'un client a, pour les points de mise à jour logicielle, une action de secours dont la configuration est la suivante : *10* minutes pour le groupe de limites *A* et *130* minutes pour le groupe de limites *B*. Quand le client ne parvient pas à atteindre son dernier point de mise à jour logicielle correct connu :
  - Le client tente d'atteindre uniquement son serveur d'origine pendant les 120 minutes suivantes. Après 10 minutes, les points de mise à jour logicielle du groupe de limites A sont ajoutés au pool de serveurs

disponibles. Toutefois, le client ne peut pas tenter de contacter ces derniers ou tout autre serveur jusqu'à ce que se soit écoulée la période initiale de 120 minutes de reconnexion au serveur d'origine.

- Après avoir essayé de localiser ce point de mise à jour logicielle d'origine pendant 120 minutes, le client peut étendre sa recherche. À ce stade, le client ajoute des serveurs au pool disponible des points de mise à jour logicielle qui se trouvent dans son groupe de limites actif et dans tous les groupes de limites voisins configurés depuis une durée inférieure ou égale à 120 minutes. Ce pool inclut les serveurs du groupe de limites A qui ont été ajoutés au pool de serveurs disponibles.
- Après 10 minutes supplémentaires (soit un total de 130 minutes après le premier échec du client dans sa tentative d'atteindre son dernier point de mise à jour logicielle correct connu), le client étend la recherche pour inclure les points de mise à jour logicielle du groupe de limites B.

**Avant la version 1706**

Avant la version 1706, les configurations de l'action de secours pour les points de mise à jour logicielle ne gèrent pas une période configurable en minutes. Le comportement de l'action de secours est limité comme suit :

- **Délai de secours (en minutes) :** cette option est grisée pour les points de mise à jour logicielle et n'est pas configurable. Elle est définie sur 120 minutes.
- **Ne jamais activer le secours :** vous pouvez bloquer le secours pour un point de mise à jour logicielle vers un groupe de limites voisin lorsque vous utilisez cette configuration.

Quand un client qui possède déjà un point de mise à jour logicielle ne parvient pas à l'atteindre, il en cherche un autre en secours. En cas d'utilisation du secours, le client reçoit la liste de tous les points de mise à jour logicielle à partir de son groupe de limites actif. S'il ne trouve pas de serveur disponible en 120 minutes, il a ensuite recours à ses groupes de limites voisins et au groupe de limites de site par défaut. Le recours aux deux groupes de limites se produit en même temps. Le délai de secours des points de mise à jour logicielle vers les groupes voisins est défini sur 120 minutes. Vous ne pouvez pas modifier ce délai. 120 minutes correspond également à la durée par défaut utilisée pour le recours au groupe de limites de site par défaut. Lorsque le client a recours à la fois à un groupe de limites voisin et au groupe de limites de site par défaut, il tente de contacter les points de mise à jour logicielle du groupe de limites voisin avant d'essayer d'utiliser ceux du groupe de limites de site par défaut.

**Basculer manuellement vers un nouveau point de mise à jour logicielle**

Outre l'action de secours, vous pouvez utiliser *Notification du client* pour forcer manuellement un appareil à basculer vers un nouveau point de mise à jour logicielle.

Quand vous basculez vers un nouveau serveur, les appareils utilisent l'action de secours pour rechercher ce serveur. Passez en revue vos configurations de groupes de limites. Vérifiez que vos points de mise à jour logicielle sont dans les groupes de limites appropriés avant de procéder à ce changement.

Pour plus d'informations, consultez Basculer manuellement les clients vers un nouveau point de mise à jour logicielle.

## Points de gestion

Depuis la version 1802, configurez des relations de secours pour les points de gestion entre les groupes de limites. Ce comportement offre un meilleur contrôle des points de gestion que les clients utilisent. L'onglet **Relations** des propriétés du groupe de limites comporte une colonne pour le point de gestion. Lors de l'ajout d'un nouveau groupe de limites de secours, le temps de secours du point de gestion est actuellement toujours égal à zéro (0). Ce comportement est identique pour le **Comportement par défaut** dans le groupe de limites de site par défaut.

Auparavant, un problème se produisait souvent pour les points de gestion protégés présents dans un réseau sécurisé. Les clients du réseau d'entreprise principal recevaient une stratégie comprenant ce point de gestion protégé, même s'ils ne pouvaient pas communiquer avec lui à travers un pare-feu. Pour résoudre ce problème, utilisez l'option **Jamais d'action de secours** pour que les clients n'utilisent en secours que les points de gestion avec lesquels ils peuvent communiquer.

Lors de la mise à niveau du site vers la version 1802, Configuration Manager ajoute tous les points de gestion sans accès via Internet au groupe de limites de site par défaut. Ce comportement de mise à niveau permet de s'assurer que les versions antérieures des clients continuent de communiquer avec les points de gestion. Pour tirer pleinement parti de cette fonctionnalité, déplacez vos points de gestion vers les groupes de limites de votre choix.

L'action de secours du groupe de limites de point de gestion ne modifie pas le comportement lors de l'installation du client (ccmsetup.exe). Si la ligne de commande ne spécifie pas le point de gestion initial avec le paramètre/MP, le nouveau client reçoit la liste complète des points de gestion disponibles. Pour son processus d'amorçage initial, le client utilise le premier point de gestion auquel il peut accéder. Une fois inscrit auprès du site, il recevra la liste des points de gestion convenablement triée avec ce nouveau comportement.

Pour que les clients utilisent cette fonctionnalité, activez le paramètre suivant : **Les clients préfèrent utiliser les points de gestion spécifiés dans les groupes de limites** dans **Paramètres de hiérarchie**.

> **NOTE**
> Les processus de déploiement de système d'exploitation ne prennent pas en charge les groupes de limites.

**Résolution des problèmes**

De nouvelles entrées apparaissent dans **LocationServices.log**. L'attribut **Localité** identifie l'un des états suivants :

- 0 : Inconnu
- 1 : Le point de gestion spécifié se trouve uniquement dans le groupe de limites de site par défaut pour l'action de secours
- 2 : Le point de gestion spécifié se trouve dans un groupe de limites voisin ou distant. S'il est à la fois dans le groupe de limites de site par défaut et dans un groupe voisin, la localité est 2.
- 3 : Le point de gestion spécifié se trouve dans le groupe de limites local ou actif. S'il est à la fois dans le groupe de limites actif et dans un groupe voisin ou le groupe de limites de site par défaut, la localité est 3. Si vous n'activez pas le paramètre des points de gestion préférés dans les Paramètres de hiérarchie, la localité est toujours 3, quel que soit le groupe de limites du point de gestion.

Les clients utilisent en premier les points de gestion locaux (localité 3), puis distants (localité 2) et enfin de secours (localité 1).

Quand un client reçoit cinq erreurs en 10 minutes et ne parvient pas à communiquer avec l'un des points de gestion de son groupe de limites actif, il tente de contacter un point de gestion d'un groupe de limites voisin ou du groupe de limites de site par défaut. Si le point de gestion du groupe de limites actif revient en ligne par la suite, le client retournera au point de gestion local lors du prochain cycle d'actualisation. Ce cycle a une durée de 24 heures, ou se termine au redémarrage du service de l'agent Configuration Manager.

## Points de gestion préférés

> **NOTE**
> Le comportement de ce paramètre de hiérarchie, **Les clients préfèrent utiliser les points de gestion spécifiés dans les groupes de limites**, change depuis la version 1802. Quand vous activez ce paramètre, Configuration Manager utilise la fonctionnalité de groupe de limites pour le point de gestion attribué. Pour plus d'informations, consultez Points de gestion.

Les points de gestion préférés permettent à un client d'identifier un point de gestion associé à son emplacement réseau actuel (limite) avec celui-ci.

- Un client essaie d'utiliser un point de gestion préféré de son site attribué avant d'en utiliser un qui n'est pas configuré comme préféré.

- Pour utiliser cette option, activez **Les clients préfèrent utiliser les points de gestion spécifiés dans les groupes de limites** dans **Paramètres de hiérarchie**. Configurez ensuite des groupes de limites au niveau de chaque site principal. Incluez les points de gestion à associer aux limites de ces groupes de limites.
- Quand vous configurez les points de gestion préférés et qu'un client organise sa propre liste de points de gestion, il place les points de gestion préférés en haut de sa liste. Cette liste comprend tous les points de gestion du site affecté au client.

> **NOTE**
> L'itinérance du client signifie qu'il change d'emplacement réseau. Il peut s'agir, par exemple, d'un ordinateur portable déplacé vers un emplacement de bureau distant. Quand un client est en itinérance, il peut utiliser un point de gestion ou un point de gestion proxy du site local comme nouvel emplacement avant d'essayer d'utiliser un serveur de son site attribué. Cette liste de serveurs de son site attribué comprend les points de gestion préférés. Pour plus d'informations, consultez Comprendre comment les clients recherchent des services et des ressources de site.

## Chevauchement des limites

Configuration Manager prend en charge les configurations de limites se chevauchant pour l'emplacement du contenu. Quand l'emplacement réseau du client appartient à plusieurs groupes de limites :

- Quand un client demande du contenu, Configuration Manager lui envoie une liste de tous les points de distribution qui disposent du contenu.
- Quand un client demande à un serveur d'envoyer ou de recevoir des informations sur la migration de son état, Configuration Manager lui envoie une liste de tous les points de migration d'état associés à un groupe de limites qui inclut l'emplacement réseau actuel du client.

Ce comportement permet au client de sélectionner le serveur le plus proche depuis lequel transférer le contenu ou les informations sur la migration de l'état.

## Exemple d'utilisation de groupes de limites

L'exemple suivant utilise un client qui recherche du contenu sur un point de distribution. Cet exemple peut s'appliquer à d'autres rôles de système de site qui utilisent des groupes de limites. Gardez à l'esprit que les points de mise à jour logicielle ne prennent pas en charge la configuration du recours à un groupe voisin, et qu'ils utilisent toujours une période de 120 minutes.

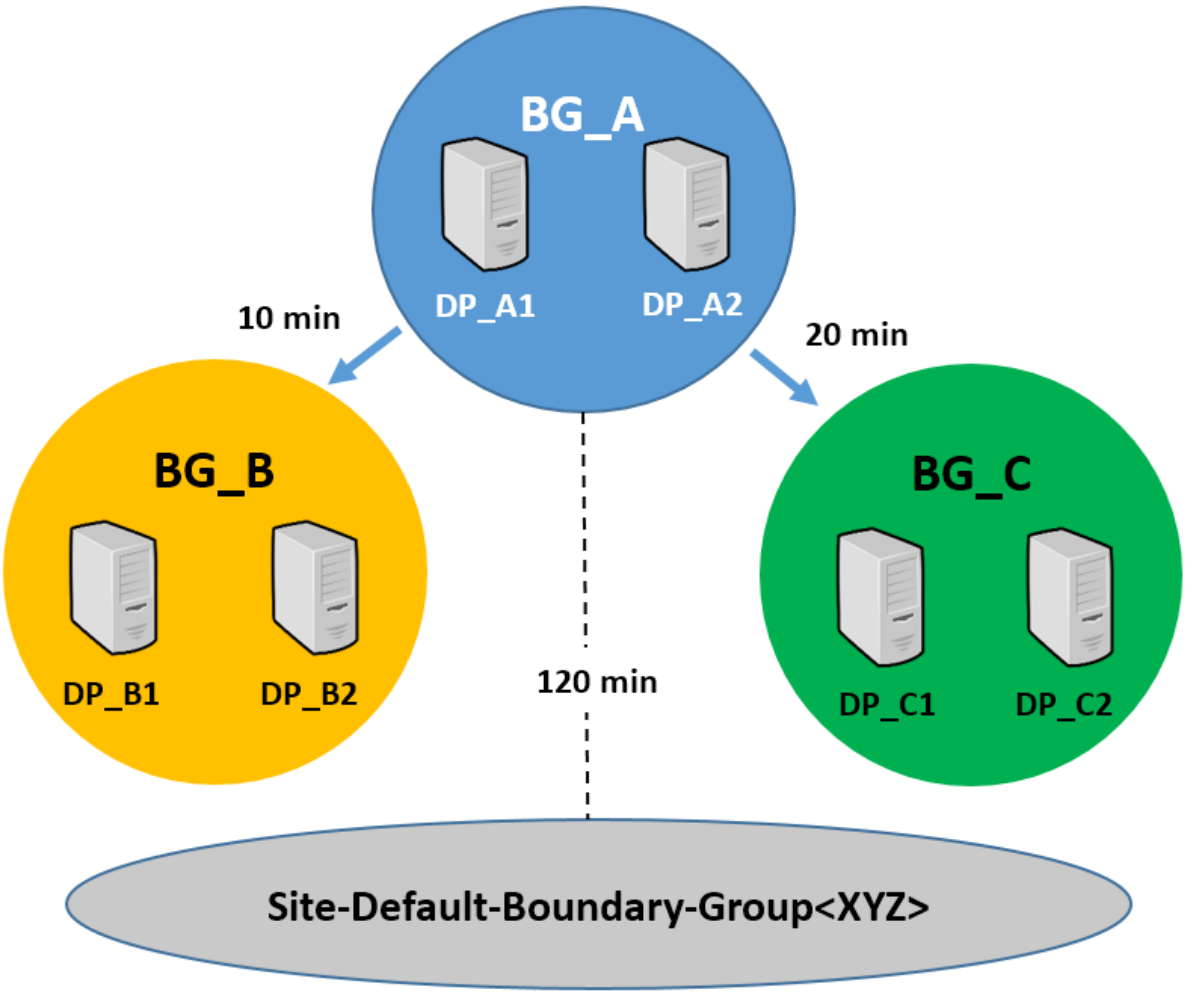
Vous créez trois groupes de limites qui ne partagent pas de limites ni de serveurs de système de site :

- Groupe BG_A avec les points de distribution DP_A1 et DP_A2 associés au groupe
- Groupe BG_B avec les points de distribution DP_B1 et DP_B2 associés au groupe
- Groupe BG_C avec les points de distribution DP_C1 et DP_C2 associés au groupe

Ajoutez les emplacements réseau de vos clients en tant que limites uniquement au groupe de limites BG_A. Configurez ensuite des relations à partir de ce groupe de limites vers les deux autres groupes de limites :

- Configurez des points de distribution pour le premier groupe *voisin* (BG_B) à utiliser après 10 minutes. Ce groupe contient les points de distribution DP_B1 et DP_B2. Les deux sont correctement connectés aux emplacements des premiers groupes de limites.
- Configurez le deuxième groupe *voisin* (BG_C) à utiliser après 20 minutes. Ce groupe contient les points de distribution DP_C1 et DP_C2. Les deux se trouvent sur un réseau étendu à distance des deux autres groupes de limites.
- Ajoutez également un point de distribution supplémentaire qui se trouve sur le serveur de site au groupe de limites de site par défaut du site. Ce serveur est l'emplacement source de contenu que vous préférez le moins, mais il se trouve au milieu de tous les groupes de limites.

Exemple de groupes de limites et de durées de secours :




Avec cette configuration :

- Le client commence la recherche de contenu dans les points de distribution de son groupe de limites *actif* (BG_A). Il passe deux minutes dans chaque point avant de passer au suivant dans le groupe. Le pool des emplacements sources de contenu valides du client inclut DP_A1 et DP_A2.
- Si le client ne parvient pas à trouver le contenu dans son groupe de limites *actuel* après une recherche de 10 minutes, il ajoute alors les points de distribution du groupe de limites BG_B à sa recherche. Il continue ensuite à rechercher le contenu dans un point de distribution de son pool combiné de serveurs. Ce pool inclut maintenant ceux des groupes de limites BG_A et BG_B. Le client continue de contacter chaque point de distribution pendant deux minutes avant de passer au serveur suivant de son pool. Le pool des emplacements sources de contenu valides du client inclut DP_A1, DP_A2, DP_B1 et DP_B2.
- Après 10 minutes supplémentaires (20 minutes au total), si le client n'a toujours pas trouvé un point de distribution avec du contenu, il étend son pool de serveurs disponibles pour inclure ceux du deuxième groupe *voisin*, le groupe de limites BG_C. Le client dispose désormais de six points de distribution pour sa recherche (DP_A1, DP_A2, DP_B2, DP_B2, DP_C1 et DP_C2). Il continue de changer de point de distribution toutes les deux minutes jusqu'à ce qu'il trouve le contenu.
- Si le client n'a pas trouvé le contenu après un total de 120 minutes, il revient en arrière pour inclure le *groupe de limites de site par défaut* dans le cadre de sa recherche continue. Le pool inclut désormais tous les points de distribution des trois groupes de limites configurés et le point de distribution final situé sur le serveur de site. Le client continue alors sa recherche de contenu, en changeant de point de distribution toutes les deux minutes jusqu'à ce qu'il trouve le contenu.

En configurant les différents groupes voisins pour être disponibles à différents moments, vous contrôlez quand des

points de distribution spécifiques sont ajoutés en tant qu'emplacement source de contenu. Le client utilise le secours sur le groupe de limites de site par défaut comme filet de protection pour le contenu qui n'est pas disponible à partir de tout autre emplacement.

## Modifications par rapport aux versions antérieures

Voici les principales modifications apportées aux groupes de limites et à la façon dont les clients recherchent le contenu dans Configuration Manager Current Branch. La plupart de ces modifications et concepts fonctionnent ensemble.

- Les configurations rapides ou lentes sont supprimées : vous ne configurez plus des points de distribution individuels pour être rapides ou lents. Au lieu de cela, chaque système de site associé à un groupe de limites est traité de la même façon. En raison de cette modification, l'onglet **References** (Références) des propriétés du groupe de limites ne prend plus en charge la configuration rapide ou lente.
- Nouveau groupe de limites par défaut sur chaque site : chaque site principal possède un nouveau groupe de limites par défaut nommé ***Groupe-limites-site-défaut<code_site>***. Quand un client n'est pas à un emplacement réseau affecté à un groupe de limites, il utilise les systèmes de site associés au groupe par défaut à partir de son site affecté. Envisagez d'utiliser ce groupe de limites en remplacement de la notion d'emplacement de secours pour le contenu.

    - **Allow fallback source locations for content** (Autoriser les emplacements sources de secours pour le contenu) est supprimé : vous ne configurez plus explicitement un point de distribution de secours à utiliser. Les options de configuration de ce paramètre sont supprimées de la console.

      En outre, le résultat de la définition du paramètre **Autoriser les clients à utiliser un emplacement source de secours pour le contenu** sur un type de déploiement pour les applications a changé. Ce paramètre sur un type de déploiement permet maintenant à un client d'utiliser le groupe de limites de site par défaut comme emplacement source de contenu.

    - Relations de groupes de limites : chaque groupe de limites peut être lié à un ou plusieurs groupes de limites supplémentaires. Ces liens forment des relations qui sont configurées sous le nouvel onglet des propriétés du groupe de limites nommé **Relations** :

        - Chaque groupe de limites auquel un client est directement associé est appelé groupe de limites **actuel**.
        - Tout groupe de limites qu'un client peut utiliser en raison d'une association entre le groupe de limites *actif* de ce client et un autre groupe est appelé groupe de limites **voisin**.
        - Sous l'onglet **Relations**, ajoutez des groupes de limites à utiliser comme groupe de limites *voisin*. Configurez également un délai en minutes de secours. Quand un client ne parvient pas à trouver le contenu à partir d'un point de distribution dans le groupe *actif*, ce délai détermine quand il doit commencer à effectuer des recherches dans les emplacements de contenu de ces groupes de limites *voisins*.

          Quand vous ajoutez ou modifiez la configuration d'un groupe de limites, vous avez la possibilité de bloquer le secours sur ce groupe de limites spécifique à partir du groupe actif que vous configurez.

      Pour utiliser la nouvelle configuration, définissez des associations explicites (liens) entre un groupe de limites et un autre. Configurez tous les points de distribution de ce groupe associé avec le même délai en minutes. Quand un client ne parvient pas à trouver une source de contenu dans son groupe de limites *actif*, la durée que vous configurez détermine quand il doit commencer à rechercher des sources de contenu dans son groupe de limites voisin.

      En plus des groupes de limites que vous configurez explicitement, chaque groupe de limites a un lien implicite vers le groupe de limites de site par défaut. Ce lien devient actif après 120 minutes. Ensuite,

le groupe de limites de site par défaut devient un groupe de limites voisin. Ce comportement permet aux clients d'utiliser les points de distribution associés à ce groupe de limites comme emplacements sources de contenu.

Ce comportement remplace ce qui était précédemment désigné sous le nom de secours pour le contenu. Remplacez ce comportement par défaut de 120 minutes en associant explicitement le groupe de limites de site par défaut à un groupe *actif*. Définissez une durée spécifique en minutes ou bloquez totalement le secours pour empêcher son utilisation.

- Les clients tentent d'obtenir le contenu à partir de chaque point de distribution pendant deux minutes au maximum : quand un client recherche un emplacement source de contenu, il tente d'accéder à chaque point de distribution pendant deux minutes avant d'essayer ensuite un autre point de distribution. Ce comportement représente un changement par rapport aux versions précédentes où les clients tentaient de se connecter à un point de distribution pendant deux heures au maximum.
  - Les clients sélectionnent au hasard le premier point de distribution dans le pool des serveurs disponibles du groupe (ou des groupes) de limites *actif(s)* du client.
  - Après deux minutes, si le client n'a pas trouvé le contenu, il bascule vers un nouveau point de distribution et tente d'obtenir le contenu de ce serveur. Ce processus se répète toutes les deux minutes jusqu'à ce que le client trouve le contenu ou atteigne le dernier serveur dans son pool.
  - Si un client ne peut pas trouver un emplacement source de contenu valide dans son pool *actif* avant la période de secours sur un groupe de limites *voisin*, le client ajoute alors les points de distribution de ce groupe *voisin* à la fin de sa liste actuelle. Il effectue ensuite des recherches dans le groupe étendu d'emplacements sources qui inclut les points de distribution des deux groupes de limites.

    > **TIP**
    > Quand vous créez un lien explicite entre le groupe de limites actif et le groupe de limites de site par défaut, puis définissez une durée de secours inférieure à celle d'un lien vers un groupe de limites voisin, les clients commencent à effectuer des recherches dans les emplacements sources du groupe de limites de site par défaut avant d'inclure le groupe voisin.

  - Quand le client ne parvient pas à obtenir le contenu du dernier serveur dans le pool, il recommence le processus.

## Procédures pour les groupes de limites

**Pour créer un groupe de limites**

1. Dans la console Configuration Manager, cliquez sur **Administration** > **Configuration de la hiérarchie** > **Groupes de limites**.
2. Dans l'onglet **Accueil** , dans le groupe **Créer** , cliquez sur **Créer un groupe limite**.
3. Dans la boîte de dialogue **Créer un groupe limite**, sélectionnez l'onglet **Général** et spécifiez un **Nom** pour ce groupe de limites.
4. Cliquez sur **OK** pour enregistrer le nouveau groupe de limites.

**Pour configurer un groupe de limites**

1. Dans la console Configuration Manager, cliquez sur **Administration** > **Configuration de la hiérarchie** > **Groupes de limites**.
2. Sélectionnez le groupe de limites à modifier.
3. Dans l'onglet **Accueil** , dans le groupe **Propriétés** , cliquez sur **Propriétés**.

4. Dans la boîte de dialogue **Propriétés** du groupe de limites, sélectionnez l'onglet **Général** pour modifier les limites membres de ce groupe de limites :

   - Pour ajouter des limites, cliquez sur **Ajouter**, cochez la case d'une ou plusieurs limites et cliquez sur **OK**.
   - Pour supprimer des limites, sélectionnez la limite à supprimer, puis cliquez sur **Supprimer**.

5. Sélectionnez l'onglet **Références** pour modifier l'attribution de site et la configuration de serveur de système de site associée :

   - Pour autoriser l'utilisation de ce groupe de limites par des clients pour l'attribution de site, sélectionnez **Utiliser ce groupe limite pour l'attribution de site**. Sélectionnez ensuite un site dans la liste déroulante **Site attribué**.
   - Pour configurer les serveurs de système de site associés à ce groupe de limites

   a. Cliquez sur **Ajouter**, puis cochez la case d'un ou plusieurs serveurs. Les serveurs sont ajoutés en tant que serveurs de système de site associés à ce groupe de limites. Seuls les serveurs sur lesquels un rôle de système de site pris en charge est installé sont disponibles.

   > **NOTE**
   > Vous pouvez sélectionner n'importe quelle combinaison de systèmes de site disponibles à partir de n'importe quel site dans la hiérarchie. Les systèmes de site sélectionnés figurent sous l'onglet **Systèmes de site** des propriétés de chaque limite appartenant à ce groupe de limites.

   b. Pour supprimer un serveur de ce groupe de limites, sélectionnez le serveur, puis cliquez sur **Supprimer**.

   > **NOTE**
   > Pour ne plus utiliser ce groupe de limites pour l'association des systèmes de site, supprimez tous les serveurs répertoriés en tant que serveurs de système de site associés.

6. Pour configurer le comportement de secours, sélectionnez l'onglet **Relations** :

   - Cliquez sur **Ajouter**, puis sélectionnez le groupe de limites à configurer.
   - Définissez une durée de secours pour les points de distribution. Après cette période de temps, les clients dans le groupe de limites pour lequel vous configurez des relations peuvent commencer à rechercher du contenu à partir des points de distribution du groupe de limites que vous ajoutez.
   - Pour ne pas avoir recours à un groupe de limites spécifique, notamment le *groupe de limites du site par défaut* qui est configuré par défaut, sélectionnez le groupe de limites et cochez la case **Jamais d'action de secours**.

7. Cliquez sur **OK** pour fermer les propriétés du groupe de limites et enregistrer la configuration.

#### Pour associer un serveur de système de site à un groupe de limites

1. Dans la console Configuration Manager, cliquez sur **Administration** > **Configuration de la hiérarchie** > **Groupes de limites**.
2. Sélectionnez le groupe de limites à modifier.
3. Dans l'onglet **Accueil** , dans le groupe **Propriétés** , cliquez sur **Propriétés**.
4. Dans la boîte de dialogue **Propriétés** du groupe de limites, sélectionnez l'onglet **Références** .

5. Sous **Sélectionner des serveurs de système de site**, cliquez sur **Ajouter**. Sélectionnez les serveurs de système de site à associer à ce groupe de limites, puis cliquez sur **OK**.

6. Cliquez sur **OK** pour fermer la boîte de dialogue et enregistrer la configuration du groupe de limites.

#### Pour configurer un site de secours pour l'attribution automatique de site

1. Dans la console Configuration Manager, cliquez sur **Administration** > **Configuration de site** > **Sites**.

2. Dans l'onglet **Accueil** , dans le groupe **Sites** , cliquez sur **Paramètres de hiérarchie**.

3. Dans l'onglet **Général** , cochez la case **Utiliser un site de secours**, puis sélectionnez un site dans la liste déroulante **Site de secours** .

4. Cliquez sur **OK** pour enregistrer la configuration.

#### Pour activer l'utilisation des points de gestion préférés

1. Dans la console Configuration Manager, cliquez sur **Administration** > **Configuration de site** > **Sites** puis, sous l'onglet **Accueil**, sélectionnez **Paramètres de hiérarchie**.

2. Sous l'onglet **Général** des paramètres de hiérarchie, sélectionnez **Les clients préfèrent utiliser les points de gestion spécifiés dans les groupes de limites**.

3. Cliquez sur **OK** pour fermer la boîte de dialogue et enregistrer la configuration.

# Se préparer à l'utilisation de groupes de disponibilité SQL Server Always On avec Configuration Manager

22/06/2018 • 24 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Préparez System Center Configuration Manager afin d'utiliser des groupes de disponibilité SQL Server Always On comme solution de haute disponibilité et de récupération d'urgence pour la base de données de site. Configuration Manager prend en charge des groupes de disponibilité :

- Sur les sites principaux et sur le site d'administration centrale.
- Localement ou dans Microsoft Azure.

Quand vous utilisez des groupes de disponibilité dans Microsoft Azure, vous pouvez encore augmenter la disponibilité de la base de données de votre site en utilisant des *groupes de disponibilité Azure*. Pour plus d'informations sur les groupes à haute disponibilité Azure, consultez Gestion de la disponibilité des machines virtuelles.

> **IMPORTANT**
> Avant de continuer, familiarisez-vous avec la configuration de SQL Server et les groupes de disponibilité SQL Server. Les informations ci-dessous font référence à la bibliothèque de documentation et aux procédures SQL Server.

## Scénarios pris en charge

Voici les scénarios pris en charge pour l'utilisation de groupes de disponibilité avec Configuration Manager. Vous trouverez les détails et les procédures pour chaque scénario à la rubrique Configurer des groupes de disponibilité pour Configuration Manager.

- Créez un groupe de disponibilité pour une utilisation avec Configuration Manager.
- Configurez un site pour utiliser un groupe de disponibilité.
- Ajouter ou supprimer des membres de réplica synchrone à partir d'un groupe de disponibilité qui héberge une base de données de site.
- Configurer des réplicas avec validation asynchrone (nécessite Configuration Manager version 1706 ou ultérieure).
- Récupérer un site à partir d'un réplica avec validation asynchrone (nécessite Configuration Manager version 1706 ou ultérieure).
- Déplacez une base de données de site d'un groupe de disponibilité vers une instance par défaut ou nommée d'un serveur SQL Server autonome.

## Prérequis

Les conditions préalables suivantes s'appliquent à tous les scénarios. Si d'autres conditions préalables s'appliquent à un scénario spécifique, ces conditions seront détaillées dans ce scénario.

**Comptes et autorisations de Configuration Manager**

**Serveur de site pour l'accès à un membre réplica :**
Le compte d'ordinateur du serveur de site doit être membre du groupe **Administrateurs locaux** sur chaque ordinateur membre du groupe de disponibilité.

**SQL Server**

**Version :**
Chaque réplica du groupe de disponibilité doit exécuter une version de SQL Server prise en charge par votre version de Configuration Manager. S'ils sont pris en charge par SQL Server, les différents nœuds d'un groupe de disponibilité peuvent exécuter des versions différentes de SQL Server.

**Édition :**
Vous devez utiliser une édition *Enterprise* de SQL Server.

**Compte :**
Chaque instance de SQL Server peut s'exécuter sous un compte d'utilisateur de domaine (**compte de service**) ou un compte n'appartenant pas à un domaine. Chaque réplica d'un groupe peut avoir une configuration différente. Les meilleures pratiques SQL Server recommandent d'utiliser un compte avec les autorisations les plus basses possible.

- Pour configurer les comptes de service et les autorisations pour SQL Server 2016, consultez Configurer les comptes de service Windows et les autorisations sur MSDN.
- Pour utiliser un compte n'appartenant pas à un domaine, vous devez utiliser des certificats. Pour plus d'informations, consultez Utiliser des certificats pour un point de terminaison de mise en miroir de bases de données (Transact-SQL).

Pour plus d'informations, consultez Créer un point de terminaison de mise en miroir de base de données pour les groupes de disponibilité Always On.

**Configurations du groupe de disponibilité**

**Membres du réplica :**

- Le groupe de disponibilité doit avoir un réplica principal.
- Avant la version 1706, vous pouviez avoir jusqu'à deux réplicas secondaires synchrones.
- À compter de la version 1706, vous pouvez utiliser les mêmes nombre et type de réplicas dans un groupe de disponibilité pris en charge par la version de SQL Server que vous utilisez.
- À partir de la version 1706, vous pouvez utiliser un réplica avec validation asynchrone pour récupérer votre réplica synchrone. Consultez les options de récupération de base de données de site dans la rubrique Sauvegarde et récupération pour plus d'informations sur la façon d'y parvenir.

  Caution

  Configuration Manager ne prend pas en charge le basculement pour utiliser le réplica avec validation asynchrone comme base de données de votre site. Étant donné que Configuration Manager ne valide pas l'état du réplica avec validation asynchrone pour vérifier qu'il est à jour, et que, par définition, un réplica de ce type peut être désynchronisé, l'utilisation d'un réplica avec validation asynchrone comme base de données de site risque de compromettre l'intégrité de votre site et de ses données.

Chaque membre du réplica doit :

- utiliser **l'instance par défaut**;
  *Depuis la version 1702, vous pouvez utiliser une **instance nommée**.*
- définir **Connexions dans le rôle principal** sur **Oui**
- définir **Secondaire accessible en lecture** sur **Oui**
- être configuré pour le **basculement manuel**.

> **TIP**
> Configuration Manager prend en charge l'utilisation de réplicas synchrones de groupe de disponibilité quand il est configuré pour le **Basculement automatique**. Toutefois, **Basculement manuel** doit être défini lorsque :
>
> - Vous exécutez le programme d'installation pour spécifier l'utilisation de la base de données de site dans le groupe de disponibilité.
> - Lorsque vous installez une mise à jour dans Configuration Manager (pas seulement les mises à jour qui s'appliquent à la base de données de site).

**Emplacement du membre du réplica :**
Tous les réplicas d'un groupe de disponibilité doivent être hébergés localement ou sur Microsoft Azure. Un groupe incluant un membre local et un membre dans Azure n'est pas pris en charge.

Lorsque vous configurez un groupe de disponibilité dans Azure et que le groupe se situe derrière un équilibreur de charge interne ou externe, les éléments suivants constituent les ports par défaut que vous devez ouvrir pour permettre au programme d'installation d'accéder à chaque réplica :

- Mappeur de point de terminaison RCP - **TCP 135**
- Server Message Block – **TCP 445**
  *Vous pouvez supprimer ce port après le déplacement de la base de données. Depuis la version 1702, ce port n'est plus nécessaire.*
- SQL Server Service Broker : **TCP 4022**
- SQL sur TCP : **TCP 1433**

Une fois l'installation terminée, les ports suivants doivent rester accessibles :

- SQL Server Service Broker : **TCP 4022**
- SQL sur TCP : **TCP 1433**

Depuis la version 1702, vous pouvez utiliser des ports personnalisés pour ces configurations. Les mêmes ports doivent être utilisés par le point de terminaison et sur tous les réplicas du groupe de disponibilité.

**Écouteur :**
Le groupe de disponibilité doit avoir au moins un **écouteur de groupe de disponibilité**. Le nom virtuel de cet écouteur est utilisé quand vous configurez Configuration Manager pour utiliser la base de données du site dans le groupe de disponibilité. Bien qu'un groupe de disponibilité puisse contenir plusieurs écouteurs, Configuration Manager ne peut en utiliser qu'un seul. Consultez Créer ou configurer un écouteur de groupe de disponibilité (SQL Server) pour plus d'informations.

**Chemins d'accès au fichier :**
Quand vous exécutez le programme d'installation de Configuration Manager pour configurer un site afin d'utiliser la base de données dans un groupe de disponibilité, chaque serveur réplica secondaire doit avoir un chemin de fichier SQL Server identique à celui utilisé pour les fichiers de base de données du site figurant sur le réplica principal actuel.

- À défaut de chemin identique, le programme d'installation ne peut pas ajouter l'instance du groupe de disponibilité comme nouvel emplacement de la base de données du site.
- En outre, le compte de service SQL Server local doit avoir une autorisation **Contrôle total** sur ce dossier.

Les serveurs de réplication secondaires doivent avoir ce chemin de fichier uniquement pendant que vous utilisez le programme d'installation pour spécifier l'instance de base de données dans le groupe de disponibilité. Une fois que le programme d'installation a configuré la base de données du site dans le groupe de disponibilité, vous pouvez supprimer le chemin inutilisé des serveurs de réplication secondaires.

Par exemple, examinez le scénario suivant :

- Vous créez un groupe de disponibilité qui utilise trois serveurs SQL Server.
- Votre serveur de réplication principal est une nouvelle installation de SQL Server 2014. Par défaut, les fichiers .MDF et .LDF de la base de données sont stockés dans C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA.
- Vos deux serveurs de réplication secondaires ont été mis à niveau vers SQL Server 2014 à partir de versions antérieures et conservent le chemin de fichier d'origine pour stocker les fichiers de base de données, à savoir C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA.
- Avant de tenter de déplacer la base de données du site vers ce groupe de disponibilité, sur chaque serveur de réplication secondaire, vous devez créer le prochain chemin de fichier, même si les réplicas secondaires n'utilisent pas cet emplacement de fichier, à savoir C:\Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA (il s'agit du même chemin que celui en cours d'utilisation sur le réplica principal).
- Vous accordez ensuite au compte de service SQL Server sur chaque réplica secondaire un accès en contrôle total à l'emplacement du fichier qui vient d'être créé sur ce serveur.
- Vous pouvez désormais exécuter correctement le programme d'installation de Configuration Manager pour configurer le site afin qu'il utilise la base de données du site figurant dans le groupe de disponibilité.

**Configurer la base de données sur un nouveau réplica :**
La base de données de chaque réplica doit être définie avec les éléments suivants :

- **Intégration du CLR** doit être *activé*
- **Max text repl size** doit être *2147483647*
- Le propriétaire de la base de données doit être le *compte SA*
- **TRUSTWORTY** doit être **ON**
- **Service Broker** doit être *activé*

Vous pouvez appliquer ces configurations uniquement à un réplica principal. Pour configurer un réplica secondaire, vous devez d'abord basculer le réplica principal vers le réplica secondaire afin de définir ce dernier comme nouveau réplica principal.

Utilisez la documentation SQL Server lorsque cela est nécessaire pour vous aider à configurer les paramètres. Par exemple, consultez TRUSTWORTHY ou Intégration du CLR dans la documentation SQL Server.

**Script de vérification**

Vous pouvez exécuter le script suivant afin de vérifier les configurations de base de données pour les réplicas principal et secondaire. Avant de pouvoir résoudre un problème sur un réplica secondaire, vous devez le modifier afin de le définir comme réplica principal.

```
SET NOCOUNT ON

DECLARE @dbname NVARCHAR(128)

SELECT @dbname = sd.name FROM sys.sysdatabases sd WHERE sd.dbid = DB_ID()

IF (@dbname = N'master' OR @dbname = N'model' OR @dbname = N'msdb' OR @dbname = N'tempdb' OR @dbname =
N'distribution' ) BEGIN
RAISERROR(N'ERROR: Script is targetting a system database.  It should be targeting the DB you created
instead.', 0, 1)
GOTO Branch_Exit;
END ELSE
PRINT N'INFO: Targetted database is ' + @dbname + N'.'

PRINT N'INFO: Running verifications....'

IF NOT EXISTS (SELECT * FROM sys.configurations c WHERE c.name = 'clr enabled' AND c.value_in_use = 1)
PRINT N'ERROR: CLR is not enabled!'
ELSE
PRINT N'PASS: CLR is enabled.'

DECLARE @repltable TABLE (
name nvarchar(max),
minimum int,
maximum int,
config_value int,
run_value int )

INSERT INTO @repltable
EXEC sp_configure 'max text repl size (B)'

IF NOT EXISTS(SELECT * from @repltable where config_value = 2147483647 and run_value = 2147483647 )
PRINT N'ERROR: Max text repl size is not correct!'
ELSE
PRINT N'PASS: Max text repl size is correct.'

IF NOT EXISTS (SELECT db.owner_sid FROM sys.databases db WHERE db.database_id = DB_ID() AND db.owner_sid =
0x01)
PRINT N'ERROR: Database owner is not sa account!'
ELSE
PRINT N'PASS: Database owner is sa account.'

IF NOT EXISTS( SELECT * FROM sys.databases db WHERE db.database_id = DB_ID() AND db.is_trustworthy_on = 1 )
PRINT N'ERROR: Trustworthy bit is not on!'
ELSE
PRINT N'PASS: Trustworthy bit is on.'

IF NOT EXISTS( SELECT * FROM sys.databases db WHERE db.database_id = DB_ID() AND db.is_broker_enabled = 1 )
PRINT N'ERROR: Service broker is not enabled!'
ELSE
PRINT N'PASS: Service broker is enabled.'

IF NOT EXISTS( SELECT * FROM sys.databases db WHERE db.database_id = DB_ID() AND
db.is_honor_broker_priority_on = 1 )
PRINT N'ERROR: Service broker priority is not set!'
ELSE
PRINT N'PASS: Service broker priority is set.'

PRINT N'Done!'

Branch_Exit:
```

## Limitations et problèmes connus

Les limitations suivantes s’appliquent à tous les scénarios.

**Configurations et options SQL Server qui ne sont pas prises en charge :**

- **Groupes de disponibilité de base**
  Depuis l'édition standard de SQL Server 2016, les groupes de disponibilité de base ne prennent pas en charge les accès en lecture aux réplicas secondaires, ce qui est obligatoire pour une utilisation avec Configuration Manager.
- **Instance de cluster de basculement**
  Les instances de cluster de basculement ne sont pas prises en charge pour un réplica que vous utilisez avec Configuration Manager.
- **MultiSubnetFailover**
  L'utilisation d'un groupe de disponibilité dans une configuration à plusieurs sous-réseaux ou avec la chaîne de connexion du mot clé MutliSubnetFailover n'est pas prise en charge.

**Serveurs SQL qui hébergent des groupes de disponibilité supplémentaires :**
Avant la version 1610 de Configuration Manager, si un groupe de disponibilité sur un serveur SQL Server héberge un ou plusieurs groupes de disponibilité en plus du groupe que vous utilisez pour Configuration Manager, chaque réplica de chacun des ces groupes de disponibilité supplémentaires doit disposer des configurations suivantes lorsque vous exécutez le programme d'installation de Configuration Manager ou installez une mise à jour pour Configuration Manager :

- **basculement manuel**
- **autoriser toute connexion en lecture seule**

**Utilisation d'une base de données non prise en charge :**

- **Configuration Manager prend uniquement en charge la base de données de site dans un groupe de disponibilité :** Les éléments suivants ne sont pas pris en charge :
  - Base de données Rapports
  - Base de données WSUS
- **Base de données préexistante :** vous ne pouvez pas utiliser la nouvelle base de données créée sur le réplica. Au lieu de cela, vous devez restaurer une copie de base de données Configuration Manager existante vers le réplica principal lors de la configuration d'un groupe de disponibilité.

**Erreurs d'installation dans le fichier ConfigMgrSetup.log :**
Lorsque vous exécutez le programme d'installation pour déplacer une base de données de site vers un groupe de disponibilité, le programme d'installation tente de traiter les rôles de la base de données sur les réplicas secondaires du groupe de disponibilité et consigne les erreurs comme suit :

- ERREUR : erreur SQL Server : [25000][3906][Microsoft][SQL Server Native Client 11.0][SQL Server]Échec de la mise à jour de la base de données « CM_AAA », car celle-ci est en lecture seule. Installation de Configuration Manager 21/1/2016 16:54:59 7344 (0x1CB0)

Ces erreurs peuvent être ignorées sans problème.

## Modifications pour la sauvegarde de site

**Sauvegarder des fichiers de base de données :**
Quand une base de données du site s'exécute dans un groupe de disponibilité, vous devez exécuter la tâche intégrée de maintenance de serveur **Sauvegarder le site** pour sauvegarder les paramètres et fichiers Configuration Manager courants. Toutefois, évitez d'utiliser les fichiers .MDF ou .LDF créés par cette sauvegarde. Au lieu de cela, effectuez des sauvegardes directes de ces fichiers de base de données à l'aide de SQL Server.

**Journal de transactions :**
Le mode de récupération de la base de données de site doit être défini sur **Complète** (condition requise pour une utilisation dans un groupe de disponibilité). Avec cette configuration, planifiez le monitorage et la gestion de la

taille du journal de transactions de la base de données de site. Dans le mode de récupération complète, les transactions ne sont pas renforcées tant qu'une sauvegarde complète de la base de données ou du journal des transactions n'a pas été effectuée. Consultez Sauvegarde et restauration des bases de données SQL Server pour plus d'informations.

## Modifications pour la récupération de site

Vous pouvez utiliser l'option de récupération de site **Ignorer la récupération de base de données (Utiliser cette option si la base de données de site n'était pas affectée)** si au moins un nœud du groupe de disponibilité reste fonctionnel.

Avant de pouvoir récupérer le site si tous les nœuds d'un groupe de disponibilité ont été perdus, vous devez recréer le groupe de disponibilité. Configuration Manager ne peut pas reconstruire ni restaurer le nœud de disponibilité. Une fois le groupe recréé et une sauvegarde restaurée et reconfigurée, vous pouvez utiliser l'option de récupération de site **Ignorer la récupération de base de données (Utiliser cette option si la base de données de site n'était pas affectée)**.

Pour plus d'informations, consultez Sauvegarde et récupération pour System Center Configuration Manager.

## Modifications pour la création de rapports

**Installez le point de Reporting Services :**
Le point de Reporting Services ne prend pas en charge l'utilisation du nom virtuel d'écouteur du groupe de disponibilité ni l'hébergement de la base de données Reporting services dans un groupe de disponibilité SQL Server Always On :

- Par défaut, l'installation du point de Reporting Services utilise le nom virtuel spécifié en tant qu'écouteur comme **nom du serveur de base de données de site** . Modifiez cette option pour spécifier un nom d'ordinateur et une instance d'un réplica dans le groupe de disponibilité.
- Pour décharger la création de rapports et augmenter la disponibilité lorsqu'un nœud de réplica est en mode hors ligne, vous pouvez installer d'autres points de Reporting Services sur chaque nœud de réplica et configurer chaque point de Reporting Services afin qu'il pointe vers son propre nom d'ordinateur.

Lorsque vous installez un point de Reporting Services sur chaque réplica du groupe de disponibilité, la création de rapports peut toujours se connecter à un serveur de point de rapport actif.

**Basculer le point de Reporting Services utilisé par la console :**
Pour exécuter des rapports, dans la console, accédez à **Surveillance** > **Vue d'ensemble** > **reporting** > **Rapports**, puis choisissez **Options de rapport**. Dans la boîte de dialogue Options de rapport, sélectionnez le point de Reporting Services souhaité.

## Étapes suivantes

Après avoir assimilé les conditions préalables, les limitations et les modifications apportées aux tâches requises lorsque vous utilisez des groupes de disponibilité, consultez Configurer des groupes de disponibilité pour Configuration Manager afin de connaître les procédures d'installation et de configuration de votre site pour utiliser des groupes de disponibilité.

# Configurer des groupes de disponibilité SQL Server Always On pour Configuration Manager

22/06/2018 • 19 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez les informations de cette rubrique pour configurer et gérer des groupes de disponibilité avec Configuration Manager.

Avant de commencer :

- Familiarisez-vous avec les informations de la rubrique Se préparer à l'utilisation de groupes de disponibilité SQL Server Always On avec Configuration Manager.
- Familiarisez-vous avec la documentation de SQL Server qui traite de l'utilisation des groupes de disponibilité et des procédures connexes. Ces informations sont requises pour effectuer les scénarios suivants.

> **TIP**
> Les liens de cette rubrique pour SQL Server pointent vers le contenu pour SQL Server 2016. Si vous n'utilisez pas cette version de SQL Server, consultez la documentation de votre version.

## Créer et configurer un groupe de disponibilité

Utilisez la procédure suivante pour créer un groupe de disponibilité, puis déplacez une copie de la base de données de site vers ce groupe de disponibilité.

Pour effectuer cette procédure, le compte que vous utilisez doit être :

- membre du groupe **Administrateurs locaux** sur chaque ordinateur qui figure dans le groupe de disponibilité.
- **sysadmin** sur chaque instance SQL Server qui héberge la base de données du site.

**Pour créer et configurer un groupe de disponibilité pour Configuration Manager**

1. Utilisez la commande suivante pour arrêter le site Configuration Manager : **Preinst.exe /stopsite**. Pour plus d'informations sur l'utilisation de PreInst.exe, consultez Utilitaire Maintenance de la hiérarchie.

2. Remplacez le mode de sauvegarde **SIMPLE** de la base de données du site par **COMPLÈTE**. Consultez Afficher ou modifier le mode de récupération d'une base de données (SQL Server) dans la documentation de SQL Server. (Les groupes de disponibilité prennent en charge uniquement le mode de récupération COMPLÈTE).

3. Utilisez SQL Server pour créer une sauvegarde complète de la base de données de votre site. Ensuite, effectuez l'une des opérations suivantes, selon que le serveur qui héberge votre base de données de site sera ou non un membre réplica du nouveau groupe de disponibilité :

   - **Sera membre de votre groupe de disponibilité :**
     Si vous utilisez ce serveur en tant que membre réplica principal initial du groupe de disponibilité, il est inutile de restaurer une copie de la base de données de site sur ce serveur ou sur un autre serveur du groupe. La base de données sera déjà en place sur le réplica principal, et SQL Server répliquera la base de données sur les réplicas secondaires à une étape ultérieure.

     - **Ne sera pas membre du groupe de disponibilité :**

Restaurez une copie de la base de données de site sur le serveur qui hébergera le réplica principal du groupe.

Pour plus d'informations sur la façon de procéder, consultez Créer une sauvegarde complète de base de données et Restaurer une sauvegarde de base de données à l'aide de SSMS dans la documentation de SQL Server.

4. Sur le serveur qui hébergera le réplica principal initial du groupe, utilisez l'Assistant Nouveau groupe de disponibilité pour créer le groupe de disponibilité. Dans l'Assistant :

   - Dans la page **Sélectionner une base de données**, sélectionnez la base de données pour votre site Configuration Manager.
   - Dans la page **Spécifier les réplicas** , configurez ce qui suit :
     - **Réplicas :** spécifiez les serveurs qui hébergeront les réplicas secondaires.
     - **Écouteur :** spécifiez le **nom d'écouteur DNS** en tant que nom DNS complet, par exemple **<Serveur_écouteur>.fabrikam.com**. Ce nom est utilisé quand vous configurez Configuration Manager pour utiliser la base de données située dans le groupe de disponibilité.
   - Dans la page **Sélectionner la synchronisation de données initiale** , sélectionnez **Complète**. Après avoir créé le groupe de disponibilité, l'Assistant sauvegarde la base de données primaire et le journal des transactions. Ensuite, il les restaure sur chaque serveur hébergeant un réplica secondaire. (Si vous ne suivez pas cette étape, vous devez restaurer une copie de la base de données du site sur chaque serveur hébergeant un réplica secondaire, et joindre manuellement cette base de données au groupe.)

5. Vérifiez la configuration sur chaque réplica :

   a. Vérifiez que le compte d'ordinateur du serveur de site est un membre du groupe **Administrateurs locaux** sur chaque ordinateur membre du groupe de disponibilité.

   b. Exécutez le script de vérification indiqué dans la configuration requise pour confirmer que la base de données de site est correctement configurée sur chaque réplica.

   c. S'il est nécessaire de définir des configurations sur les réplicas secondaires, vous devez basculer manuellement le réplica principal vers le réplica secondaire avant de continuer. Vous pouvez uniquement configurer la base de données d'un réplica principal. Pour plus d'informations, consultez Effectuer un basculement manuel planifié d'un groupe de disponibilité (SQL Server) dans la documentation de SQL Server.

6. Une fois que tous les réplicas répondent aux conditions requises, le groupe de disponibilité est prêt à être utilisé avec le Configuration Manager.

## Configurer un site pour utiliser la base de données dans le groupe de disponibilité

Après avoir créé et configuré le groupe de disponibilité, utilisez la maintenance de site Configuration Manager pour configurer le site afin d'utiliser la base de données hébergée par le groupe de disponibilité.

L'installation d'un nouveau site avec sa base de données dans un groupe de disponibilité n'est pas prise en charge. Par exemple, si vous utilisez le support 1702 de référence, vous devez installer le site à l'aide d'une seule instance SQL Server. Une fois le site installé, vous pouvez déplacer la base de données de site vers le groupe de disponibilité.

Pour effectuer cette procédure, le compte que vous utilisez pour exécuter le programme d'installation Configuration Manager doit être :

- membre du groupe **Administrateurs locaux** sur chaque ordinateur membre du groupe de disponibilité.
- **sysadmin** sur chaque instance SQL Server qui héberge la base de données du site.

> **IMPORTANT**
> Lorsque vous utilisez Microsoft Intune avec Configuration Manager dans une configuration hybride, le déplacement de la base de données de site vers ou depuis un groupe de disponibilité déclenche une resynchronisation des données avec le cloud. Cette resynchronisation est inévitable.

**Pour configurer un site afin d'utiliser le groupe de disponibilité**

1. Exécutez **Installation de Configuration Manager** à partir de ***<Dossier_installation_site_Configuration_Manager>*\BIN\X64\setup.exe**.
2. Sur la page **Mise en route** , sélectionnez **Effectuer une maintenance de site ou réinitialiser ce site**, puis cliquez sur **Suivant**.
3. Sélectionnez l'option **Modifier la configuration de SQL Server** , puis cliquez sur **Suivant**.
4. Reconfigurez ce qui suit pour la base de données du site :
   - **Nom du serveur SQL Server :** entrez le nom virtuel de l'**écouteur** de groupe de disponibilité que vous avez configuré lors de la création du groupe de disponibilité. Le nom virtuel doit être un nom DNS complet, comme ***<serveur_point_de_terminaison>*.fabrikam.com**.
   - **Instance :** cette valeur doit être vide pour spécifier l'instance par défaut pour l'*écouteur* du groupe de disponibilité. Si la base de données du site actuel s'exécute sur une instance nommée, celle-ci est répertoriée et doit être désactivée.
   - **Base de données :** laissez le nom tel qu'il s'affiche. Il s'agit du nom de la base de données du site actuel.
5. Après avoir fourni les informations relatives au nouvel emplacement de la base de données, exécutez le programme d'installation avec vos processus et configurations normaux.

## Ajouter ou supprimer des membres réplicas synchrones

Si votre base de données de site est hébergée dans un groupe de disponibilité, utilisez les procédures suivantes pour ajouter ou supprimer des membres réplicas synchrones. Pour plus d'informations sur le type et le nombre de réplicas qui sont pris en charge, consultez **Configurations des groupes de disponibilité** sous Prérequis dans la rubrique traitant de la préparation des groupes de disponibilité.

Pour effectuer les procédures suivante, le compte doit que vous utilisez doit être :

- membre du groupe **Administrateurs locaux** sur chaque ordinateur membre du groupe de disponibilité.
- **sysadmin** sur chaque instance SQL Server qui héberge ou hébergera la base de données du site.

**Pour ajouter un nouveau membre réplica synchrone**

Le processus pour ajouter un réplica secondaire à un groupe de disponibilité utilisé avec Configuration Manager peut être complexe et dynamique et passer par des étapes et des procédures qui varient en fonction des environnements. Nous travaillons à améliorer Configuration Manager pour simplifier ce processus. D'ici-là, si vous devez ajouter des réplicas secondaires, consultez le blog suivant sur TechNet pour obtenir de l'aide.

- ConfigMgr 1702 : Ajouter un nœud (réplica secondaire) à un groupe de disponibilité AO SQL existant

**Pour supprimer un membre réplica**

Pour cette procédure, utilisez les informations de Supprimer un réplica secondaire d'un groupe de disponibilité (SQL Server) dans la documentation de SQL Server.

## Configurer un réplica avec validation asynchrone

À partir de Configuration Manager version 1706, vous pouvez ajouter un réplica asynchrone à un groupe de disponibilité que vous utilisez avec Configuration Manager. Pour ce faire, vous n'avez pas besoin d'exécuter les scripts de configuration requis pour configurer un réplica synchrone. (en effet, il n'existe aucune prise en charge pour l'utilisation de ce réplica asynchrone en tant que base de données de site.) Consultez la documentation de SQL Server pour plus d'informations sur l'ajout de réplicas secondaires aux groupes de disponibilité.

## Utiliser le réplica asynchrone pour récupérer votre site

Avec Configuration Manager version 1706 et versions ultérieures, vous pouvez utiliser un réplica asynchrone pour récupérer votre base de données de site. Pour ce faire, vous devez arrêter le site principal actif pour empêcher les écritures supplémentaires sur la base de données de site. Après avoir arrêté le site, vous pouvez utiliser un réplica asynchrone au lieu d'utiliser une base de données récupérée manuellement.

Pour arrêter le site, vous pouvez utiliser l'outil de maintenance hiérarchique pour arrêter les services principaux sur le serveur de site. Utilisez la ligne de commande : **Preinst.exe /stopsite**

L'arrêt du site est équivalent à l'arrêt du service Gestionnaire de composants de site (sitecomp) suivi du service SMS_Executive sur le serveur de site.

## Cesser d'utiliser un groupe de disponibilité

Lorsque vous ne souhaitez plus héberger la base de données de votre site dans un groupe de disponibilité, procédez comme suit. Cela implique de déplacer la base de données de site vers une seule instance SQL Server.

Pour effectuer cette procédure, le compte que vous utilisez doit être :

- membre du groupe **Administrateurs locaux** sur chaque ordinateur membre du groupe de disponibilité
- **sysadmin** sur chaque instance SQL Server qui héberge la base de données du site.

> **IMPORTANT**
> Lorsque vous utilisez Microsoft Intune avec Configuration Manager dans une configuration hybride, le déplacement de la base de données de site vers ou depuis un groupe de disponibilité déclenche une resynchronisation des données avec le cloud. Cette opération est inévitable.

**Pour replacer la base de données du site à partir d'un groupe de disponibilité dans une instance SQL Server unique**

1. Arrêtez le site Configuration Manager à l'aide de la commande suivante : **Preinst.exe /stopsite**. Pour plus d'informations, consultez Outil Maintenance de la hiérarchie.

2. Utilisez SQL Server pour créer une sauvegarde complète de la base de données de votre site à partir du réplica principal. Pour plus d'informations sur la façon de procéder, consultez Créer une sauvegarde complète de base de données (SQL Server) dans la documentation de SQL Server.

3. Si le serveur représentant le réplica principal pour le groupe de disponibilité hébergera l'instance unique de la base de données du site, vous pouvez ignorer cette étape :

   - Utilisez SQL Server pour restaurer la sauvegarde de la base de données du site sur le serveur qui hébergera la base de données du site. Consultez Restaurer une sauvegarde de base de données à l'aide de SSMS dans la documentation de SQL Server.

4. Sur le serveur qui hébergera la base de données de site (le réplica principal ou le serveur sur lequel vous

avez restauré la base de données de site), remplacez le modèle de sauvegarde **Complète** de la base de données par **SIMPLE**. Consultez Afficher ou modifier le mode de récupération d'une base de données (SQL Server) dans la documentation de SQL Server.

5. Exécutez le **programme d'installation de Configuration Manager** à partir de ***<dossier_d'installation_du_site_Configuration_Manager>*** **\BIN\X64\setup.exe**.
6. Sur la page **Mise en route** , sélectionnez **Effectuer une maintenance de site ou réinitialiser ce site**, puis cliquez sur **Suivant**.
7. Sélectionnez l'option **Modifier la configuration de SQL Server** , puis cliquez sur **Suivant**.
8. Reconfigurez ce qui suit pour la base de données du site :
   - **Nom du serveur SQL Server :** entrez le nom du serveur hébergeant actuellement la base de données du site.
   - **Instance :** spécifiez l'instance nommée hébergeant la base de données du site, ou laissez ce champ vide si la base de données se trouve sur l'instance par défaut.
   - **Base de données :** laissez le nom tel qu'il s'affiche. Il s'agit du nom de la base de données du site actuel.
9. Après avoir fourni les informations relatives au nouvel emplacement de la base de données, exécutez le programme d'installation avec vos processus et configurations normaux. Une fois l'exécution du programme d'installation terminée, le site redémarre et commence à utiliser le nouvel emplacement de la base de données.
10. Pour nettoyer les serveurs qui étaient membres du groupe de disponibilité, suivez les instructions de Supprimer un groupe de disponibilité (SQL Server) dans la documentation de SQL Server.

# Utiliser un cluster SQL Server pour la base de données du site System Center Configuration Manager

22/06/2018 • 8 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez utiliser un cluster SQL Server pour héberger la base de données du site System Center Configuration Manager. La base de données du site est le seul rôle de système de site pris en charge sur un cluster de serveurs.

> **IMPORTANT**
> La configuration réussie des clusters SQL Server s'appuie sur la documentation et les procédures fournies dans la bibliothèque de documentation de SQL Server.

Un cluster permet de prendre en charge le basculement et d'améliorer la fiabilité de la base de données de site. Toutefois, il n'offre pas d'autres avantages en matière de traitement ou d'équilibrage de la charge. En fait, une détérioration des performances peut survenir car le serveur de site doit trouver le nœud actif du cluster SQL Server avant de se connecter à la base de données de site.

Avant d'installer Configuration Manager, vous devez préparer le cluster SQL Server pour prendre en charge Configuration Manager. (Voir les prérequis plus loin dans cette section.)

Au cours de l'installation de Configuration Manager, l'enregistreur du service VSS (service de cliché instantané des volumes) est installé sur chaque nœud d'ordinateur physique du cluster Microsoft Windows Server. Cela permet de prendre en charge la tâche de maintenance **Serveur de site de sauvegarde**.

Après l'installation du site, Configuration Manager vérifie toutes les heures la présence de modifications apportées au nœud de cluster. Configuration Manager gère automatiquement toutes les modifications éventuellement détectées qui affectent les installations des composants Configuration Manager (comme un basculement de nœud ou l'ajout d'un nouveau nœud au cluster SQL Server).

## Options prises en charge pour l'utilisation d'un cluster de basculement SQL Server

Les options suivantes sont prises en charge pour les clusters de basculement SQL Server utilisés comme base de données de site :

- Cluster d'instance unique
- Configuration d'instances multiples
- Nœuds actifs multiples
- Instance nommée ou par défaut

Tenez compte des prérequis suivants :

- La base de données du site doit être distante du serveur du site. (Le cluster ne peut pas inclure le serveur système du site.)

- Vous devez ajouter le compte d'ordinateur du serveur de site au groupe Administrateurs local de chaque serveur dans le cluster.
- Pour prendre en charge l'authentification Kerberos, le protocole de communication réseau **TCP/IP** doit être activé pour la connexion réseau de chaque nœud de cluster SQL Server. L'utilisation de**canaux nommés** n'est pas obligatoire, mais peut faciliter la résolution des problèmes d'authentification Kerberos. Les paramètres de protocole réseau sont configurés dans le **Gestionnaire de configuration SQL Server**, sous **Configuration du réseau SQL Server**.
- Si vous utilisez une infrastructure PKI, consultez Configuration requise des certificats PKI pour Configuration Manager, afin de connaître les conditions de certificat quand vous utilisez un cluster SQL Server pour la base de données de site.

Tenez compte des limitations suivantes :

- **Installation et configuration :**
  - Des sites secondaires ne peuvent pas utiliser un cluster SQL Server.
  - Vous n'avez pas la possibilité de spécifier des emplacements de fichier autres que les emplacements par défaut pour la base de données du site quand vous utilisez un cluster SQL Server.
- **Fournisseur SMS :**
  - L'installation d'une instance du fournisseur SMS n'est pas prise en charge sur un cluster SQL Server ou sur un ordinateur utilisé comme nœud SQL Server en cluster.
- **Options de réplication de données :**
  - Si vous envisagez d'utiliser des **vues distribuées**, vous ne pouvez pas utiliser un cluster SQL Server pour héberger la base de données de site.
- **Sauvegarde et récupération :**
  - Configuration Manager ne prend pas en charge la sauvegarde DPM (Data Protection Manager) d'un cluster SQL Server qui utilise une instance nommée. Par contre, il prend en charge la sauvegarde DPM sur un cluster SQL Server qui utilise l'instance par défaut de SQL Server.

## Préparer une instance SQL Server en cluster pour la base de données de site

Voici les tâches principales à effectuer afin de préparer votre base de données de site :

- Créez le cluster virtuel SQL Server pour héberger la base de données du site dans un environnement de cluster Windows Server existant. Pour connaître la procédure d'installation et de configuration d'un cluster SQL Server, consultez la documentation spécifique à votre version de SQL Server. Par exemple, si vous utilisez SQL Server 2008 R2, consultez Installation d'un cluster de basculement SQL Server 2008 R2.
- Sur chaque ordinateur du cluster SQL Server, vous pouvez placer un fichier dans le dossier racine de chaque lecteur sur lequel vous ne voulez pas que Configuration Manager installe les composants du site. Ce fichier doit être nommé **NO_SMS_ON_DRIVE.SMS**. Par défaut, Configuration Manager installe certains composants sur chaque nœud physique pour prendre en charge des opérations telles que la sauvegarde.
- Ajoutez le compte ordinateur du serveur de site au groupe **Administrateurs locaux** de chaque ordinateur du nœud de cluster Windows Server.
- Dans l'instance SQL Server virtuelle, attribuez le rôle SQL Server **administrateur système** au compte d'utilisateur qui exécutera le programme d'installation de Configuration Manager.

**Pour installer un nouveau site avec un serveur SQL Server en cluster**

Pour installer un site qui utilise une base de données de site en cluster, exécutez le programme d'installation de Configuration Manager en suivant votre processus habituel pour installer un site, mais en apportant la modification suivante :

- Dans la page **Informations sur la base de données** , spécifiez le nom de l'instance de cluster SQL Server virtuelle qui doit héberger la base de données du site. L'instance virtuelle remplace le nom de l'ordinateur qui exécute SQL Server.

  > **IMPORTANT**
  > Lorsque vous entrez le nom de l'instance de cluster SQL Server virtuelle, n'entrez pas le nom du serveur Windows Server virtuel créé par le cluster Windows Server. Si vous utilisez le nom du serveur Windows Server virtuel, la base de données de site est installée sur le disque dur local du nœud de cluster Windows Server actif. Cela empêche le basculement en cas d'échec de ce nœud.

# Emplacements personnalisés pour les fichiers de base de données du site System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

System Center Configuration Manager prend en charge les emplacements personnalisés pour les fichiers de base de données SQL Server.

> **NOTE**
> Cette possibilité de spécifier des emplacements de fichiers autres que les emplacements par défaut n'est pas disponible quand vous utilisez un cluster SQL Server.

**Durant l'installation** d'un nouveau site principal ou d'un site d'administration centrale, vous pouvez :

- **Spécifier des emplacements de fichiers autres que ceux par défaut pour la base de données du site** : le programme d'installation de Configuration Manager crée alors la base de données du site en utilisant ces emplacements.
- **Spécifier l'utilisation d'une base de données SQL Server déjà créée qui utilise des emplacements de fichiers personnalisés** : le programme d'installation de Configuration Manager utilise alors cette base de données déjà créée et ses emplacements de fichiers préconfigurés.

**Après l'installation**, vous pouvez modifier l'emplacement des fichiers de base de données du site. Pour ce faire, vous devez arrêter le site et modifier l'emplacement du fichier dans SQL Server :

- Sur le serveur de site Configuration Manager, arrêtez le service **SMS_Executive**.
- Utilisez la documentation de votre version de SQL Server pour savoir comment déplacer une base de données utilisateur. Par exemple, si vous utilisez SQL Server 2014, consultez Déplacer des bases de données utilisateur sur TechNet.
- Après avoir déplacé le fichier de base de données, redémarrez le service **SMS_Executive** sur le serveur de site Configuration Manager.

# Configurer l'administration basée sur des rôles pour System Center Configuration Manager

22/06/2018 • 32 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Dans System Center Configuration Manager, l'administration basée sur des rôles combine des rôles de sécurité, des étendues de sécurité et des regroupements attribués pour définir l'étendue administrative de chaque utilisateur administratif. Une étendue administrative inclut les objets qu'un utilisateur administratif peut afficher dans la console Configuration Manager et les tâches associées à ces objets que cet administrateur est autorisé à exécuter. Les configurations d'administration basée sur des rôles s'appliquent à chaque site dans une hiérarchie.

Si vous n'êtes pas encore familier avec les concepts de l'administration basée sur les rôles, consultez Principes de base de l'administration basée sur des rôles pour System Center Configuration Manager.

Les informations figurant dans les procédures suivantes peuvent vous aider à créer et à configurer une administration basée sur des rôles ainsi que les paramètres de sécurité correspondants :

- Créer des rôles de sécurité personnalisés
- Configurer des rôles de sécurité
- Configurer des étendues de sécurité pour un objet
- Configurer des regroupements pour gérer la sécurité
- Créer un utilisateur administratif
- Modifier l'étendue administrative d'un utilisateur administratif

## Créer des rôles de sécurité personnalisés

Configuration Manager fournit plusieurs rôles de sécurité intégrés. Si vous avez besoin de rôles de sécurité supplémentaires, vous pouvez créer un rôle de sécurité personnalisé à l'aide d'une copie d'un rôle de sécurité existant, que vous modifiez par la suite. Vous pouvez créer un rôle de sécurité personnalisé pour accorder aux utilisateurs administratifs les autorisations de sécurité supplémentaires dont ils ont besoin et qui ne figurent pas dans le rôle de sécurité actuellement attribué. Un rôle de sécurité personnalisé permet de leur accorder uniquement les autorisations dont ils ont besoin sans pour autant leur attribuer un rôle de sécurité avec plus d'autorisations que nécessaire.

Pour créer un rôle de sécurité à l'aide d'un rôle de sécurité existant en tant que modèle, procédez comme suit.

**Pour créer des rôles de sécurité personnalisés**

1. Dans la console Configuration Manager, cliquez sur **Administration**.
2. Dans l'espace de travail **Administration**, développez **Sécurité**, puis choisissez **Rôles de sécurité**.

   Utilisez l'une des procédures suivantes pour créer le rôle de sécurité :

   - Pour créer un rôle de sécurité personnalisé, effectuez les actions suivantes :

     a. Sélectionnez un rôle de sécurité existant à utiliser comme source pour le nouveau rôle de sécurité.

b. Dans l'onglet **Accueil** puis dans le groupe **Rôle de sécurité**, choisissez **Copier**. Vous créez ainsi une copie du rôle de sécurité source.

c. Dans l'Assistant Copier le rôle de sécurité, spécifiez un **Nom** pour le nouveau rôle de sécurité personnalisé.

d. Dans **Attributions d'opérations de sécurité**, développez chaque nœud **Opérations de sécurité** pour afficher les actions disponibles.

e. Pour modifier la configuration d'une opération de sécurité, cliquez sur la flèche vers le bas dans la colonne **Valeur**, puis choisissez **Oui** ou **Non**.

Caution

Lorsque vous configurez un rôle de sécurité personnalisé, veillez à ne pas accorder les autorisations dont les utilisateurs administratifs associés à ce nouveau rôle n'ont pas besoin. Par exemple, la valeur **Modifier** pour l'opération de sécurité **Rôles de sécurité** permet aux utilisateurs administratifs de modifier un rôle auquel ils ont accès, même s'ils ne le possèdent pas.

f. Après avoir configuré les autorisations, choisissez **OK** pour enregistrer le nouveau rôle de sécurité.

- Pour importer un rôle de sécurité exporté à partir d'une autre hiérarchie Configuration Manager, effectuez les actions suivantes :

a. Dans l'onglet **Accueil** puis dans le groupe **Créer**, choisissez **Importer un rôle de sécurité**.

b. Spécifiez le fichier .xml qui contient la configuration du rôle de sécurité que vous souhaitez importer. Choisissez **Ouvrir** pour terminer la procédure et enregistrer le rôle de sécurité.

> **NOTE**
> Après avoir importé un rôle de sécurité, vous pouvez en modifier les propriétés pour changer les autorisations d'objet associées au rôle de sécurité.

## Configurer des rôles de sécurité

Les groupes d'autorisations de sécurité définis pour un rôle de sécurité sont appelés des attributions d'opérations de sécurité. Les attributions d'opérations de sécurité représentent une association de types d'objet et d'actions disponibles pour chaque type d'objet. Vous pouvez modifier les opérations de sécurité disponibles pour un rôle de sécurité personnalisé, mais pas modifier les rôles de sécurité prédéfinis par Configuration Manager.

Utilisez la procédure suivante pour modifier les opérations de sécurité pour un rôle de sécurité.

**Pour modifier des rôles de sécurité**

1. Dans la console Configuration Manager, choisissez **Administration**.
2. Dans l'espace de travail **Administration**, développez **Sécurité**, puis choisissez **Rôles de sécurité**.
3. Sélectionnez le rôle de sécurité personnalisé à modifier.
4. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
5. Choisissez l'onglet **Autorisations**.
6. Dans **Attributions d'opérations de sécurité**, développez chaque nœud **Opérations de sécurité**

pour afficher les actions disponibles.

7. Pour modifier la configuration d'une opération de sécurité, cliquez sur la flèche vers le bas dans la colonne **Valeur**, puis choisissez **Oui** ou **Non**.

   Caution

   Lorsque vous configurez un rôle de sécurité personnalisé, veillez à ne pas accorder les autorisations dont les utilisateurs administratifs associés à ce nouveau rôle n'ont pas besoin. Par exemple, la valeur **Modifier** pour l'opération de sécurité **Rôles de sécurité** permet aux utilisateurs administratifs de modifier un rôle auquel ils ont accès, même s'ils ne le possèdent pas.

8. Après avoir terminé la configuration des attributions de l'opération de sécurité, choisissez **OK** pour enregistrer le nouveau rôle de sécurité.

## Configurer des étendues de sécurité pour un objet

L'association d'une étendue de sécurité à un objet est gérée à partir de l'objet et non à partir de l'étendue de sécurité. Les seules configurations directes prises en charge par l'étendue de sécurité sont les modifications apportées à son nom et à sa description. Pour modifier le nom et la description d'une étendue de sécurité lorsque vous affichez les propriétés d'étendue de sécurité, vous devez disposer de l'autorisation **Modifier** pour l'objet sécurisable **Étendues de sécurité** .

Quand vous créez un objet dans Configuration Manager, il est associé à chaque étendue de sécurité qui est associée aux rôles de sécurité du compte utilisé pour créer l'objet, si ces rôles de sécurité accordent l'autorisation **Créer** ou **Définir l'étendue de sécurité**. Une fois l'objet créé, vous ne pouvez modifier que les étendues de sécurité qui lui sont associées.

Par exemple, un rôle de sécurité accordant l'autorisation de créer un groupe de limites vous est attribué. Lorsque vous créez un groupe de limites, vous n'avez aucune option à laquelle attribuer des étendues de sécurité spécifiques. En revanche, les étendues de sécurité disponibles à partir des rôles de sécurité qui vous sont associés sont attribuées automatiquement au nouveau groupe de limites. Après l'enregistrement du nouveau groupe de limites, vous pouvez modifier les étendues de sécurité qui lui sont associées.

Utilisez la procédure suivante pour configurer les étendues de sécurité attribuées à un objet.

**Pour configurer des étendues de sécurité pour un objet**

1. Dans la console Configuration Manager, sélectionnez un objet qui autorise l'attribution à une étendue de sécurité.
2. Dans l'onglet **Accueil** puis dans le groupe **Classer**, choisissez **Définir des étendues de sécurité**.
3. Dans la boîte de dialogue **Définir des étendues de sécurité** , activez ou désactivez les étendues de sécurité auxquelles cet objet est associé. Chaque objet prenant en charge des étendues de sécurité doit être attribué à une étendue de sécurité au moins.
4. Choisissez **OK** pour enregistrer les étendues de sécurité attribuées.

> **NOTE**
>
> Lorsque vous créez un objet, vous pouvez l'attribuer à plusieurs étendues de sécurité. Pour modifier le nombre d'étendues de sécurité associées à l'objet, vous devez effectuer cette opération une fois l'objet créé.

## Configurer des regroupements pour gérer la sécurité

Aucune procédure de configuration de regroupements n'est disponible pour l'administration basée sur des rôles. Il n'existe pas de configuration d'administration basée sur des rôles pour les regroupements. Vous attribuez des regroupements à un utilisateur administratif lorsque vous le configurez. Les opérations de

sécurité de regroupement qui sont activées dans les rôles de sécurité attribués aux utilisateurs déterminent les autorisations d'un utilisateur administratif sur les regroupements et les ressources de ces derniers (leurs membres).

Lorsqu'un utilisateur administratif dispose d'autorisations sur un regroupement, il dispose également d'autorisations sur des regroupements limités à ce regroupement. Par exemple, votre organisation utilise un regroupement nommé Tous les postes de travail, et il existe un regroupement nommé Tous les bureaux en Amérique du Nord qui est limité au regroupement Tous les postes de travail. Si un utilisateur administratif dispose des autorisations sur Tous les postes de travail, il dispose également des mêmes autorisations sur le regroupement Tous les bureaux en Amérique du Nord.

En outre, un utilisateur administratif ne peut pas utiliser l'autorisation **Supprimer** ou **Modifier** sur un regroupement qui lui est attribué directement. Mais il peut utiliser ces autorisations sur les regroupements limités à ce regroupement. Dans l'exemple précédent, l'utilisateur administratif peut supprimer ou modifier le regroupement Tous les bureaux en Amérique du Nord, mais pas supprimer ou modifier le regroupement Tous les postes de travail.

## Créer un utilisateur administratif

Pour accorder aux personnes ou aux membres d'un groupe de sécurité l'accès pour gérer Configuration Manager, créez un utilisateur administratif dans Configuration Manager et spécifiez le compte Windows de l'utilisateur ou du groupe d'utilisateurs. Au moins un rôle de sécurité et une étendue de sécurité doivent être attribués à chaque utilisateur administratif dans Configuration Manager. Vous pouvez également attribuer des regroupements pour limiter l'étendue administrative de l'utilisateur administratif.

Utilisez les procédures suivantes pour créer de nouveaux utilisateurs administratifs.

#### Pour créer un nouvel utilisateur administratif

1. Dans la console Configuration Manager, choisissez **Administration**.
2. Dans l'espace de travail **Administration**, développez **Sécurité**, puis choisissez **Utilisateurs administratifs**.
3. Dans l'onglet **Accueil** puis dans le groupe **Créer**, choisissez **Ajouter un utilisateur ou un groupe**.
4. Choisissez **Parcourir**, puis sélectionnez le compte d'utilisateur ou le groupe à utiliser pour le nouvel utilisateur administratif.

   > **NOTE**
   > Pour l'administration basée sur la console, seuls les utilisateurs du domaine ou les groupes de sécurité peuvent devenir des utilisateurs administratifs.

5. Dans **Associated security roles (Rôles de sécurité associés)**, choisissez **Ajouter** pour ouvrir la liste des rôles de sécurité disponibles, activez la case à cocher d'un ou de plusieurs rôles de sécurité, puis choisissez **OK**.
6. Sélectionnez l'une des deux options suivantes pour définir le comportement de l'objet sécurisable pour le nouvel utilisateur :

   - **Tous les objets sécurisables pertinents pour les rôles de sécurité auxquels ils sont associés** : cette option associe l'utilisateur administratif à l'étendue de sécurité **Tout** ainsi qu'aux regroupements intégrés de niveau racine pour **Tous les systèmes** et **Tous les utilisateurs et groupes d'utilisateurs**. Les rôles de sécurité attribués à l'utilisateur définissent l'accès aux objets. Les nouveaux objets créés par cet utilisateur administratif sont attribués à l'étendue de sécurité **Par défaut** .

- **Only securable objects in specified security scopes or collections (Seuls les objets sécurisables dans les étendues de sécurité ou les regroupements spécifiés)** : par défaut, cette option associe l'utilisateur administratif à l'étendue de sécurité **Par défaut**, ainsi qu'aux regroupements **Tous les systèmes** et **Tous les utilisateurs et groupes d'utilisateurs**. Toutefois, les étendues de sécurité et les regroupements réels sont limités à ceux qui sont associés au compte que vous avez utilisé pour créer le nouvel utilisateur administratif. Cette option prend en charge l'ajout ou la suppression d'étendues de sécurité et de regroupements pour personnaliser l'étendue administrative de l'utilisateur administratif.

> **IMPORTANT**
> Les options précédentes associent chaque étendue de sécurité et chaque regroupement attribués, à chaque rôle de sécurité attribué à l'utilisateur administratif. Vous pouvez utiliser une troisième option, **Seuls les objets sécurisables définis par les rôles de sécurité de l'utilisateur administratif**, pour associer des rôles de sécurité individuellement à des étendues de sécurité et des regroupements spécifiques. Cette troisième option est disponible après la création du nouvel utilisateur administratif, lorsque vous modifiez l'utilisateur administratif.

7. Selon l'option sélectionnée à l'étape 6, effectuez l'action suivante :

   - Si vous avez sélectionné **Tous les objets sécurisables pertinents pour les rôles de sécurité auxquels ils sont associés**, choisissez **OK** pour terminer cette procédure.
   - Si vous avez sélectionné **Seuls les objets sécurisables dans des étendues de sécurité ou des regroupements spécifiés**, choisissez **Ajouter** pour sélectionner des regroupements et des étendues de sécurité supplémentaires. Vous pouvez également sélectionner un ou plusieurs objets dans la liste, puis choisir **Supprimer** pour les supprimer. Choisissez **OK** pour terminer cette procédure.

## Modifier l'étendue administrative d'un utilisateur administratif

Vous pouvez modifier l'étendue administrative d'un utilisateur administratif en ajoutant ou en supprimant des rôles de sécurité, des étendues de sécurité et des regroupements associés à l'utilisateur. Chaque utilisateur administratif doit être associé à au moins un rôle de sécurité et une étendue de sécurité. Vous devrez peut-être affecter un ou plusieurs regroupements à l'étendue administrative de l'utilisateur. La plupart des rôles de sécurité interagissent avec les regroupements et ne fonctionnent pas correctement sans regroupement attribué.

Lorsque vous modifiez un utilisateur administratif, vous pouvez modifier le comportement des objets sécurisables au niveau de leur association avec les rôles de sécurité attribués. Les trois comportements que vous pouvez sélectionner sont les suivants :

- **Tous les objets sécurisables pertinents pour les rôles de sécurité auxquels ils sont associés** : cette option associe l'utilisateur administratif à l'étendue **Tout** ainsi qu'aux regroupements intégrés de niveau racine pour **Tous les systèmes** et **Tous les utilisateurs et groupes d'utilisateurs**. Les rôles de sécurité attribués à l'utilisateur définissent l'accès aux objets.
- **Seuls les objets sécurisables dans les étendues de sécurité ou les regroupements spécifiés**: cette option associe l'utilisateur administratif aux mêmes étendues de sécurité et regroupements qui sont associés au compte que vous utilisez pour configurer l'utilisateur administratif. Cette option prend en charge l'ajout ou la suppression de rôles de sécurité et de regroupements pour personnaliser l'étendue administrative de l'utilisateur administratif.
- **Seuls les objets sécurisables définis par les rôles de sécurité de l'utilisateur administratif**: cette option permet de créer des associations spécifiées entre des rôles de sécurité individuels et des

étendues de sécurité et regroupements spécifiques pour l'utilisateur.

> **NOTE**
> Cette option est disponible uniquement lorsque vous modifiez les propriétés d'un utilisateur administratif.

La configuration actuelle du comportement de l'objet sécurisable modifie le processus qui vous permet d'attribuer des rôles de sécurité supplémentaires. Utilisez les procédures suivantes, basées sur les différentes options des objets sécurisables, pour vous aider à gérer un utilisateur administratif.

Utilisez la procédure suivante pour afficher et gérer la configuration des objets sécurisables pour un utilisateur administratif.

**Pour afficher et gérer le comportement de l'objet sécurisable pour un utilisateur administratif**

1. Dans la console Configuration Manager, choisissez **Administration**.
2. Dans l'espace de travail **Administration**, développez **Sécurité**, puis choisissez **Utilisateurs administratifs**.
3. Sélectionnez l'utilisateur administratif à modifier.
4. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
5. Choisissez l'onglet **Étendues de sécurité** pour afficher la configuration actuelle des objets sécurisables de cet utilisateur administratif.
6. Pour modifier le comportement de l'objet sécurisable, sélectionnez une nouvelle option pour le comportement de l'objet sécurisable. Après avoir modifié cette configuration, consultez la procédure appropriée pour obtenir des instructions supplémentaires sur la configuration des étendues de sécurité et des regroupements ainsi que des rôles de sécurité pour cet utilisateur administratif.
7. Choisissez **OK** pour terminer la procédure.

Utilisez la procédure suivante pour modifier un utilisateur administratif dont le comportement de l'objet sécurisable est **Tous les objets sécurisables pertinents pour les rôles de sécurité auxquels ils sont associés**.

**Pour l'option : Tous les objets sécurisables pertinents pour les rôles de sécurité auxquels ils sont associés**

1. Dans la console Configuration Manager, choisissez **Administration**.
2. Dans l'espace de travail **Administration**, développez **Sécurité**, puis choisissez **Utilisateurs administratifs**.
3. Sélectionnez l'utilisateur administratif à modifier.
4. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
5. Cliquez sur l'onglet **Étendues de sécurité** afin de confirmer que l'utilisateur administratif est configuré pour **Tous les objets sécurisables pertinents pour les rôles de sécurité auxquels ils sont associés**.
6. Pour modifier les rôles de sécurité attribués, choisissez l'onglet **Rôles de sécurité**.
   - Pour attribuer des rôles de sécurité supplémentaires à cet utilisateur administratif, choisissez **Ajouter**, activez la case à cocher de chaque rôle de sécurité supplémentaire que vous souhaitez attribuer, puis choisissez **OK**.
   - Pour supprimer des rôles de sécurité, sélectionnez-en un ou plusieurs dans la liste, puis choisissez **Supprimer**.

7. Pour modifier le comportement de l'objet sécurisable, choisissez l'onglet **Étendues de sécurité** et sélectionnez une nouvelle option pour le comportement de l'objet sécurisable. Après avoir modifié cette configuration, consultez la procédure appropriée pour obtenir des instructions supplémentaires sur la configuration des étendues de sécurité et des regroupements ainsi que des rôles de sécurité pour cet utilisateur administratif.

   > **NOTE**
   >
   > Lorsque le comportement de l'objet sécurisable est **Tous les objets sécurisables pertinents pour les rôles de sécurité auxquels ils sont associés**, vous ne pouvez ni ajouter ni supprimer d'étendues de sécurité ou de regroupements.

8. Choisissez **OK** pour terminer cette procédure.

Utilisez la procédure suivante pour modifier un utilisateur administratif pour lequel le comportement de l'objet sécurisable est paramétré sur **Seuls les objets sécurisables dans des étendues de sécurité ou des regroupements spécifiés**.

**Pour l'option : Seuls les objets sécurisables dans des étendues de sécurité ou des regroupements spécifiés**

1. Dans la console Configuration Manager, choisissez **Administration**.
2. Dans l'espace de travail **Administration**, développez **Sécurité**, puis choisissez **Utilisateurs administratifs**.
3. Sélectionnez l'utilisateur administratif à modifier.
4. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
5. Choisissez l'onglet **Étendues de sécurité** afin de confirmer que l'utilisateur est configuré pour **Seuls les objets sécurisables dans des étendues de sécurité ou des regroupements spécifiés**.
6. Pour modifier les rôles de sécurité attribués, choisissez l'onglet **Rôles de sécurité**.
   - Pour attribuer des rôles de sécurité supplémentaires à cet utilisateur, choisissez **Ajouter**, activez la case à cocher de chaque rôle de sécurité supplémentaire que vous souhaitez attribuer, puis choisissez **OK**.
   - Pour supprimer des rôles de sécurité, sélectionnez-en un ou plusieurs dans la liste, puis choisissez **Supprimer**.
7. Pour modifier les étendues de sécurité et les regroupements associés aux rôles de sécurité, choisissez l'onglet **Étendues de sécurité**.
   - Pour associer de nouvelles étendues de sécurité ou de nouveaux regroupements à tous les rôles de sécurité attribués à cet utilisateur administratif, choisissez **Ajouter** et sélectionnez l'une des quatre options. Si vous sélectionnez **Étendue de sécurité** ou **Regroupement**, activez la case à cocher d'un ou de plusieurs objets pour terminer cette sélection, puis choisissez **OK**.
   - Pour supprimer une étendue de sécurité ou un regroupement, sélectionnez l'objet puis choisissez **Supprimer**.
8. Choisissez **OK** pour terminer cette procédure.

Utilisez la procédure suivante pour modifier un utilisateur administratif pour lequel le comportement de l'objet sécurisable est paramétré sur **Seuls les objets sécurisables déterminés par les rôles de sécurité de l'utilisateur administratif**.

**Pour l'option : Seuls les objets sécurisables déterminés par les rôles de sécurité de l'utilisateur administratif**

1. Dans la console Configuration Manager, choisissez **Administration**.

2. Dans l'espace de travail **Administration**, développez **Sécurité**, puis choisissez **Utilisateurs administratifs**.
3. Sélectionnez l'utilisateur administratif à modifier.
4. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
5. Choisissez l'onglet **Étendues de sécurité** afin de confirmer que l'utilisateur administratif est configuré pour **Seuls les objets sécurisables dans des étendues de sécurité ou des regroupements spécifiés**.
6. Pour modifier les rôles de sécurité attribués, choisissez l'onglet **Rôles de sécurité**.
   - Pour attribuer des rôles de sécurité supplémentaires à cet utilisateur administratif, choisissez **Ajouter**. Dans la boîte de dialogue **Ajouter un rôle de sécurité**, sélectionnez un ou plusieurs rôles de sécurité disponibles, choisissez **Ajouter**, puis sélectionnez un type d'objet à associer aux rôles de sécurité sélectionnés. Si vous sélectionnez **Étendue de sécurité** ou **Regroupement**, activez la case à cocher d'un ou de plusieurs objets pour terminer cette sélection, puis choisissez **OK**.

     **NOTE**
     Vous devez configurer au moins une étendue sécurité avant que les rôles de sécurité sélectionnés puissent être attribués à l'utilisateur administratif. Lorsque vous sélectionnez plusieurs rôles de sécurité, chaque étendue de sécurité et regroupement que vous configurez est associé à chacun des rôles de sécurité sélectionnés.

   - Pour supprimer des rôles de sécurité, sélectionnez-en un ou plusieurs dans la liste, puis choisissez **Supprimer**.
7. Pour modifier les étendues de sécurité et les regroupements associés à un rôle de sécurité spécifique, choisissez l'onglet **Étendues de sécurité**, sélectionnez le rôle de sécurité, puis choisissez **Modifier**.
   - Pour associer de nouveaux objets à ce rôle de sécurité, choisissez **Ajouter** et sélectionnez le type d'objet à associer aux rôles de sécurité sélectionnés. Si vous sélectionnez **Étendue de sécurité** ou **Regroupement**, activez la case à cocher d'un ou de plusieurs objets pour terminer cette sélection, puis choisissez **OK**.

     **NOTE**
     Vous devez configurer au moins une étendue de sécurité.

   - Pour supprimer une étendue de sécurité ou un regroupement associé à ce rôle de sécurité, sélectionnez l'objet et choisissez **Supprimer**.
   - Lorsque vous avez terminé de modifier les objets associés, choisissez **OK**.
8. Choisissez **OK** pour terminer cette procédure.

   **Caution**
   Lorsqu'un rôle de sécurité accorde aux utilisateurs administratifs l'autorisation de déployer un regroupement, ces utilisateurs administratifs peuvent distribuer des objets depuis n'importe quelle étendue de sécurité pour laquelle il disposent d'autorisations de **Lecture** , même si cette étendue de sécurité est associée à un rôle de sécurité différent.

# Configurer les services Azure à utiliser avec Configuration Manager

22/06/2018 • 24 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez **l'Assistant Services Azure** pour simplifier le processus de configuration des services cloud Azure que vous utilisez avec Configuration Manager. Cet Assistant fournit une expérience de configuration commune en utilisant des inscriptions d'applications web Azure AD (Azure Active Directory). Ces applications fournissent des détails d'abonnement et de configuration, et authentifient les communications avec Azure AD. Grâce à cette application, vous n'avez pas besoin d'entrer ces mêmes informations chaque fois que vous configurez un nouveau composant ou service Configuration Manager avec Azure.

## Services disponibles

Configurez les services Azure suivants à l'aide de cet Assistant :

- **Gestion cloud** : Ce service permet aux clients et au site de s'authentifier à l'aide d'Azure AD. Cette authentification permet d'autres scénarios, par exemple :
  - Installer et attribuer des clients Configuration Manager exécutant Windows 10 avec Azure AD pour l'authentification
  - Configurer la découverte d'utilisateurs Azure AD
  - Prendre en charge certains scénarios de passerelle de gestion cloud
- **Connecteur OMS** : Connectez-vous à Operations Management Suite (OMS). Synchronisez des données telles que des regroupements avec OMS Log Analytics.
- **Connecteur Upgrade Readiness** : Connectez-vous à Upgrade Readiness dans Windows Analytics. Consultez les données de compatibilité de mise à niveau des clients.
- **Microsoft Store pour Entreprises** : Connectez-vous au Microsoft Store pour Entreprises. Obtenez des applications du Store pour votre organisation que vous pouvez déployer avec Configuration Manager.

**Détails sur le service**

Le tableau suivant répertorie des informations sur chacun des services.

- **Locataires** : nombre d'instances de service que vous pouvez configurer. Chaque instance doit être un locataire Azure distinct.
- **Clouds** : tous les services prennent en charge le cloud Azure global, mais les services ne prennent pas tous en charge les clouds privés, tels que le cloud Azure US Government.
- **Application web** : indique si le service utilise une application Azure AD de type *Application/API web*, également appelée application serveur dans Configuration Manager.
- **Application native** : indique si le service utilise une application Azure AD de type *Native*, également appelée application cliente dans Configuration Manager.
- **Actions** : indique si vous pouvez importer ou créer ces applications dans l'Assistant Services Azure Configuration Manager.

| SERVICE | LOCATAIRES | CLOUDS | APPLICATION WEB | APPLICATION NATIVE | ACTIONS |
|---|---|---|---|---|---|
| Gestion cloud avec découverte d'utilisateurs Azure AD | Plusieurs | Public | ✓ | ✓ | Importer, Créer |
| Connecteur OMS | Un | Public, privé | ✓ | ✗ | Importation |
| Upgrade Readiness | Un | Public | ✓ | ✗ | Importation |
| Microsoft Store pour Entreprises et Éducation | Un | Public | ✓ | ✗ | Importer, Créer |

**À propos des applications Azure AD**

Des services Azure différents nécessitent des configurations distinctes, que vous définissez dans le portail Azure. En outre, les applications pour chaque service peuvent nécessiter des autorisations distinctes sur des ressources Azure.

Vous pouvez utiliser une seule application pour plusieurs services. Il n'existe qu'un seul objet à gérer dans Configuration Manager et Azure AD. Quand la clé de sécurité de l'application expire, il vous suffit d'actualiser une clé.

La configuration la plus sécurisée consiste à utiliser des applications distinctes pour chaque service. Une application pour un service peut nécessiter des autorisations supplémentaires qui s'avèrent inutiles pour un autre service. L'utilisation d'une application pour différents services peut fournir à l'application plus d'autorisations que nécessaire.

Quand vous créez des services Azure supplémentaires dans l'Assistant, Configuration Manager est conçu pour réutiliser les informations qui sont communes aux services. Ce comportement vous évite d'avoir à entrer les mêmes informations plusieurs fois.

Pour plus d'informations sur les autorisations d'application nécessaires et les configurations pour chaque service, consultez l'article Configuration Manager approprié dans Services disponibles.

Pour plus d'informations sur les applications Azure, commencez par les articles suivants :

- Authentification et autorisation dans Azure App Service
- Vue d'ensemble des applications web
- Concepts de base de l'inscription d'une application dans Azure AD
- Inscrire une application auprès de votre locataire Azure Active Directory

## Avant de commencer

Après avoir choisi le service auquel vous souhaitez vous connecter, reportez-vous au tableau dans Détails sur le service. Ce tableau fournit les informations nécessaires pour terminer l'Assistant Services Azure. Ayez préalablement une discussion avec votre administrateur Azure AD. Décidez si vous créez manuellement les applications à l'avance dans le portail Azure pour en importer ensuite les détails dans Configuration Manager. Vous pouvez aussi utiliser Configuration Manager pour créer directement les applications dans Azure AD. Pour collecter les données nécessaires à partir d'Azure AD, passez en revue les informations contenues dans les autres sections de cet article.

Certains services nécessitent que les applications Azure AD disposent d'autorisations spécifiques. Passez en revue les informations pour chaque service afin de déterminer les autorisations requises. Par exemple, avant de pouvoir importer une application web, un administrateur Azure doit tout d'abord la créer dans le portail Azure. Lors de la configuration du connecteur Upgrade Readiness ou OMS, vous devez donner à votre application web tout juste inscrite une autorisation de *contributeur* sur le groupe de ressources qui contient l'espace de travail OMS approprié. Cette autorisation permet à Configuration Manager d'accéder à cet espace de travail. Recherchez le nom de l'inscription d'application dans le panneau **Ajouter des utilisateurs** au moment d'attribuer l'autorisation. Ce processus est le même que lors de la fourniture à Configuration Manager d'autorisations sur OMS. Un administrateur Azure doit attribuer ces autorisations avant que vous n'importiez l'application dans Configuration Manager.

## Démarrer l'Assistant Services Azure

1. Dans la console Configuration Manager, accédez à l'espace de travail **Administration**, développez **Services cloud**, puis sélectionnez le nœud **Services Azure**.
2. Sous l'onglet **Accueil** du ruban, dans le groupe **Services Azure**, cliquez sur **Configurer les services Azure**.
3. Dans la page **Services Azure** de l'Assistant Services Azure :
   a. Spécifiez un **Nom** pour l'objet dans Configuration Manager.
   b. Spécifiez une **Description** facultative pour vous aider à identifier le service.
   c. Sélectionnez le service Azure que vous souhaitez connecter à Configuration Manager.
4. Cliquez sur **Suivant** pour passer à la page Propriétés de l'application Azure de l'Assistant Services Azure.

## Propriétés de l'application Azure

Dans la page **Application** de l'Assistant Services Azure, sélectionnez d'abord **l'environnement Azure** dans la liste. Reportez-vous au tableau dans Détails sur le service pour connaître l'environnement actuellement disponible pour le service.

Le reste de la page Application varie selon le service spécifique. Reportez-vous au tableau dans Détails sur le service pour connaître le type d'application utilisé par le service et l'action que vous pouvez effectuer.

- Si l'application prend en charge les deux actions Importer et Créer, cliquez sur **Parcourir**. Cette action ouvre la boîte de dialogue Application serveur ou la boîte de dialogue Application cliente.
- Si l'application prend uniquement en charge l'action Importer, cliquez sur **Importer**. Cette action ouvre la boîte de dialogue Importer des applications (serveur) ou la boîte de dialogue Importer des applications (client).

Après avoir spécifié les applications dans cette page, cliquez sur **Suivant** pour passer à la page Configuration ou Découverte de l'Assistant Services Azure.

### Application web

Il s'agit d'une application Azure AD de type *Application/API web*, également appelée application serveur dans Configuration Manager.

#### Boîte de dialogue Application serveur

Quand vous cliquez sur **Parcourir** pour **Application web** dans la page Application de l'Assistant Services Azure, il ouvre la boîte de dialogue Application serveur. Il affiche une liste qui indique les propriétés suivantes de toutes les applications web existantes :

- Nom convivial du locataire
- Nom convivial de l'application

- Type de service

Il existe trois actions possibles à partir de la boîte de dialogue Application serveur :

- Pour réutiliser une application web existante, sélectionnez-la dans la liste.
- Cliquez sur **Importer** pour ouvrir la boîte de dialogue Importer des applications.
- Cliquez sur **Créer** pour ouvrir la boîte de dialogue Créer une application serveur.

Après avoir sélectionné, importé ou créé une application web, cliquez sur **OK** pour fermer la boîte de dialogue Application serveur. Cette action renvoie à la page Application de l'Assistant Services Azure.

#### Boîte de dialogue Importer des applications (serveur)

Quand vous cliquez sur **Importer** dans la boîte de dialogue Application serveur ou la page Application de l'Assistant Services Azure, il ouvre la boîte de dialogue Importer des applications. Cette page vous permet d'entrer des informations sur une application web Azure AD qui est déjà créée dans le portail Azure. Les métadonnées relatives à cette application web sont importées dans Configuration Manager. Spécifiez les informations suivantes :

- **Nom du locataire Azure AD**
- **ID de locataire Azure AD**
- **Nom de l'application** : nom convivial pour l'application.
- **ID de client**
- **Clé secrète**
- **Expiration de la clé secrète** : sélectionnez une date ultérieure dans le calendrier.
- **URI ID d'application** : cette valeur doit être unique dans votre locataire Azure AD. Elle se trouve dans le jeton d'accès utilisé par le client Configuration Manager pour demander l'accès au service. Par défaut, cette valeur est https://ConfigMgrService.

Après avoir entré les informations, cliquez sur **Vérifier**. Cliquez ensuite sur **OK** pour fermer la boîte de dialogue Importer des applications. Cette action renvoie à la page Application de l'Assistant Services Azure ou à la boîte de dialogue Application serveur.

#### Boîte de dialogue Créer une application serveur

Quand vous cliquez sur **Créer** dans la boîte de dialogue Application serveur, la boîte de dialogue Créer une application serveur s'ouvre. Cette page permet d'automatiser la création d'une application web dans Azure AD. Spécifiez les informations suivantes :

- **Nom de l'application** : nom convivial pour l'application.
- **URL de la page d'accueil** : cette valeur n'est pas utilisée par Configuration Manager, mais est requise par Azure AD. Par défaut, cette valeur est https://ConfigMgrService.
- **URI ID d'application** : cette valeur doit être unique dans votre locataire Azure AD. Elle se trouve dans le jeton d'accès utilisé par le client Configuration Manager pour demander l'accès au service. Par défaut, cette valeur est https://ConfigMgrService.
- **Période de validité de la clé secrète** : cliquez sur la liste déroulante et sélectionnez **1 an** ou **2 ans**. Un an est la valeur par défaut.

Cliquez sur **Se connecter** pour vous authentifier auprès d'Azure en tant qu'utilisateur administratif. Ces informations d'identification ne sont pas enregistrées par Configuration Manager. Ce rôle ne nécessite pas d'autorisations dans Configuration Manager et ne doit pas obligatoirement être le même compte que celui qui exécute l'Assistant Services Azure. Après vous être authentifié correctement auprès d'Azure, la page affiche le **Nom du locataire Azure AD** pour référence.

Cliquez sur **OK** pour créer l'application web dans Azure AD et fermer la boîte de dialogue Créer une application serveur. Cette action renvoie à la boîte de dialogue Application serveur.

### Application cliente native

Il s'agit d'une application Azure AD de type *Native*, également appelée application cliente dans Configuration Manager.

#### Boîte de dialogue Application cliente

Quand vous cliquez sur **Parcourir** pour **Application cliente native** dans la page Application de l'Assistant Services Azure, il ouvre la boîte de dialogue Application cliente. Il affiche une liste qui indique les propriétés suivantes de toutes les applications natives existantes :

- Nom convivial du locataire
- Nom convivial de l'application
- Type de service

Il existe trois actions possibles à partir de la boîte de dialogue Application cliente :

- Pour réutiliser une application native existante, sélectionnez-la dans la liste.
- Cliquez sur **Importer** pour ouvrir la boîte de dialogue Importer des applications.
- Cliquez sur **Créer** pour ouvrir la boîte de dialogue Créer une application cliente.

Après avoir sélectionné, importé ou créé une application native, cliquez sur **OK** pour fermer la boîte de dialogue Application cliente. Cette action renvoie à la page Application de l'Assistant Services Azure.

#### Boîte de dialogue Importer des applications (client)

Quand vous cliquez sur **Importer** dans la boîte de dialogue Application cliente, la boîte de dialogue Importer des applications s'ouvre. Cette page vous permet d'entrer des informations sur une application native Azure AD qui est déjà créée dans le portail Azure. Les métadonnées relatives à cette application native sont importées dans Configuration Manager. Spécifiez les informations suivantes :

- **Nom de l'application** : nom convivial pour l'application.
- **ID de client**

Après avoir entré les informations, cliquez sur **Vérifier**. Cliquez ensuite sur **OK** pour fermer la boîte de dialogue Importer des applications. Cette action renvoie à la boîte de dialogue Application cliente.

#### Boîte de dialogue Créer une application cliente

Quand vous cliquez sur **Créer** dans la boîte de dialogue Application cliente, la boîte de dialogue Créer une application cliente s'ouvre. Cette page permet d'automatiser la création d'une application native dans Azure AD. Spécifiez les informations suivantes :

- **Nom de l'application** : nom convivial pour l'application.
- **URL de réponse** : cette valeur n'est pas utilisée par Configuration Manager, mais est requise par Azure AD. Par défaut, cette valeur est https://ConfigMgrService.

Cliquez sur **Se connecter** pour vous authentifier auprès d'Azure en tant qu'utilisateur administratif. Ces informations d'identification ne sont pas enregistrées par Configuration Manager. Ce rôle ne nécessite pas d'autorisations dans Configuration Manager et ne doit pas obligatoirement être le même compte que celui qui exécute l'Assistant Services Azure. Après vous être authentifié correctement auprès d'Azure, la page affiche le **Nom du locataire Azure AD** pour référence.

Cliquez sur **OK** pour créer l'application native dans Azure AD et fermer la boîte de dialogue Créer une application cliente. Cette action renvoie à la boîte de dialogue Application cliente.

## Configuration ou Découverte

Après avoir spécifié les applications natives et web dans la page des applications, l'Assistant Services Azure passe à une page **Configuration** ou **Découverte**, selon le service auquel vous vous connectez. Les détails de cette page varient d'un service à l'autre. Pour plus d'informations, consultez l'un des articles suivants :

- Service de **gestion cloud**, page **Découverte** : Configurer la découverte d'utilisateurs Azure AD
- Service du **connecteur OMS**, page **Configuration** : Configurer la connexion à OMS
- Service du **connecteur Upgrade Readiness**, page **Configuration** : Utiliser l'Assistant Azure pour créer la connexion
- Service du **Microsoft Store pour Entreprises**, page **Configuration** : Configurer la synchronisation du Microsoft Store pour Entreprises

Pour finir, terminez l'Assistant Services Azure via les pages de résumé, de progression et de fin. Vous avez terminé la configuration d'un service Azure dans Configuration Manager. Répétez ce processus pour configurer d'autres services Azure.

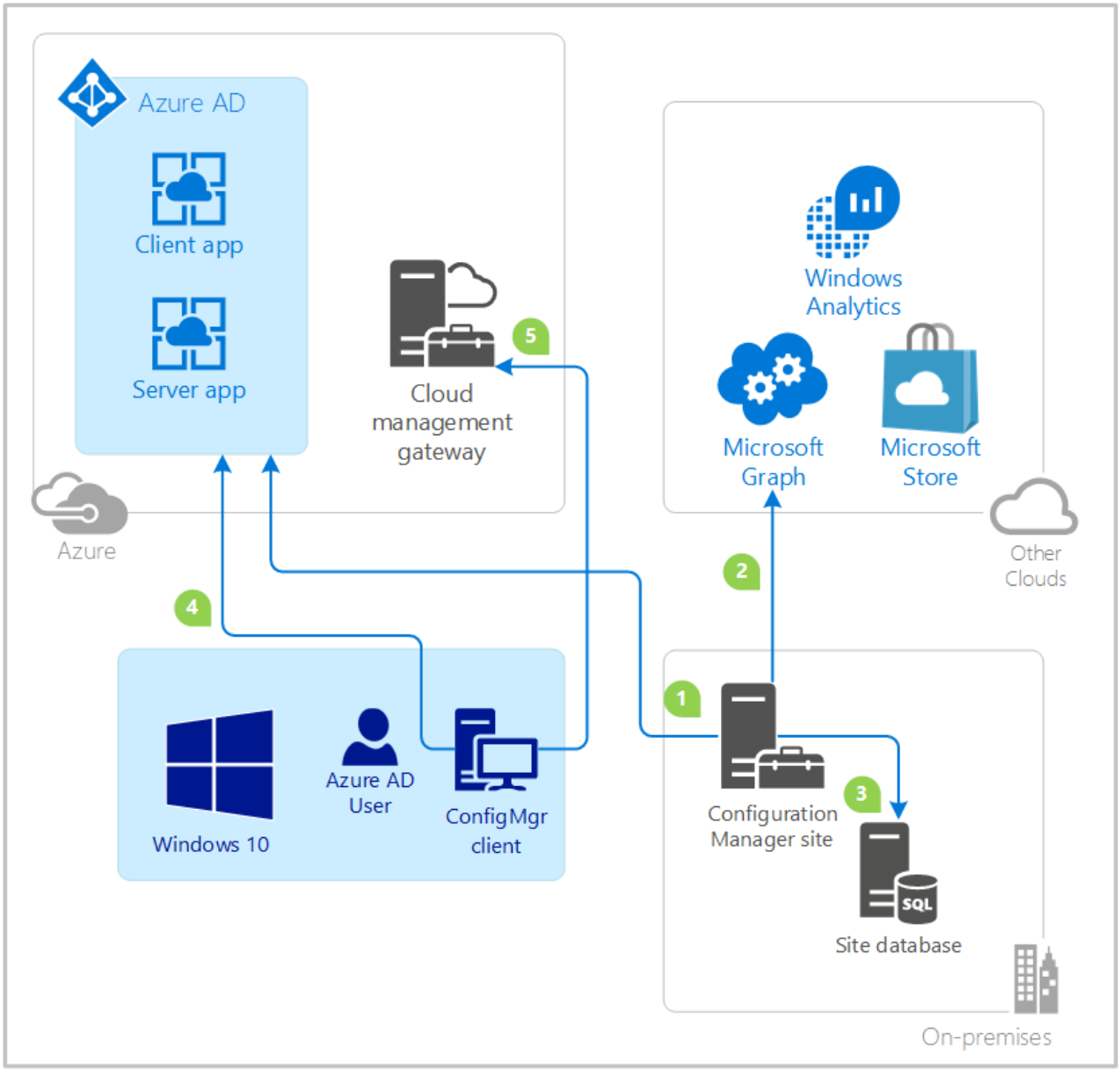
## Afficher la configuration d'un service Azure

Vous pouvez afficher les propriétés d'un service Azure que vous avez configuré en vue de son utilisation. Dans la console Configuration Manager, accédez à l'espace de travail **Administration**, développez **Services cloud**, puis sélectionnez **Services Azure**. Sélectionnez le service que vous souhaitez afficher ou modifier, puis cliquez sur **Propriétés**.

Si vous sélectionnez un service, puis cliquez sur **Supprimer** dans le ruban, cette action supprime la connexion dans Configuration Manager. Elle ne supprime pas l'application dans Azure AD. Demandez à votre administrateur Azure de supprimer l'application quand elle est devenue inutile. Vous pouvez aussi exécuter l'Assistant Services Azure pour importer l'application.

## Flux de données de gestion cloud

Le diagramme suivant est un flux de données conceptuel pour l'interaction entre Configuration Manager, Azure AD et des services cloud connectés. Cet exemple utilise le service de **gestion cloud**, qui inclut un client Windows 10 ainsi que des applications serveur et clientes. Les flux sont similaires pour d'autres services.




1. L'administrateur Configuration Manager importe ou crée les applications serveur et clientes dans Azure AD.
2. La méthode de découverte d'utilisateurs Azure AD de Configuration Manager s'exécute. Le site utilise le jeton d'application serveur Azure AD pour rechercher des objets utilisateur dans Microsoft Graph.
3. Le site stocke des données sur les objets utilisateur. Pour plus d'informations, consultez Découverte d'utilisateurs Azure AD.
4. Le client Configuration Manager demande le jeton d'utilisateur Azure AD. Le client génère la revendication à l'aide de l'ID de l'application cliente Azure AD et de l'application serveur comme audience. Pour plus d'informations, consultez Revendications des jetons de sécurité Azure AD.
5. Le client s'authentifie auprès du site en présentant le jeton Azure AD à la passerelle de gestion cloud et/ou au point de gestion HTTPS local.

# Comptes utilisés dans System Center Configuration Manager

22/06/2018 • 47 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez les informations suivantes pour identifier les groupes Windows et les comptes utilisés dans System Center Configuration Manager, savoir comment ils sont utilisés et connaître les exigences associées.

## Groupes Windows créés et utilisés par Configuration Manager

Configuration Manager crée automatiquement et, très souvent, gère automatiquement les groupes Windows suivants :

> **NOTE**
> Lorsque que Configuration Manager crée un groupe sur un ordinateur qui est membre d'un domaine, ce groupe est un groupe de sécurité local. Si l'ordinateur est un contrôleur de domaine, ce groupe est un groupe de domaine local qui est partagé entre tous les contrôleurs de domaine du domaine.

**ConfigMgr_CollectedFilesAccess**

Configuration Manager utilise ce groupe pour autoriser la consultation des fichiers collectés par l'inventaire logiciel.

Le tableau suivant répertorie des détails supplémentaires pour ce groupe :

| DÉTAIL | PLUS D'INFORMATIONS |
|---|---|
| Type et emplacement | Ce groupe est un groupe de sécurité local créé sur le serveur de site principal.<br><br>Lorsque vous désinstallez un site, ce groupe n'est pas supprimé automatiquement. Il doit être supprimé manuellement. |
| Adhésion | Configuration Manager gère automatiquement l'appartenance au groupe. Les membres incluent les utilisateurs administratifs qui disposent de l'autorisation **Afficher les fichiers collectés** pour l'objet sécurisable **Regroupement** depuis un rôle de sécurité attribué. |
| Autorisations | Par défaut, ce groupe dispose de l'autorisation **Read** pour le dossier suivant sur le serveur de site : **%path%\Microsoft Configuration Manager\sinv.box\FileCol**. |

**ConfigMgr_DViewAccess**

Ce groupe est un groupe de sécurité local créé par Configuration Manager sur le serveur de base de données du site ou le serveur réplica de base de données. Il n'est pas utilisé actuellement, mais est réservé à un usage ultérieur.

**Utilisateurs du contrôle à distance ConfigMgr**

Les outils de contrôle à distance de Configuration Manager utilisent ce groupe pour stocker les comptes et les groupes que vous configurez dans la liste Observateurs autorisés qui est attribuée à chaque client.

Le tableau suivant répertorie des détails supplémentaires pour ce groupe :

| DÉTAIL | PLUS D'INFORMATIONS |
|---|---|
| Type et emplacement | Ce groupe est un groupe de sécurité local créé sur le client Configuration Manager, lorsque le client reçoit une stratégie qui active les outils de contrôle à distance.<br><br>Lorsque vous désactivez les outils de contrôle à distance pour un client, ce groupe n'est pas supprimé automatiquement. Il doit être supprimé manuellement sur chaque ordinateur client. |
| Adhésion | Par défaut, ce groupe ne contient aucun membre. Lorsque vous ajoutez des utilisateurs à la liste Observateurs autorisés, ils sont automatiquement ajoutés à ce groupe.<br><br>Vous pouvez utiliser la liste Observateurs autorisés pour gérer l'appartenance à ce groupe au lieu d'y ajouter directement des utilisateurs ou des groupes.<br><br>En plus d'être un observateur autorisé, un utilisateur administratif doit disposer de l'autorisation **Contrôle à distance** sur l'objet **Regroupement**. Vous pouvez attribuer cette autorisation à l'aide du rôle de sécurité Opérateur d'outils à distance. |
| Autorisations | Par défaut, ce groupe ne possède pas d'autorisations sur les emplacements de l'ordinateur. Il ne sert qu'à contenir la liste Observateurs autorisés. |

### Administrateurs SMS

Configuration Manager utilise ce groupe pour autoriser l'accès au fournisseur SMS, via Windows Management Instrumentation (WMI). L'accès au fournisseur SMS est requis pour afficher et modifier des objets dans la console Configuration Manager.

> **NOTE**
> La configuration de l'administration basée sur les rôles d'un utilisateur administratif détermine quels objets celui-ci peut consulter et gérer, lorsqu'il utilise la console Configuration Manager.

Le tableau suivant répertorie des détails supplémentaires pour ce groupe :

| DÉTAIL | PLUS D'INFORMATIONS |
|---|---|
| Type et emplacement | Ce groupe est un groupe de sécurité local créé sur chaque ordinateur qui dispose d'un fournisseur SMS.<br><br>Lorsque vous désinstallez un site, ce groupe n'est pas supprimé automatiquement. Il doit être supprimé manuellement. |

| DÉTAIL | PLUS D'INFORMATIONS |
| --- | --- |
| Adhésion | Configuration Manager gère automatiquement l'appartenance au groupe. Par défaut, chaque utilisateur administratif d'une hiérarchie et le compte d'ordinateur du serveur de site sont membres du groupe Administrateurs SMS sur chaque ordinateur du fournisseur SMS d'un site. |
| Autorisations | La définition des autorisations et des droits des administrateurs SMS s'effectue dans le composant logiciel enfichable MMC Contrôle WMI. Par défaut, les autorisations **Enable Account** et **Remote Enable** sont accordées au groupe Administrateurs SMS sur l'espace de noms Root\SMS. Les utilisateurs authentifiés disposent des autorisations **Méthodes d'exécution**, **Écriture fournisseur** et **Activer le compte**.<br><br>Les administrateurs qui utiliseront une console Configuration Manager distante doivent posséder des autorisations DCOM d'activation à distance à la fois sur le serveur de site et sur l'ordinateur du fournisseur SMS. Il est recommandé d'accorder ces droits aux Administrateurs SMS pour simplifier l'administration plutôt que d'accorder ces droits directement aux utilisateurs ou groupes. Pour plus d'informations, consultez la section Configurer les autorisations DCOM pour les consoles Configuration Manager distantes dans l'article Modifier votre infrastructure System Center Configuration Manager. |

**SMS_SiteSystemToSiteServerConnection_MP_<code_site>**

Les points de gestion Configuration Manager qui sont distants du serveur de site utilisent ce groupe pour se connecter à la base de données du site. Ce groupe fournit un accès au point de gestion pour les dossiers Boîte de réception sur le serveur de site et la base de données du site.

Le tableau suivant répertorie des détails supplémentaires pour ce groupe :

| DÉTAIL | PLUS D'INFORMATIONS |
| --- | --- |
| Type et emplacement | Ce groupe est un groupe de sécurité local créé sur chaque ordinateur qui dispose d'un fournisseur SMS.<br><br>Lorsque vous désinstallez un site, ce groupe n'est pas supprimé automatiquement. Il doit être supprimé manuellement. |
| Adhésion | Configuration Manager gère automatiquement l'appartenance au groupe. Par défaut, l'appartenance inclut les comptes d'ordinateur des ordinateurs distants qui disposent d'un point de gestion pour le site. |
| Autorisations | Par défaut, ce groupe dispose des autorisations **Lecture**, **Lecture et exécution** et **Affichage du contenu du dossier** pour le dossier **%path%\Microsoft Configuration Manager\inboxes** sur le serveur de site. Ce groupe dispose de l'autorisation supplémentaire **Écriture** sur les sous-dossiers de **inboxes** dans lesquels le point de gestion écrit les données client. |

**SMS_SiteSystemToSiteServerConnection_SMSProv_<code_site>**

Les ordinateurs fournisseurs SMS Configuration Manager qui sont distants du serveur de site utilisent ce groupe pour se connecter à celui-ci.

Le tableau suivant répertorie des détails supplémentaires pour ce groupe :

| DÉTAIL | PLUS D'INFORMATIONS |
|---|---|
| Type et emplacement | Ce groupe est un groupe de sécurité local créé sur le serveur de site.<br><br>Lorsque vous désinstallez un site, ce groupe n'est pas supprimé automatiquement. Il doit être supprimé manuellement. |
| Adhésion | Configuration Manager gère automatiquement l'appartenance au groupe. Par défaut, l'appartenance comprend le compte d'ordinateur ou le compte d'utilisateur de domaine utilisé pour se connecter au serveur de site depuis chaque ordinateur distant ayant installé un fournisseur SMS pour le site. |
| Autorisations | Par défaut, ce groupe dispose des autorisations **Lecture**, **Lecture et exécution** et **Affichage du contenu du dossier** pour le dossier **%path%\Microsoft Configuration Manager\inboxes** sur le serveur de site. Ce groupe dispose de l'autorisation supplémentaire **Écriture** ou des autorisations **Écriture** et **Modifier** sur les sous-dossiers de **inboxes** auxquels le fournisseur SMS doit avoir accès.<br><br>Ce groupe dispose des autorisations **Lecture**, **Lecture et exécution**, **Affichage du contenu du dossier**, **Écriture** et **Modification** pour les dossiers situés sous **%path%\Microsoft Configuration Manager\OSD\boot** et **Lecture** pour les dossiers situés sous **%path%\Microsoft Configuration Manager\OSD\Bin** sur le serveur de site. |

**SMS_SiteSystemToSiteServerConnection_Stat_<code_site>**

Le Gestionnaire de répartition de fichiers sur les ordinateurs de système de site distants Configuration Manager utilise ce groupe pour se connecter au serveur de site.

Le tableau suivant répertorie des détails supplémentaires pour ce groupe :

| DÉTAIL | PLUS D'INFORMATIONS |
|---|---|
| Type et emplacement | Ce groupe est un groupe de sécurité local créé sur le serveur de site.<br><br>Lorsque vous désinstallez un site, ce groupe n'est pas supprimé automatiquement. Il doit être supprimé manuellement. |
| Adhésion | Configuration Manager gère automatiquement l'appartenance au groupe. Par défaut, l'appartenance comprend le compte d'ordinateur ou le compte d'utilisateur de domaine utilisé pour se connecter au serveur de site depuis chaque ordinateur de système de site distant qui exécute le Gestionnaire de répartition de fichiers. |

| DÉTAIL | PLUS D'INFORMATIONS |
| --- | --- |
| Autorisations | Par défaut, ce groupe dispose des autorisations **Lecture**, **Écriture et exécution** et **Affichage du contenu du dossier** sur le dossier **%path%\Microsoft Configuration Manager\inboxes** et ses sous-dossiers sur le serveur de site. Ce groupe dispose des autorisations supplémentaires **Écriture** et **Modifier** sur le dossier **%path%\Microsoft Configuration Manager\inboxes\statmgr.box** sur ce serveur de site. |

**SMS_SiteToSiteConnection_<code_site>**

Configuration Manager utilise ce groupe pour activer la réplication de fichiers entre les sites d'une hiérarchie. Pour chaque site distant qui transfère directement des fichiers vers ce site, ce groupe contient les comptes configurés en tant que **compte de réplication de fichiers**.

Le tableau suivant répertorie des détails supplémentaires pour ce groupe :

| DÉTAIL | PLUS D'INFORMATIONS |
| --- | --- |
| Type et emplacement | Ce groupe est un groupe de sécurité local créé sur le serveur de site. |
| Adhésion | Lorsque vous installez un nouveau site en tant qu'enfant d'un autre site, Configuration Manager ajoute automatiquement le compte de l'ordinateur du nouveau site au groupe situé sur le serveur de site parent. Configuration Manager ajoute également le compte d'ordinateur du site parent au groupe sur le serveur de site. Si vous spécifiez un autre compte pour les transferts de fichiers, ajoutez ce compte à ce groupe sur le serveur de site de destination.<br><br>Lorsque vous désinstallez un site, ce groupe n'est pas supprimé automatiquement. Il doit être supprimé manuellement. |
| Autorisations | Par défaut, ce groupe dispose du **contrôle intégral** pour le dossier **%path%\Microsoft Configuration Manager\inboxes\despoolr.box\receive** . |

# Comptes utilisés par Configuration Manager

Vous pouvez utiliser les comptes suivants pour Configuration Manager.

**Compte de découverte de groupes Active Directory**

Le **compte de découverte de groupes Active Directory** permet de détecter les groupes de sécurité locaux, globaux et universels, les membres de ces groupes et les membres des groupes de distribution à partir des emplacements spécifiés dans Active Directory Domain Services. Les groupes de distribution ne sont pas découverts en tant que ressources de groupe.

Ce compte peut être un compte d'ordinateur du serveur de site qui exécute la découverte ou un compte d'utilisateur Windows. Celui-ci doit disposer de l'autorisation d'accès **Lecture** aux emplacements Active Directory spécifiés pour cette découverte.

**Compte de découverte de systèmes Active Directory**

Le **compte de découverte de systèmes Active Directory** est utilisé pour détecter des ordinateurs partir des emplacements spécifiés dans les services de domaine Active Directory.

Ce compte peut être un compte d'ordinateur du serveur de site qui exécute la découverte ou un compte d'utilisateur Windows. Celui-ci doit disposer de l'autorisation d'accès **Lecture** aux emplacements Active Directory spécifiés pour cette découverte.

#### Compte de découverte d'utilisateurs Active Directory

Le **compte de découverte d'utilisateurs Active Directory** est utilisé pour détecter des comptes d'utilisateur partir des emplacements spécifiés dans les services de domaine Active Directory.

Ce compte peut être un compte d'ordinateur du serveur de site qui exécute la découverte ou un compte d'utilisateur Windows. Celui-ci doit disposer de l'autorisation d'accès **Lecture** aux emplacements Active Directory spécifiés pour cette découverte.

#### Compte de forêt Active Directory

Le **compte de forêt Active Directory** est utilisé pour découvrir l'infrastructure de réseau à partir de forêts Active Directory. Les sites d'administration centrale et les sites principaux l'utilisent également pour publier des données dans les services AD DS d'une forêt.

> **NOTE**
> Les sites secondaires utilisent toujours le compte d'ordinateur du serveur de site secondaire pour publier dans Active Directory.

> **NOTE**
> Le Compte de forêt Active Directory doit être un compte global utilisé pour détecter des forêts non approuvées et publier des données dans celles-ci. Si vous n'utilisez pas le compte d'ordinateur du serveur de site, vous ne pouvez sélectionner qu'un compte global.

Ce compte doit disposer des autorisations de **Lecture** pour chaque forêt Active Directory dont vous souhaitez découvrir l'infrastructure réseau.

Ce compte doit disposer des autorisations **Contrôle intégral** pour le conteneur Gestion du système et tous ses objets enfants dans chaque forêt Active Directory où vous souhaitez publier les données de site.

#### Compte du serveur proxy du point de synchronisation Asset Intelligence

Le point de synchronisation Asset Intelligence utilise le **compte du serveur proxy du point de synchronisation Asset Intelligence** pour accéder à Internet via un serveur proxy ou un pare-feu qui exige un accès authentifié.

> **IMPORTANT**
> Spécifiez un compte qui dispose des autorisations minimales pour le serveur proxy requis ou le pare-feu.

#### Compte de point d'enregistrement de certificat

Le **compte du point d'enregistrement du certificat** connecte le point d'enregistrement du certificat à la base de données Configuration Manager. Le compte d'ordinateur du serveur du point d'enregistrement de certificat est utilisé par défaut, mais vous pouvez configurer un compte d'utilisateur à la place. Chaque fois que le point d'enregistrement de certificat est dans un domaine non approuvé du serveur de site, vous devez spécifier un compte d'utilisateur. Ce compte ne requiert qu'un accès en **Lecture** sur la base de données du site, car le système de messages d'état gère les tâches d'écriture.

#### Compte Capturer l'image du système d'exploitation

Configuration Manager utilise le **compte Capturer l'image du système d'exploitation** pour accéder au

dossier qui stocke les images capturées lorsque vous déployez des systèmes d'exploitation. Ce compte est requis si vous ajoutez l'étape **Capturer l'image du système d'exploitation** à la séquence de tâches.

Le compte doit disposer d'autorisations en **Lecture** et en **Écriture** sur le partage réseau sur lequel l'image capturée est stockée.

Si le mot de passe du compte est modifié dans Windows, vous devez mettre à jour la séquence de tâches avec le nouveau mot de passe. Le client Configuration Manager reçoit le nouveau mot de passe quand il télécharge la stratégie du client.

Si vous utilisez ce compte, vous pouvez créer un compte d'utilisateur de domaine avec des autorisations minimales pour accéder aux ressources réseau nécessaires et l'utiliser pour tous les comptes de séquence de tâches.

> **IMPORTANT**
> N'attribuez pas d'autorisations d'ouverture de session interactive à ce compte.
>
> N'utilisez pas le compte d'accès réseau pour ce compte.

**Compte d'installation poussée du client**

Le **compte d'installation push du client** est utilisé pour se connecter à des ordinateurs et installer le logiciel client Configuration Manager si vous déployez des clients via l'installation push du client. Si ce compte n'est pas spécifié, c'est le compte du serveur de site qui est utilisé pour installer le logiciel client.

Ce compte doit être membre du groupe **Administrateurs** local sur les ordinateurs où le logiciel client Configuration Manager doit être installé. Il ne nécessite pas de droits **Administrateur de domaine**.

Vous pouvez spécifier un ou plusieurs comptes d'installation Push du client, que Configuration Manager teste successivement jusqu'à ce que l'un d'eux fonctionne.

> **TIP**
> Pour améliorer la coordination des mises à jour de comptes dans des déploiements Active Directory étendus, créez un compte avec un autre nom, puis ajoutez le nouveau compte à la liste des comptes d'installation Push du client dans Configuration Manager. Laissez suffisamment de temps aux services de domaine Active Directory pour répliquer le nouveau compte, puis supprimez l'ancien compte de Configuration Manager et des services de domaine Active Directory.

> **IMPORTANT**
> N'accordez pas à ce compte le droit d'ouvrir une session locale.

**Compte de connexion du point d'inscription**

Le **compte de connexion du point d'inscription** permet de connecter le point d'inscription à la base de données Configuration Manager. Le compte d'ordinateur du point d'inscription est utilisé par défaut, mais vous pouvez configurer un compte d'utilisateur à la place. Chaque fois que le point d'inscription est dans un domaine non approuvé à partir du serveur de site, vous devez spécifier un compte d'utilisateur. Ce compte requiert un accès en **Lecture** et en **Écriture** à la base de données du site.

**Compte de connexion Exchange Server**

Le **compte de connexion du serveur Exchange Server** connecte le serveur de site à l'ordinateur Exchange Server spécifié pour rechercher et gérer des appareils mobiles qui se connectent à Exchange Server. Ce compte nécessite des applets de commande PowerShell Exchange qui fournissent les autorisations requises pour l'ordinateur Exchange Server. Pour plus d'informations sur cette solution, consultez Gérer des appareils mobiles à

l'aide de System Center Configuration Manager et d'Exchange.

### Compte du serveur proxy du connecteur Exchange Server

Le connecteur Exchange Server utilise le **compte du serveur proxy du connecteur Exchange Server** pour accéder à Internet via un serveur proxy ou un pare-feu qui exige un accès authentifié.

> **IMPORTANT**
> Spécifiez un compte qui dispose des autorisations minimales pour le serveur proxy requis ou le pare-feu.

### Compte de connexion du point de gestion

Le **compte de connexion du point de gestion** permet de connecter le point de gestion à la base de données de site Configuration Manager pour permettre l'envoi et la récupération d'informations pour les clients. Le compte d'ordinateur du point de gestion est utilisé par défaut, mais vous pouvez configurer un compte d'utilisateur à la place. Chaque fois que le point de gestion est dans un domaine non approuvé à partir du serveur de site, vous devez spécifier un compte d'utilisateur.

Créez le compte comme un compte doté de droits limités, compte local sur l'ordinateur qui exécute Microsoft SQL Server.

> **IMPORTANT**
> N'accordez pas à ce compte des autorisations d'ouverture de session interactive.

### Compte de connexion multidiffusion

Les points de distribution configurés pour la multidiffusion utilisent le **compte de connexion multidiffusion** pour lire les informations de la base de données de site. Le compte d'ordinateur du point de distribution est utilisé par défaut, mais vous pouvez configurer un compte d'utilisateur à la place. Chaque fois que la base de données de site est dans une forêt non approuvée, vous devez spécifier un compte d'utilisateur. Par exemple, si votre centre de données dispose d'un réseau de périmètre dans une forêt autre que celle du serveur de site et de la base de données du site, vous pouvez utiliser ce compte pour lire les informations sur la multidiffusion à partir de la base de données du site.

Si vous créez ce compte, créez-le en tant que compte local doté de droits limités sur l'ordinateur qui exécute Microsoft SQL Server.

> **IMPORTANT**
> N'accordez pas à ce compte des autorisations d'ouverture de session interactive.

### Compte d'accès au réseau

Les ordinateurs clients utilisent le **compte d'accès au réseau** lorsqu'ils ne peuvent pas utiliser leur compte d'ordinateur local pour accéder au contenu sur les points de distribution. Par exemple, cela s'applique aux clients du groupe de travail et aux ordinateurs de domaines non approuvés. Ce compte peut également être utilisé pendant le déploiement du système d'exploitation, si l'ordinateur qui installe le système d'exploitation n'a pas encore un compte d'ordinateur sur le domaine.

> **NOTE**
> Le compte d'accès au réseau n'est jamais utilisé comme contexte de sécurité pour exécuter des applications et des programmes, installer des mises à jour logicielles ou exécuter des séquences de tâches. Il n'est utilisé que pour accéder aux ressources du réseau.

Accordez à ce compte les autorisations minimales appropriées sur le contenu dont le client a besoin pour accéder au logiciel. Le compte doit disposer du droit **Accéder à cet ordinateur à partir du réseau** sur le point de distribution ou d'un autre serveur sur lequel se trouve le contenu du package. Vous pouvez configurer jusqu'à 10 comptes d'accès réseau par site.

> **WARNING**
> Lorsque Configuration Manager tente d'utiliser le compte nomordinateur$ pour télécharger le contenu et qu'il n'y parvient pas, il essaie automatiquement de réutiliser le compte d'accès réseau, même s'il a préalablement fait une tentative qui a échoué.

Créez le compte dans n'importe quel domaine fournissant l'accès nécessaire aux ressources. Le compte d'accès réseau doit toujours inclure un nom de domaine. La sécurité directe n'est pas prise en charge pour ce compte. Si vous disposez de points de distribution dans plusieurs domaines, créez le compte dans un domaine approuvé.

> **TIP**
> Pour éviter les verrouillages de compte, ne modifiez pas le mot de passe d'un compte d'accès réseau existant. Au lieu de cela, créez un compte et configurez-le dans Configuration Manager. Après un délai suffisant pendant lequel tous les clients ont reçu les informations du nouveau compte, supprimez l'ancien compte des dossiers partagés du réseau et supprimez le compte.

> **IMPORTANT**
> N'accordez pas à ce compte des autorisations d'ouverture de session interactive.
>
> N'accordez pas à ce compte le droit de joindre les ordinateurs au domaine. Si vous devez joindre les ordinateurs au domaine au cours d'une séquence de tâches, utilisez le compte de jonction de domaine de l'Éditeur de séquence de tâches.

**Compte d'accès au package**

Un **compte d'accès au package** vous permet de définir des autorisations NTFS pour spécifier les utilisateurs et les groupes d'utilisateurs autorisés à accéder à un dossier de package sur des points de distribution. Par défaut, Configuration Manager n'accorde cet accès qu'aux comptes d'accès générique **Utilisateurs** et **Administrateurs**. Vous pouvez contrôler l'accès des ordinateurs clients à l'aide d'autres comptes ou groupes Windows. Les appareils mobiles n'utilisent pas les comptes d'accès au package, car ils récupèrent toujours le contenu du package de façon anonyme.

Par défaut, lorsque Configuration Manager crée le partage du package sur un point de distribution, il accorde un accès en **Lecture** au groupe **Utilisateurs** local et un **Contrôle intégral** au groupe **Administrateurs** local. Les autorisations requises dépendent du package. Si vous avez des clients dans des groupes de travail ou dans des forêts non approuvées, ceux-ci utiliseront le compte d'accès réseau pour accéder au contenu du package. Assurez-vous que le compte d'accès réseau bénéficie d'autorisations sur le package à l'aide des comptes d'accès au package définis.

Utilisez des comptes dans un domaine susceptible d'accéder aux points de distribution. Si vous créez ou modifiez le compte après la création du package, vous devez redistribuer ce dernier. La mise à jour du package ne modifie pas les autorisations NTFS sur le package.

Il est inutile d'ajouter le compte d'accès réseau comme un compte d'accès au package, car l'appartenance au groupe Utilisateurs l'ajoute automatiquement. Le fait de restreindre le compte d'accès au package au compte d'accès réseau uniquement n'empêche pas les clients d'accéder au package.

**Compte du point de Reporting Services**

SQL Server Reporting Services utilise le **compte du point de Reporting Services** pour récupérer les données

des rapports Configuration Manager à partir de la base de données de site. Le compte d'utilisateur Windows et le mot de passe que vous spécifiez sont chiffrés et stockés dans la base de données SQL Server Reporting Services.

> **NOTE**
> Le compte que vous spécifiez doit avoir des autorisations Connexion locale sur l'ordinateur hébergeant la base de données Reporting Services.

#### Comptes d'observateurs autorisés des outils de contrôle à distance

Les comptes que vous spécifiez en tant qu' **Observateurs autorisés** pour le contrôle à distance sont une liste d'utilisateurs autorisés à utiliser la fonctionnalité Outils de contrôle à distance sur les clients.

#### Compte d'installation du système de site

Le serveur de site utilise le **compte d'installation du système de site** pour installer, réinstaller, désinstaller et configurer des systèmes de site. Si vous configurez le système de site afin qu'il établisse des connexions à ce système de site, Configuration Manager utilise également ce compte pour extraire les données de l'ordinateur du système de site après l'installation du système de site et de tous les rôles de ce dernier. Chaque système de site peut avoir un autre compte d'installation du système de site, mais vous ne pouvez configurer qu'un compte d'installation du système de site pour gérer tous les rôles de système de site sur ce système de site.

Ce compte nécessite des autorisations d'administrateur locales sur les systèmes de site que les administrateurs installeront et configureront. De plus, ce compte doit disposer du droit **Accéder à cet ordinateur à partir du réseau** dans la stratégie de sécurité sur les systèmes de site que les administrateurs installeront et configureront.

> **TIP**
> Si vous avez plusieurs contrôleurs de domaine et si ces comptes sont utilisés dans plusieurs domaines, vérifiez qu'ils ont été répliqués avant de configurer le système de site.
>
> Lorsque vous spécifiez un compte local sur chaque système de site à gérer, cette configuration est plus sécurisée que l'utilisation de comptes de domaine, car elle limite les dommages que les personnes malveillantes peuvent provoquer en cas de compromission du compte. Toutefois, les comptes de domaine sont plus faciles à gérer. Examinez le compromis entre sécurité et efficacité d'administration.

#### Compte de connexion au serveur SMTP

Le serveur de site utilise le **compte de connexion au serveur SMTP** pour envoyer des alertes par courrier électronique quand le serveur SMTP requiert un accès authentifié.

> **IMPORTANT**
> Spécifiez un compte qui dispose des autorisations minimales pour envoyer des courriers électroniques.

#### Compte de connexion de point de mise à jour logicielle

Le serveur de site utilise le **compte de connexion de point de mise à jour logicielle** pour les deux services de mise à jour logicielle suivants :

- Windows Server Update Services (WSUS) Configuration Manager, qui configure des paramètres tels que les définitions de produit, les classifications et les paramètres en amont.
- WSUS Synchronization Manager, qui demande la synchronisation à un serveur WSUS en amont ou Microsoft Update.

Le compte d'installation du système de site peut installer les composants des mises à jour logicielles, mais il ne

peut pas exécuter des fonctions de mise à jour logicielle sur le point de mise à jour logicielle. Si vous ne pouvez pas utiliser le compte d'ordinateur du serveur de site pour cette fonctionnalité car le point de mise à jour logicielle se trouve dans une forêt non approuvée, vous devez spécifier ce compte en complément du compte d'installation du système de site.

Ce compte doit être un administrateur local sur l'ordinateur où WSUS est installé. Il doit également faire partie du groupe Administrateurs de WSUS local.

**Compte du serveur proxy du point de mise à jour logicielle**

Le point de mise à jour logicielle utilise le **compte du serveur proxy du point de mise à jour logicielle** pour accéder à Internet via un serveur proxy ou un pare-feu qui requiert un accès authentifié.

> **IMPORTANT**
> Spécifiez un compte qui dispose des autorisations minimales pour le serveur proxy requis ou le pare-feu.

**Compte du site source**

Le processus de migration utilise le **compte de site source** pour accéder au fournisseur SMS du site source. Ce compte nécessite des autorisations en **Lecture** vers les objets de site du site source pour collecter des données pour les tâches de migration.

Si vous mettez à niveau les points de distribution Configuration Manager 2007 ou les sites secondaires ayant des points de distribution au même emplacement vers des points de distribution System Center Configuration Manager, ce compte doit également disposer d'autorisations en **Suppression** sur la classe **Site** pour pouvoir supprimer le point de distribution du site Configuration Manager 2007 au cours de la mise à niveau.

> **NOTE**
> Le compte de site source et le compte de base de données du site source sont identifiés comme **Gestionnaire de migration** dans le nœud **Comptes** de l'espace de travail **Administration** dans la console Configuration Manager.

**Compte de base de données du site source**

Le processus de migration utilise le **compte de base de données du site source** pour accéder à la base de données SQL Server du site source. Pour collecter des données à partir de la base de données SQL Server du site source, le compte de base de données du site source doit disposer des autorisations **Lecture** et **Exécution** sur la base de données SQL Server du site source.

> **NOTE**
> Si vous utilisez le compte d'ordinateur System Center Configuration Manager, assurez-vous que toutes les conditions suivantes sont remplies pour ce compte :
>
> - Il est membre du groupe de sécurité **Utilisateurs du modèle COM distribué** dans le domaine où le site Configuration Manager 2007 réside.
> - Il est membre du groupe de sécurité **Administrateurs SMS** .
> - Il possède l'autorisation **Lecture** sur tous les objets de Configuration Manager 2007.

> **NOTE**
> Le compte du site source et le compte de base de données du site source sont identifiés comme **Gestionnaire de migration** dans le nœud **Comptes** de l'espace de travail **Administration** dans la console Configuration Manager.

**Compte de jonction de domaine de l'Éditeur de séquence de tâches**

Le **compte de jonction de domaine de l'Éditeur de séquence de tâches** est utilisé dans une séquence de tâches pour joindre un ordinateur nouvellement mis en image à un domaine. Il est nécessaire si vous ajoutez l'étape **Joindre le domaine ou le groupe de travail** à une séquence de tâches, puis sélectionnez l'option **Joindre un domaine**. Vous pouvez également configurer ce compte si vous ajoutez l'étape **Appliquer les paramètres réseau** à une séquence de tâches, mais cette opération n'est pas obligatoire.

Ce compte exige le droit **Jonction de domaine** dans le domaine que l'ordinateur doit joindre.

> **TIP**
> Si vous avez besoin de ce compte pour vos séquences de tâches, vous pouvez créer un compte d'utilisateur de domaine doté des autorisations d'accès minimales aux ressources réseau nécessaires, puis l'utiliser pour tous les comptes de séquence de tâches.

> **IMPORTANT**
> N'attribuez pas d'autorisations d'ouverture de session interactive à ce compte.
>
> N'utilisez pas le compte d'accès réseau pour ce compte.

**Compte de connexion à un dossier réseau de l'Éditeur de séquence de tâches**

Une séquence de tâches utilise le **compte de connexion à un dossier réseau de l'Éditeur de séquence de tâches** pour se connecter à un dossier partagé sur le réseau. Ce compte est obligatoire si vous ajoutez l'étape **Connexion à un dossier réseau** à une séquence de tâches.

Ce compte nécessite les autorisations permettant d'accéder au dossier partagé spécifié. Ce doit être un compte de domaine d'utilisateur.

> **TIP**
> Si vous avez besoin de ce compte pour vos séquences de tâches, vous pouvez créer un compte d'utilisateur de domaine doté des autorisations d'accès minimales aux ressources réseau nécessaires, puis l'utiliser pour tous les comptes de séquence de tâches.

> **IMPORTANT**
> N'attribuez pas d'autorisations d'ouverture de session interactive à ce compte.
>
> N'utilisez pas le compte d'accès réseau pour ce compte.

**Compte d'identification de la séquence de tâches**

Le **compte d'identification de la séquence de tâches** est utilisé pour exécuter des lignes de commande dans des séquences de tâches avec des informations d'identification différentes de celles du compte système local. Ce compte est requis si vous ajoutez l'étape **Exécuter la ligne de commande** à une séquence de tâches, sans que la séquence s'exécute avec les autorisations du compte système local sur l'ordinateur géré.

Configurez le compte pour qu'il dispose des autorisations minimales permettant d'exécuter la ligne de commande spécifiée dans la séquence de tâches. Ce compte requiert des autorisations d'ouverture de session interactive et, en général, la possibilité d'installer des logiciels et d'accéder aux ressources du réseau.

**IMPORTANT**

N'utilisez pas le compte d'accès réseau pour ce compte.

Ne configurez jamais le compte comme un administrateur de domaine.

Ne configurez jamais de profils itinérants pour ce compte. Quand la séquence de tâches s'exécute, elle télécharge le profil itinérant du compte. Le profil devient alors accessible sur l'ordinateur local.

Limitez la portée du compte. Par exemple, créez différents comptes d'identification de la séquence de tâches pour chaque séquence de tâches, de sorte que, si un compte est compromis, seuls les ordinateurs clients auxquels ce compte a accès sont compromis.

Si la ligne de commande nécessite un accès administratif sur l'ordinateur, créez un compte d'administrateur local réservé au compte d'identification de la séquence de tâches sur tous les ordinateurs qui exécutent cette dernière. Supprimez le compte dès que vous n'en avez plus besoin.

# Communications entre points de terminaison dans System Center Configuration Manager

22/06/2018 • 28 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

## Communications entre les systèmes d'un site

Quand des systèmes de site ou des composants Configuration Manager communiquent sur le réseau avec d'autres systèmes de site ou d'autres composants Configuration Manager du site, ils utilisent l'un des protocoles suivants, selon la configuration du site :

- SMB (Server Message Block)
- HTTP
- HTTPS

À l'exception de la communication depuis le serveur de site vers un point de distribution, ces communications de serveur à serveur dans un site peuvent avoir lieu à tout moment et n'utilisent aucun mécanisme de contrôle de la bande passante réseau. Comme vous ne pouvez pas contrôler la communication entre systèmes de site, vérifiez que vous installez des serveurs de système de site à des emplacements dotés de réseaux rapides et bien connectés.

Pour gérer plus facilement le transfert de contenu depuis le serveur de site vers des points de distribution :

- Configurez le point de distribution pour la planification et le contrôle de la bande passante réseau. Ces contrôles ressemblent aux configurations utilisées par les adresses intersites et vous pouvez souvent utiliser cette configuration au lieu d'installer un autre site Configuration Manager quand le transfert de contenu vers des emplacements réseau distants est votre préoccupation principale en ce qui concerne la bande passante.
- Vous pouvez installer un point de distribution comme un point de distribution préparé. Un point de distribution préparé vous permet d'utiliser du contenu qui est placé manuellement sur le serveur de point de distribution et supprime la nécessité de transférer des fichiers de contenu sur le réseau.

Pour plus d'informations, consultez Gérer la bande passante réseau pour la gestion de contenu.

## Communications depuis les clients vers les systèmes de site et les services

Les clients lancent des communications vers les rôles de système de site, les services de domaine Active Directory et les services en ligne. Pour activer ces communications, les pare-feu doivent autoriser le trafic réseau entre les clients et le point de terminaison de leurs communications. Les points de terminaison sont les suivants :

- **Point du site web du catalogue des applications** : Prend en charge les communications HTTP et HTTPS
- **Ressources cloud** : Inclut Microsoft Azure et Microsoft Intune
- **Module de stratégie de Configuration Manager (NDES)** : Prend en charge les communications HTTP et HTTPS

- **Points de distribution** : Prennent en charge les communications HTTP et HTTPS. HTTPS est obligatoire pour les points de distribution cloud
- **Point d'état de secours** : Prend en charge les communications HTTP
- **Point de gestion** : Prend en charge les communications HTTP et HTTPS
- **Microsoft Update**
- **Points de mise à jour logicielle** : Prennent en charge les communications HTTP et HTTPS
- **Points de migration d'état** : Prennent en charge les communications HTTP et HTTPS
- **Divers services de domaine**

Avant qu'un client puisse communiquer avec un rôle de système de site, le client utilise l'emplacement du service pour rechercher un rôle de système de site prenant en charge son protocole (HTTP ou HTTPS). Par défaut, les clients utilisent la méthode la plus sûre à leur disposition :

- Pour utiliser le protocole HTTPS, vous devez disposer d'une infrastructure à clé publique (PKI) et installer des certificats PKI sur des clients et serveurs. Pour plus d'informations sur la façon d'utiliser des certificats, consultez Configuration requise des certificats PKI pour System Center Configuration Manager.
- Quand vous déployez un rôle de système de site qui utilise Internet Information Services (IIS) et prend en charge les communications des clients, vous devez spécifier si les clients se connectent au système de site à l'aide de HTTP ou HTTPS. Si vous utilisez le protocole HTTP, vous devez également envisager les options de signature et de chiffrement. Pour plus d'informations, consultez Planification de la signature et du chiffrement dans Planifier la sécurité dans System Center Configuration Manager.

Pour plus d'informations sur l'emplacement de service par les clients, consultez Comprendre comment les clients recherchent des services et des ressources de site pour System Center Configuration Manager.

Pour plus d'informations sur les ports et protocoles utilisés par les clients pour communiquer avec ces points de terminaison, consultez Ports utilisés dans System Center Configuration Manager.

**Éléments à prendre en considération pour les communications de clients à partir d'Internet ou d'une forêt non approuvée**

Les rôles de système de site suivants installés sur les sites principaux prennent en charge les connexions de clients qui se trouvent dans des emplacements non approuvés, comme Internet ou une forêt non approuvée. (Les sites secondaires ne prennent pas en charge les connexions du client à partir d'emplacements non approuvés) :

- Point du site web du catalogue des applications
- Module de stratégie de Configuration Manager
- Point de distribution (HTTPS est requis par les points de distribution cloud)
- Point proxy d'inscription
- Point d'état de secours
- Point de gestion
- Point de mise à jour logicielle

**À propos des systèmes de site accessibles sur Internet :**

Vous n'avez pas besoin d'une relation d'approbation entre la forêt d'un client et celle du serveur de système de site. Toutefois, quand la forêt qui contient un système de site accessible sur Internet approuve la forêt qui contient les comptes d'utilisateurs, cette configuration prend en charge les stratégies utilisateur pour les appareils sur Internet quand vous activez le paramètre client **Autoriser les demandes de stratégie utilisateur depuis des**

**clients Internet** de la **Stratégie client**.

Par exemple, les configurations suivantes illustrent la prise en charge par la gestion des clients basés sur Internet des stratégies utilisateur pour les appareils situés sur Internet :

- Le point de gestion basé sur Internet est le réseau de périmètre sur lequel réside un contrôleur de domaine en lecture seule pour authentifier l'utilisateur et un pare-feu qui intervient autorise les paquets Active Directory.
- Le compte d'utilisateur se trouve dans la forêt A (Intranet) et le point de gestion basé sur Internet dans la forêt B (le réseau de périmètre). La forêt B approuve la forêt A et un pare-feu qui intervient autorise les paquets d'authentification.
- Le compte d'utilisateur et le point de gestion basé sur Internet sont dans la forêt A (Intranet). Le point de gestion est publié sur Internet à l'aide d'un serveur proxy web (comme Forefront Threat Management Gateway).

> **NOTE**
> Si l'authentification Kerberos échoue, l'authentification NTLM est ensuite automatiquement utilisée.

Comme l'indique l'exemple précédent, vous pouvez placer des systèmes de site basés sur Internet dans l'Intranet lorsqu'ils sont publiés sur Internet à l'aide d'un serveur proxy Web, tel que ISA Server et Forefront Threat Management Gateway. Ces systèmes de site peuvent être configurés pour la connexion du client à partir d'Internet uniquement, ou pour les connexions du client à partir d'Internet et d'un intranet. Quand vous utilisez un serveur proxy web, vous pouvez le configurer pour le pontage SSL (Secure Sockets Layer) vers SSL (plus sécurisé) ou le tunnel SSL, comme suit :

- **Pontage SSL vers SSL :**
  La configuration recommandée quand vous utilisez des serveurs web proxy pour la gestion de clients sur Internet est le pontage SSL vers SSL, qui utilise une terminaison SSL avec authentification. Les ordinateurs clients doivent être authentifiés à l'aide de l'authentification de l'ordinateur et les clients hérités de l'appareil mobile sont authentifiés à l'aide de l'authentification utilisateur. Les appareils mobiles inscrits par Configuration Manager ne prennent pas en charge le pontage SSL.

  La terminaison SSL au niveau du serveur Web proxy présente l'avantage que les paquets provenant d'Internet sont inspectés avant d'être transférés au réseau interne. Le serveur Web proxy authentifie la connexion du client, l'arrête, puis ouvre une nouvelle connexion authentifiée vers les systèmes de site basés sur Internet. Quand les clients Configuration Manager utilisent un serveur web proxy, leur identité (GUID client) est contenue en toute sécurité dans la charge utile du paquet pour éviter que le point de gestion prenne le serveur web proxy pour le client. Le pontage n'est pas pris en charge dans Configuration Manager de HTTP vers HTTPS ou de HTTPS vers HTTP.

- **Tunneling** :
  Si votre serveur web proxy ne peut pas prendre en charge la configuration requise pour le pontage SSL, ou si vous souhaitez configurer la prise en charge Internet pour les appareils mobiles inscrits par Configuration Manager, le tunneling SSL est aussi pris en charge. Il s'agit d'une option moins sûre car les paquets SSL d'Internet sont transférés aux systèmes de site sans terminaison SSL et ne peuvent donc pas être inspectés à la recherche de contenu malveillant. Lors de l'utilisation du tunnel SSL, aucune configuration n'est requise pour les certificats pour le serveur Web proxy.

## Communications dans les forêts Active Directory

System Center Configuration Manager prend en charge des sites et des hiérarchies qui recouvrent des forêts Active Directory.

Configuration Manager prend également en charge les ordinateurs de domaine qui ne se trouvent pas dans la même forêt Active Directory que le serveur de site, et les ordinateurs qui se trouvent dans des groupes de travail :

- **Pour prendre en charge des ordinateurs de domaine situés dans une forêt qui n'est pas approuvée par la forêt de votre serveur de site**, vous pouvez procéder comme suit :
  - Installez des rôles de système de site dans cette forêt non approuvée, en activant l'option de publication des informations de site dans cette forêt Active Directory.
  - Gérez ces ordinateurs comme des ordinateurs de groupe de travail.

  Quand vous installez des serveurs de système de site dans une forêt Active Directory non approuvée, les communications des clients de cette forêt vers le serveur restent internes à cette forêt, ce qui permet à Configuration Manager d'authentifier l'ordinateur avec Kerberos. Quand vous publiez des informations de site dans la forêt du client, le client peut récupérer les informations de site, notamment la liste des points de gestion disponibles, à partir de sa forêt Active Directory, au lieu de télécharger ces informations à partir de son point de gestion attribué.

  > **NOTE**
  > Pour gérer les appareils qui se trouvent sur Internet, vous pouvez installer des rôles système de site de type Internet dans votre réseau de périmètre lorsque des serveurs de système de site se trouvent dans une forêt Active Directory. Ce scénario ne nécessite pas d'approbation bidirectionnelle entre le réseau de périmètre et la forêt du serveur de site.

- **Pour prendre en charge des ordinateurs situés dans un groupe de travail**, vous devez effectuer les opérations suivantes :
  - Approuvez manuellement les ordinateurs du groupe de travail qui utilisent des connexions client HTTP pour accéder aux rôles de système de site. En effet, Configuration Manager ne peut pas authentifier ces ordinateurs avec Kerberos.
  - Configurez les clients du groupe de travail avec le compte d'accès réseau pour permettre à ces ordinateurs de récupérer le contenu à partir des points de distribution.
  - Fournir aux clients du groupe de travail une méthode de remplacement pour rechercher les points de gestion. Vous pouvez utiliser la publication DNS, WINS, ou attribuer directement un point de gestion. Cela est dû au fait que ces clients ne peuvent pas récupérer les informations de site à partir des services de domaine Active Directory.

  Ressources connexes dans cette bibliothèque de contenu :
  - Gérer les conflits d'enregistrement pour les clients Configuration Manager
  - Compte d'accès au réseau
  - Installer des clients Configuration Manager sur des ordinateurs de groupe de travail

**Scénarios de prise en charge d'un site ou d'une hiérarchie qui s'étend sur plusieurs domaines et forêts**

**Communication entre les sites d'une hiérarchie qui s'étend sur des forêts**

Ce scénario nécessite une approbation de forêt bidirectionnelle prenant en charge l'authentification Kerberos. Si vous n'avez pas d'approbation de forêt bidirectionnelle prenant en charge l'authentification Kerberos, Configuration Manager ne prend pas en charge de site enfant dans la forêt distante.

**Configuration Manager prend en charge l'installation d'un site enfant dans une forêt distante qui possède l'approbation bidirectionnelle requise avec la forêt du site parent.**

- Par exemple, vous pouvez placer un site secondaire dans une autre forêt de son site parent principal tant que l'approbation nécessaire existe.

> **NOTE**
> Un site enfant peut être un site principal (où le site d'administration centrale est le site parent) ou un site secondaire.

Les communications intersite dans Configuration Manager utilisent la réplication de base de données et les transferts basés sur des fichiers. Quand vous installez un site, vous devez spécifier un compte à utiliser pour installer le site sur le serveur indiqué. Ce compte établit et conserve également la communication entre les sites.

Une fois que le site a installé et lancé avec succès les transferts basés sur des fichiers et la réplication de base de données, il est inutile de configurer autre chose pour la communication vers le site.

**Lorsqu'une approbation de forêt bidirectionnelle existe, Configuration Manager ne nécessite aucune étape de configuration supplémentaire.**

Par défaut, lorsque vous installez un nouveau site en tant qu'enfant d'un autre site, Configuration Manager configure les éléments suivants :

- Un itinéraire de réplication de fichiers intersite sur chaque site qui utilise le compte d'ordinateur du serveur de site. Configuration Manager ajoute le compte d'ordinateur de chaque ordinateur au groupe **SMS_SiteToSiteConnection_<code_site>** sur l'ordinateur de destination.
- Réplication de base de données entre les serveurs SQL Server sur chaque site.

Les configurations suivantes doivent également être définies :

- Les appareils réseau et les pare-feu qui interviennent doivent autoriser les paquets réseau requis par Configuration Manager.
- La résolution de noms doit fonctionner entre les forêts.
- Pour installer un site ou un rôle de système de site, vous devez spécifier un compte qui dispose des autorisations d'administrateur local sur l'ordinateur spécifié.

#### Communication dans un site qui s'étend sur des forêts

Ce scénario ne nécessite aucune approbation de forêt bidirectionnelle.

**Les sites principaux prennent en charge l'installation de rôles de système de site sur les ordinateurs des forêts distantes**.

- Le point de service web du catalogue des applications est la seule exception. Il est uniquement pris en charge dans la même forêt que le serveur de site.
- Si le rôle de système de site accepte les connexions depuis Internet, comme bonne pratique de sécurité, installez ces rôles de système de site dans un emplacement où la limite de forêt fournit une protection pour le serveur de site (par exemple, dans un réseau de périmètre).

**Pour installer un rôle de système de site sur un ordinateur situé dans une forêt non approuvée :**

- Vous devez spécifier un **Compte d'installation du système de site**, utilisé pour installer le rôle de système de site. (Ce compte doit disposer d'informations d'identification administratives locales pour la connexion.) Ensuite, installez les rôles de système de site sur l'ordinateur spécifié.
- Vous devez sélectionner l'option de système de site **Exiger que le serveur de site établisse des connexions vers ce système de site**. Pour cela, le serveur de site doit établir des connexions au serveur de système de site pour transférer des données. De cette manière, l'ordinateur qui se trouve dans l'emplacement non approuvé ne peut pas établir de contact avec le serveur de site au sein de votre réseau approuvé. Ces connexions utilisent le **Compte d'installation du système de site**.

**Pour utiliser un rôle de système de site installé dans une forêt non approuvée,** les pare-feu doivent

autoriser le trafic réseau, même quand le serveur de site lance le transfert de données.

Par ailleurs, les rôles de système de site suivants requièrent un accès direct à la base de données de site. Par conséquent, les pare-feu doivent autoriser le trafic applicable de la forêt non approuvée vers les sites SQL Server :

- Point de synchronisation Asset Intelligence
- Point Endpoint Protection
- Point d'inscription
- Point de gestion
- Point du service de rapport
- Point de migration d'état

Pour plus d'informations, consultez Ports utilisés dans System Center Configuration Manager.

**Vous serez peut-être amené à configurer l'accès des rôles système de site à la base de données du site :**

Les rôles de système de site de point d'inscription et de point de gestion se connectent à la base de données de site.

- Par défaut, quand ces rôles de système de site sont installés, Configuration Manager configure le compte d'ordinateur du nouveau serveur de système de site comme compte de connexion pour le rôle de système de site et ajoute le compte au rôle de base de données SQL Server approprié.
- Lorsque vous installez ces rôles de système de site dans un domaine non approuvé, vous devez configurer le compte de connexion du rôle de système de site pour autoriser le rôle de système de site à obtenir des informations à partir de la base de données.

Si vous configurez un compte d'utilisateur de domaine comme compte de connexion pour ces rôles de système de site, assurez-vous que le compte d'utilisateur de domaine dispose des accès appropriés à la base de données SQL Server sur ce site :

- Point de gestion : **compte de connexion à la base de données du point de gestion**.
- Point d'inscription : **compte de connexion du point d'inscription**.

Lorsque vous planifiez des rôles de système de site dans d'autres forêts, tenez compte des informations supplémentaires suivantes :

- Si vous exécutez un pare-feu Windows, configurez les profils de pare-feu applicables pour transmettre les communications entre le serveur de base de données du site et les ordinateurs qui sont installés avec des rôles de système de site distants. Pour plus d'informations sur les profils de pare-feu, consultez Présentation des profils de Pare-feu.
- Lorsque le point de gestion basé sur Internet approuve la forêt contenant les comptes d'utilisateur, les stratégies utilisateur sont prises en charge. Lorsqu'il n'existe aucune relation d'approbation, seules les stratégies d'ordinateur sont prises en charge.

#### Communication entre les clients et les rôles de système de site quand les clients ne se trouvent pas dans la même forêt Active Directory que leur serveur de site

Configuration Manager prend en charge les scénarios suivants pour les clients qui ne se trouvent pas dans la même forêt que le serveur de site de leur site :

- Il existe une relation d'approbation de forêt bidirectionnelle entre la forêt du client et celle du serveur du site.
- Le serveur de rôle de système de site se trouve dans la même forêt que le client.

- Le client se trouve sur un ordinateur de domaine sans approbation de forêt bidirectionnelle avec le serveur de site, et les rôles de système de site ne sont pas installés dans la forêt du client.
- Le client se trouve sur un ordinateur de groupe de travail.

Les clients se trouvant sur un ordinateur joint à un domaine peuvent utiliser les services de domaine Active Directory pour l'emplacement du service si leur site est publié dans leur forêt Active Directory.

Pour publier des informations de site dans une autre forêt Active Directory, vous devez effectuer les opérations suivantes :

- Spécifiez la forêt et activez la publication dans cette forêt dans le nœud **Forêts Active Directory** de l'espace de travail **Administration** .
- Configurez chaque site pour publier ses données dans les services de domaine Active Directory. Cette configuration permet aux clients se trouvant dans cette forêt d'extraire des informations de site et de trouver des points de gestion. Pour un client qui ne peut pas utiliser les services de domaine Active Directory pour l'emplacement du service, vous pouvez utiliser DNS, WINS ou le point de gestion attribué du client.

**Placer le connecteur du serveur Exchange Server dans une forêt distante**

Pour prendre en charge ce scénario, assurez-vous que la résolution de noms fonctionne entre les forêts (par exemple, via une configuration DNS supplémentaire) et spécifiez le nom de domaine complet (FQDN) intranet du serveur Exchange Server au moment où vous configurez le connecteur du serveur Exchange Server. Pour plus d'informations, consultez Gérer les appareils mobiles avec System Center Configuration Manager et Exchange.

# Outil de maintenance hiérarchique (Preinst.exe) pour System Center Configuration Manager

22/06/2018 • 14 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

L'outil de maintenance hiérarchique (Preinst.exe) transfère des commandes au service Gestionnaire de hiérarchie de System Center Configuration Manager, si ce service est en cours d'exécution. Quand vous installez un site Configuration Manager, l'outil de maintenance hiérarchique est automatiquement installé. Preinst.exe se trouve dans le dossier partagé \<*nom_serveur_site*>\SMS_<*code_site*\bin\X64\00000409 sur le serveur de site.

Vous pouvez utiliser l'outil de maintenance hiérarchique dans les cas suivants :

- Quand l'échange de clé sécurisé est requis, il existe des situations dans lesquelles vous devez effectuer manuellement l'échange initial de clé publique entre les sites. Pour plus d'informations, consultez Échanger manuellement des clés publiques entre des sites dans cette rubrique.
- Pour supprimer les tâches actives qui concernent un site de destination qui n'est plus disponible.
- Pour supprimer un serveur de site de la console Configuration Manager quand vous ne pouvez pas désinstaller le site à l'aide du programme d'installation. Par exemple, si vous supprimez physiquement un site Configuration Manager sans exécuter d'abord le programme d'installation pour désinstaller le site, les informations du site sont conservées dans la base de données du site parent, lequel continuera d'essayer de communiquer avec le site enfant supprimé. Pour résoudre ce problème, vous devez exécuter l'outil de maintenance hiérarchique et supprimer manuellement le site enfant de la base de données du site parent.
- Pour arrêter simultanément tous les services Configuration Manager sur un site, et éviter ainsi d'avoir à les arrêter un à un.
- Lorsque vous restaurez un site, vous pouvez utiliser l'option CHILDKEYS pour distribuer les clés publiques à partir de plusieurs sites enfants vers le site de récupération.

Pour exécuter l'outil de maintenance hiérarchique, l'utilisateur doit disposer de privilèges d'administration sur l'ordinateur local. De plus, l'utilisateur doit disposer de façon explicite du droit de sécurité d'administration du site. Le fait d'hériter de ce droit par l'appartenance à un groupe qui dispose de ce droit n'est pas suffisant.

## Options de ligne de commande de l'outil de maintenance hiérarchique

Lorsque vous utilisez l'outil de maintenance hiérarchique, vous devez l'exécuter localement sur le site d'administration centrale, le site principal ou le serveur de site secondaire.

Pour exécuter l'outil de maintenance hiérarchique, utilisez la syntaxe suivante : preinst.exe /<option>. Les options de ligne de commande sont les suivantes.

**/DELJOB <*Code_site*>** : utilisez cette option sur un site pour supprimer l'ensemble des travaux ou commandes entre le site actuel et le site de destination spécifié.

**/DELSITE <*code_site_enfant_à_supprimer*>** : utilisez cette option sur un site parent pour supprimer les données des sites enfants dans la base de données de site du site parent. En règle générale, cette option est utilisée si un ordinateur du serveur de site est désactivé avant de désinstaller le site à partir de celui-ci.

> **NOTE**
> L'option /DELSITE ne désinstalle pas le site sur l'ordinateur spécifié par le paramètre ChildSiteCodeToRemove. Cette option supprime uniquement les informations du site dans la base de données de site Configuration Manager.

**/DUMP <*code_site*>** : utilisez cette option sur le serveur de site local pour écrire des images de contrôle de site dans le dossier racine du lecteur sur lequel le site est installé. Vous pouvez écrire une image de contrôle de site spécifique dans le dossier ou écrire tous les fichiers de contrôle de site de la hiérarchie.

- /DUMP <*code_site*> écrit l'image de contrôle de site uniquement pour le site spécifié.
- /DUMP écrit les fichiers de contrôle de site pour tous les sites.

Une image est une représentation binaire du fichier de contrôle de site, stockée dans la base de données de site Configuration Manager. L'image du fichier de contrôle de site enregistrée représente la somme de l'image de base et des images delta en attente.

Une fois l'image du fichier de contrôle de site supprimée à l'aide de l'outil de maintenance hiérarchique, le nom du fichier est au format sitectrl_<*code_site*>.ct0.

**/STOPSITE** : utilisez cette option sur le serveur de site local pour lancer un cycle d'arrêt du service Gestionnaire de composant de site dans Configuration Manager, ce qui réinitialise partiellement le site. L'exécution de ce cycle d'arrêt entraîne l'arrêt de certains services Configuration Manager sur un serveur de site et ses systèmes de site distants. Ces services sont marqués en vue d'être réinstallés. À la suite de ce cycle d'arrêt, certains mots de passe sont automatiquement modifiés lorsque les services sont réinstallés.

> **NOTE**
> Si vous souhaitez enregistrer un arrêt, une réinstallation et un changement de mot de passe pour le Gestionnaire de composants de site, activez l'enregistrement de ce composant avant de vous servir de cette option de ligne de commande.

Après le démarrage du cycle d'arrêt, il fonctionne automatiquement en ignorant les composants et les ordinateurs qui ne répondent pas. Toutefois, si le service Gestionnaire de composants de site ne peut pas accéder à un système de site distant pendant le cycle d'arrêt, les composants installés sur ce système de site sont réinstallés au prochain démarrage du Gestionnaire de composants de site. Lors de son redémarrage, le service Gestionnaire de composants de site tente plusieurs réinstallations de tous les services marqués en vue d'une réinstallation, jusqu'à ce qu'il réussisse.

Vous pouvez redémarrer le service Gestionnaire de composants de site avec le Gestionnaire de services. Après son redémarrage, tous les services affectés sont désinstallés, réinstallés et redémarrés. Lorsque vous avez utilisé l'option /STOPSITE pour initialiser un cycle d'arrêt, vous ne pouvez pas éviter les cycles de réinstallation après le redémarrage du service Gestionnaire de composants de site.

**/KEYFORPARENT** - Utilisez cette option sur un site pour distribuer la clé publique du site à un site parent.

L'option /KEYFORPARENT copie la clé publique du site dans le fichier <*code_site*>.CT4 situé à la racine du lecteur des fichiers programme. Après avoir exécuté preinst.exe avec cette option, copiez manuellement le fichier <*code_site*>.CT4 dans le dossier ...\Inboxes\hman.box (et non pas hman.box\pubkey) du site parent.

**/KEYFORCHILD** - Utilisez cette option sur un site pour distribuer la clé publique du site à un site enfant.

L'option /KEYFORCHILD copie la clé publique du site dans le fichier <*code_site*>.CT5 à la racine du lecteur des fichiers programme. Après avoir exécuté preinst.exe avec cette option, copiez manuellement le fichier <*code_site*>.CT5 dans le dossier ...\Inboxes\hman.box (et non pas hman.box\pubkey) du site enfant.

**/CHILDKEYS** - Vous pouvez utiliser cette option sur les sites enfants d'un site que vous récupérez. Utilisez cette

option pour distribuer les clés publiques de plusieurs sites enfants sur le site en cours de récupération.

L'option /CHILDKEYS copie la clé du site sur lequel vous exécutez l'option, et toutes les clés publiques des sites enfants de ce site, dans le fichier <*code_site*>.CT6.

Après avoir exécuté preinst.exe avec cette option, copiez manuellement le fichier <*code_site*>.CT6 dans le dossier ...\Inboxes\hman.box (et non pas hman.box\pubkey) du site en cours de récupération.

**/PARENTKEYS** - Vous pouvez utiliser cette option sur le site parent d'un site que vous récupérez. Utilisez cette option pour distribuer les clés publiques de tous les sites parents sur le site en cours de récupération.

L'option /PARENTKEYS copie la clé du site sur lequel vous exécutez l'option, ainsi que les clés de chaque site parent situé au-dessus de ce site, dans le fichier <code_site>.CT7.

Après avoir exécuté preinst.exe avec cette option, copiez manuellement le fichier <*code_site*>.CT7 dans le dossier ...\Inboxes\hman.box (et non pas hman.box\pubkey) du site en cours de récupération.

# Échanger manuellement des clés publiques entre des sites

Par défaut, l'option **Nécessite l'échange de clés sécurisées** est activée pour les sites Configuration Manager. Quand l'échange de clé sécurisé est requis, il existe deux situations dans lesquelles vous devez effectuer manuellement l'échange initial de clé entre les sites :

- Le schéma Active Directory n'a pas été étendu pour Configuration Manager.
- Les sites Configuration Manager ne publient pas de données de site dans Active Directory.

Vous pouvez utiliser l'outil de maintenance hiérarchique pour exporter les clés publiques pour chaque site. Une fois qu'elles ont été exportées, vous devez échanger manuellement les clés entre les sites.

> **NOTE**
> Après l'échange manuel des clés, vous pouvez consulter le fichier journal **hman.log** , qui enregistre les modifications de la configuration du site et la publication des informations du site vers les services de domaine Active Directory, sur le serveur du site parent pour vous assurer que le site principal a traité la nouvelle clé publique.

#### Pour transférer manuellement la clé publique du site enfant vers le site parent

1. Lorsque vous êtes connecté au site enfant, ouvrez une invite de commande et naviguez jusqu'à l'emplacement de **Preinst.exe**.
2. Tapez la commande suivante pour exporter la clé publique du site enfant : **Preinst /keyforparent**
3. L'option /keyforparent copie la clé publique du site enfant dans le fichier **<code_site>.CT4** situé à la racine du lecteur système.
4. Déplacez le fichier **<code_site>.CT4** vers le dossier **<répertoire_installation>\inboxes\hman.box** du site parent.

#### Pour transférer manuellement la clé publique du site parent vers le site enfant

1. Lorsque vous êtes connecté au site parent, ouvrez une invite de commande et naviguez jusqu'à l'emplacement de **Preinst.exe**.
2. Tapez la commande suivante pour exporter la clé publique du site parent : **Preinst /keyforchild**.
3. L'option /keyforchild copie la clé publique du site parent dans le fichier **<code_site>.CT5** situé à la racine du lecteur système.
4. Déplacez le fichier **<code_site>.CT5** vers le dossier **<répertoire_installation>\inboxes\hman.box** du site enfant.

# Prise en charge internationale dans System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les sections suivantes fournissent des détails techniques qui vous aideront à mettre System Center Configuration Manager en conformité avec des exigences internationales spécifiques.

## Normes GB18030

Configuration Manager respecte les normes GB18030 pour permettre son utilisation en Chine. Un déploiement de Configuration Manager doit disposer des configurations suivantes pour respecter les exigences des normes GB18030 :

- Chaque ordinateur serveur de site et chaque ordinateur SQL Server utilisés avec Configuration Manager doivent utiliser un système d'exploitation chinois.
- Chaque base de données de site et chaque instance de SQL Server dans la hiérarchie doit utiliser le même classement et doit correspondre à l'un des éléments suivants :
  - Chinese_Simplified_Pinyin_100_CI_AI
  - Chinese_Simplified_Stroke_Order_100_CI_AI

  > **NOTE**
  > Ces classements de bases de données constituent une exception aux exigences décrites dans Prise en charge des versions de SQL Server pour System Center Configuration Manager.

- Vous devez placer un fichier portant le nom **GB18030.SMS** dans le dossier racine du volume du système de chaque ordinateur du serveur de site dans la hiérarchie. Ce fichier ne contient pas de données et peut être un fichier texte vide, nommé pour répondre à cette exigence.

# Interopérabilité entre les différentes versions de System Center Configuration Manager

22/06/2018 • 15 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez installer et utiliser plusieurs hiérarchies indépendantes de System Center Configuration Manager sur le même réseau. Toutefois, étant donné que des hiérarchies différentes de Configuration Manager n'interagissent pas en dehors du processus de migration, chaque hiérarchie nécessite une configuration pour éviter des conflits. En outre, vous pouvez créer certaines configurations pour faciliter l'interaction des ressources que vous gérez avec les systèmes de site de la hiérarchie correcte.

Les sections suivantes fournissent des informations sur l'utilisation de différentes versions de Configuration Manager sur le même réseau :

- Interopérabilité entre System Center Configuration Manager et les versions antérieures du produit
- Interopérabilité de la console Configuration Manager
- Limitations de Configuration Manager dans une hiérarchie de versions mixtes

## Interopérabilité entre System Center Configuration Manager et les versions antérieures du produit

Les sites de différentes versions ne peuvent pas coexister dans la même hiérarchie, sauf pendant le processus de mise à niveau de System Center 2012 Configuration Manager vers System Center Configuration Manager ou d'une version de System Center Configuration Manager vers une version plus récente (à l'aide de mises à jour dans la console).

Étant donné que vous pouvez déployer un site et une hiérarchie System Center Configuration Manager côte à côte avec un site ou une hiérarchie System Center 2012 Configuration Manager qui existe déjà, nous vous recommandons d'empêcher les clients de l'une des versions de tenter de joindre un site à partir de l'autre version.

Par exemple, si plusieurs hiérarchies Configuration Manager ont des limites qui se chevauchent (voir Chevauchement des limites) qui incluent les mêmes emplacements réseau, une bonne pratique consiste à attribuer chaque nouveau client à un site spécifique au lieu d'utiliser l'attribution de site automatique. Pour plus d'informations sur l'attribution de site automatique dans System Center 2012 Configuration Manager, consultez Guide pratique pour attribuer des clients à un site dans System Center Configuration Manager.

De plus, vous ne pouvez pas installer un client à partir de System Center 2012 Configuration Manager sur un ordinateur qui héberge un rôle système de site de System Center Configuration Manager, ni installer un client System Center Configuration Manager sur un ordinateur qui héberge un rôle système de site de System Center 2012 Configuration Manager.

De même, les clients suivants et la connexion VPN (Virtual Private Network) suivante ne sont pas pris en charge :

- Toute version de client System Center 2012 Configuration Manager ou antérieure
- Tout client de gestion des appareils System Center 2012 Configuration Manager ou antérieur
- Client de gestion des appareils Windows CE Platform Builder (toute version)
- Connexion VPN System Center Mobile Device Manager

**Considérations sur l'attribution de sites aux clients**

Les clients System Center Configuration Manager peuvent être attribués à un seul site principal. Si l'attribution automatique de site est utilisée pour attribuer des clients à un site lors de l'installation du client, et qu'une même limite est configurée sur plusieurs groupes et différents sites sont attribués aux groupes de limites, l'attribution de site d'un client n'est pas prévisible.

Si des limites se chevauchent sur plusieurs hiérarchies et sites Configuration Manager, les clients risquent de ne pas être attribués au site que vous escomptez ou de n'être attribués à aucun site.

Les clients System Center Configuration Manager vérifient la version du site Configuration Manager avant de procéder à l'attribution de site et ne peuvent pas être attribués à une version précédente quand et si des limites se chevauchent. Toutefois, les clients System Center 2012 Configuration Manager peuvent être incorrectement attribués à un site System Center Configuration Manager.

Pour empêcher l'attribution involontaire de clients au mauvais site quand les limites des deux hiérarchies se chevauchent, nous vous recommandons de configurer les paramètres d'installation du client Configuration Manager de manière à attribuer des clients à un site spécifique.

# Limitations de Configuration Manager dans une hiérarchie de versions mixtes

Pendant la mise à niveau d'un site System Center Configuration Manager, il se peut que la version varie d'un site à l'autre. Par exemple, vous pouvez mettre à niveau un site d'administration centrale vers une nouvelle version, mais en raison des fenêtres de maintenance de site, un ou plusieurs sites principaux ne peuvent pas être mis à niveau avant une date et une heure futures.

Quand différents sites dans une même hiérarchie exécutent différentes versions, certaines fonctionnalités ne sont pas disponibles. Cela peut affecter la manière dont vous gérez les objets Configuration Manager dans la console Configuration Manager, ainsi que les fonctionnalités accessibles aux clients. Généralement, la fonctionnalité de la version la plus récente de Configuration Manager n'est pas accessible sur des sites ou par des clients qui exécutent une version de Service Pack antérieure.

**Limitations liées à la mise à niveau de Configuration Manager**

| OBJET | DÉTAILS |
|---|---|
| Compte d'accès réseau | **Mise à niveau de System Center 2012 Configuration Manager vers System Center Configuration Manager :** quand vous affichez les détails du compte d'accès réseau à partir d'une console Configuration Manager connectée à un site d'administration centrale mis à jour vers System Center Configuration Manager, la console n'affiche pas les détails des comptes qui sont configurés sur un site principal qui exécute System Center 2012 Configuration Manager. Une fois le site principal mis à niveau vers la même version que le site d'administration centrale, les détails du compte sont visibles dans la console.<br><br>**Mise à niveau entre des versions de System Center Configuration Manager :** quand vous affichez les détails du compte d'accès réseau à partir d'une console Configuration Manager connectée à un site d'administration centrale ayant été mis à jour vers une nouvelle version de System Center Configuration Manager, la console n'affiche pas de détails pour les comptes qui sont configurés sur un site principal qui exécute une version antérieure. Une fois le site principal mis à niveau vers la même version que le site d'administration centrale, les détails du compte sont visibles dans la console. |

| OBJET | DÉTAILS |
| --- | --- |
| Images de démarrage pour le déploiement de système d'exploitation | **Mise à niveau de System Center 2012 Configuration Manager vers System Center Configuration Manager :** quand le site de niveau supérieur d'une hiérarchie se met à niveau vers System Center Configuration Manager, les images de démarrage par défaut sont automatiquement mises à jour vers des images de démarrage basées sur Windows Assessment and Deployment Kit 10 (Windows ADK). Utilisez ces images de démarrage uniquement pour les déploiements sur des clients de sites System Center Configuration Manager. Pour plus d'informations, consultez Planification de l'interopérabilité des déploiements de systèmes d'exploitation dans System Center Configuration Manager.<br><br>**Mise à niveau entre des versions de System Center Configuration Manager :** tant que les nouvelles versions de cm6long ne mettent pas à jour la version de Windows ADK en cours d'utilisation, il n'y a aucune incidence sur les images de démarrage. |
| Nouvelles étapes de séquence de tâche | Quand vous créez une séquence de tâches avec une étape introduite dans une version de Configuration Manager qui n'est pas disponible dans une version antérieure, vous pouvez rencontrer les problèmes suivants :<br><br>-- Une erreur se produit quand vous essayez de modifier la séquence de tâches à partir d'un site exécutant une version précédente de Configuration Manager.<br><br>-- La séquence de tâches ne s'exécute pas sur un ordinateur exécutant une version antérieure du client Configuration Manager. |
| Communications entre le client et un point de gestion de niveau inférieur | Un client Configuration Manager qui communique avec un point de gestion d'un site exécutant une version plus ancienne que celle du client ne peut utiliser que les fonctionnalités prises en charge par la version de niveau inférieur de Configuration Manager. Par exemple, si vous déployez du contenu d'un site Configuration Manager récemment mis à niveau vers un client qui communique avec un point de gestion qui n'a pas encore été mis à niveau vers cette version, ce client ne peut pas utiliser les nouvelles fonctionnalités de la version la plus récente. |

## Interopérabilité de la console Configuration Manager

Le tableau suivant contient des informations sur l'utilisation de la console Configuration Manager dans un environnement qui possède un mélange de versions de Configuration Manager.

| ENVIRONNEMENT D'INTEROPÉRABILITÉ | PLUS D'INFORMATIONS |
| --- | --- |

| ENVIRONNEMENT D'INTEROPÉRABILITÉ | PLUS D'INFORMATIONS |
| --- | --- |
| Un environnement avec à la fois System Center 2012 Configuration Manager et System Center Configuration Manager | Pour gérer un site Configuration Manager, la console et le site auquel elle se connecte doivent tous les deux exécuter la même version de Configuration Manager. Par exemple, vous ne pouvez pas utiliser une console System Center 2012 Configuration Manager pour gérer un site System Center Configuration Manager, ou vice versa.<br><br>L'installation à la fois de la console System Center 2012 Configuration Manager et de la console System Center Configuration Manager sur le même ordinateur n'est pas prise en charge. |
| Environnement avec plusieurs versions de System Center Configuration Manager | System Center Configuration Manager ne prend pas en charge l'installation de plusieurs consoles Configuration Manager sur un ordinateur. Pour utiliser plusieurs consoles propres à différentes versions de System Center Configuration Manager, vous devez installer les différentes consoles sur des ordinateurs distincts.<br><br>Pendant le processus de mise à jour de sites dans une hiérarchie avec une nouvelle version, vous pouvez connecter une console à un site qui exécute une version plus récente et afficher des informations sur d'autres sites de cette hiérarchie. Toutefois, cette configuration n'est pas recommandée, car les différences entre la version de la console et la version du site Configuration Manager risquent d'entraîner des problèmes de données, et certaines fonctionnalités qui sont disponibles dans la dernière version du produit ne sont pas disponibles dans la console.<br><br>La gestion d'un site avec une console dont la version ne correspond pas à la version du site n'est pas prise en charge. Elle peut entraîner une perte de données et exposer votre site à des risques. Par exemple, l'utilisation d'une console avec la version 1610 pour gérer un site qui exécute la version 1606 n'est pas prise en charge. |

# Modules linguistiques dans Configuration Manager

10/07/2018 • 6 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cet article fournit des détails techniques sur la prise en charge linguistique dans Configuration Manager. Les clients et serveurs du site Configuration Manager sont considérés comme étant indépendants de la langue. Ajoutez la prise en charge des langues d'affichage en installant les **modules linguistiques du serveur** ou les **modules linguistiques du client** sur le site d'administration centrale et sur les sites principaux. Vous sélectionnez les langues de serveur et de client à prendre en charge sur ce site parmi les fichiers de modules linguistiques disponibles au cours du processus d'installation.

Installez plusieurs langues sur chaque site. Il vous suffit d'installer les langues que vous utilisez.

- Chaque site prend en charge plusieurs langues pour les consoles Configuration Manager.
- Sur chaque site, vous pouvez installer des modules linguistiques client individuels et ajouter ainsi une prise en charge uniquement des langues client souhaitées.

Lorsque vous installez la prise en charge pour une langue qui correspond aux composants suivants :

- Langue d'affichage d'un ordinateur : les consoles Configuration Manager et l'interface utilisateur client qui s'exécutent sur cet ordinateur affichent les informations dans cette langue.
- Langue qui correspond aux préférences linguistiques en vigueur sur le navigateur Web d'un ordinateur : les connexions aux informations Web, notamment le catalogue d'applications et SQL Server Reporting Services, s'affichent dans cette langue.

Lorsque vous exécutez le programme d'installation de Configuration Manager, les fichiers de modules linguistiques sont téléchargés dans le cadre des fichiers prérequis et redistribuables. Vous pouvez également utiliser le Téléchargeur d'installation pour télécharger ces fichiers avant d'exécuter le programme d'installation.

## Langues du serveur

Aidez-vous du tableau suivant pour mapper un ID de paramètres régionaux à la langue que vous souhaitez prendre en charge sur des serveurs. Pour plus d'informations sur les ID de paramètres régionaux, consultez ID de paramètres régionaux attribués par Microsoft.

| LANGUE DU SERVEUR | ID DE PARAMÈTRES RÉGIONAUX (LCID) | CODE EN TROIS LETTRES |
|---|---|---|
| Anglais (par défaut) | 0409 | ENU |
| Chinois (traditionnel, Hong Kong R.A.S.) | 0c04 | ZHH |
| Chinois (simplifié) | 0804 | CHS |
| Chinois (traditionnel, Taïwan) | 0404 | CHT |
| Tchèque | 0405 | CSY |
| Néerlandais - Pays-bas | 0413 | NLD |

| LANGUE DU SERVEUR | ID DE PARAMÈTRES RÉGIONAUX (LCID) | CODE EN TROIS LETTRES |
|---|---|---|
| Français | 040c | FRA |
| Allemand | 0407 | DEU |
| Hongrois | 040e | HUN |
| Italien - Italie | 0410 | ITA |
| Japonais | 0411 | JPN |
| Coréen | 0412 | KOR |
| Polonais | 0415 | PLK |
| Portugais - Brésil | 0416 | PTB |
| Portugais - Portugal | 0816 | PTG |
| Russe | 0419 | RUS |
| Espagnol - Espagne | 0c0a | ESN |
| Suédois | 041d | SVE |
| Turc | 041f | TRK |

## Langues du client

Aidez-vous du tableau suivant pour mapper un ID de paramètres régionaux à la langue que vous voulez prendre en charge sur des ordinateurs clients. Pour plus d'informations sur les ID de paramètres régionaux, consultez ID de paramètres régionaux attribués par Microsoft.

| LANGUE DU CLIENT | ID DE PARAMÈTRES RÉGIONAUX (LCID) | CODE EN TROIS LETTRES |
|---|---|---|
| Anglais (par défaut) | 0409 | ENG |
| Chinois (traditionnel, Hong Kong R.A.S.) | 0c04 | ZHH |
| Chinois simplifié | 0804 | CHS |
| Chinois (traditionnel, Taïwan) | 0404 | CHT |
| Tchèque | 0405 | CSY |
| Danois | 0406 | DAN |
| Néerlandais - Pays-bas | 0413 | NLD |
| Finnois | 040b | FIN |

| LANGUE DU CLIENT | ID DE PARAMÈTRES RÉGIONAUX (LCID) | CODE EN TROIS LETTRES |
|---|---|---|
| Français | 040c | FRA |
| Allemand | 0407 | DEU |
| Grec | 0408 | ELL |
| Hongrois | 040e | HUN |
| Italien - Italie | 0410 | ITA |
| Japonais | 0411 | JPN |
| Coréen | 0412 | KOR |
| Norvégien | 0414 | NOR |
| Polonais | 0415 | PLK |
| Portugais (Brésil) | 0416 | PTB |
| Portugais (Portugal) | 0816 | PTG |
| Russe | 0419 | RUS |
| Espagnol - Espagne | 0c0a | ESN |
| Suédois | 041d | SVE |
| Turc | 041f | TRK |

**Langues du client d'appareil mobile**

Quand vous ajoutez des prises en charge linguistiques pour des appareils mobiles, toutes les langues du client d'appareil mobile prises en charge sont incluses. Vous ne pouvez pas sélectionner individuellement les modules linguistiques pour la prise en charge linguistique sur les appareils mobiles.

## Identifier les modules linguistiques installés

Pour savoir quels modules linguistiques sont installés sur un ordinateur qui exécute le client Configuration Manager, recherchez l'ID de paramètres régionaux (LCID) des modules linguistiques installés dans le Registre de l'ordinateur. Ces informations sont disponibles dans le chemin de registre suivant :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CCMSetup\InstalledLangs
```

Personnalisez l'inventaire matériel pour rassembler ces informations. Puis, générez un rapport personnalisé pour afficher les détails linguistiques. Pour plus d'informations sur l'inventaire matériel personnalisé, consultez Guide pratique pour configurer l'inventaire matériel. Pour plus d'informations sur la création de rapports, consultez Gérer les rapports Configuration Manager.

# Fichiers journaux dans System Center Configuration Manager

22/06/2018 • 103 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Dans Configuration Manager, les composants des clients et des serveurs de site enregistrent les informations sur les processus dans des fichiers journaux individuels. Vous pouvez utiliser les informations contenues dans ces fichiers journaux pour résoudre les problèmes susceptibles de survenir. Par défaut, Configuration Manager active la journalisation pour les composants client et serveur.

Les sections suivantes contiennent des détails sur les différents fichiers journaux disponibles. Surveillez les journaux des clients et serveurs Configuration Manager afin de connaître les détails des opérations, ainsi que pour afficher les informations d'erreur pour résoudre les problèmes.

- Passerelle de gestion cloud
- Paramètres de conformité et accès aux ressources d'entreprise
- Accès conditionnel
- Console Configuration Manager
- Gestion de contenu
- Détection
- Endpoint Protection
- Extensions
- Inventaire
- Contrôle
- Migration
- Appareils mobiles
- Déploiement de systèmes d'exploitation
- Gestion de l'alimentation
- Contrôle à distance
- Rapports
- Administration basée sur des rôles
- Point de connexion de service
- Mises à jour logicielles
- Wake On LAN
- Maintenance de Windows 10
- Agent Windows Update
- Serveur WSUS

## À propos des fichiers journaux de Configuration Manager

La plupart des processus dans Configuration Manager consignent des informations sur les opérations dans un fichier journal dédié à ce processus. Ces fichiers journaux sont identifiés par des extensions de fichier **.log** ou **.lo_**. Configuration Manager écrit dans un fichier .log jusqu'à ce que ce journal atteigne sa taille maximale. Une fois le journal plein, le fichier .log est copié vers un fichier portant le même nom mais avec l'extension .lo_, et le processus ou le composant continue à écrire dans le fichier .log. Quand le fichier .log atteint à nouveau sa taille maximale, le fichier .lo_ est remplacé et le processus se répète. Certains composants établissent un historique du fichier journal en ajoutant une date et une heure au nom du fichier journal, et en conservant l'extension .log. Le client pour Linux et UNIX constitue une exception à la taille maximale et à l'utilisation du fichier .lo_. Pour plus d'informations sur la façon dont le client pour Linux et UNIX utilise les fichiers journaux, consultez Gérer des fichiers journaux dans le client pour Linux et UNIX dans cet article.

Pour afficher les journaux, utilisez la visionneuse du journal Configuration Manager, CMTrace, qui se trouve dans le dossier \\SMSSetup\Tools du média source de Configuration Manager. Il est ajouté à toutes les images de démarrage ajoutées à la Bibliothèque de logiciels.

### Configurer des options de journalisation à l'aide du Gestionnaire de service de Configuration Manager

Vous pouvez changer l'emplacement où Configuration Manager stocke les fichiers journaux, ainsi que leur taille.

Pour modifier la taille des fichiers journaux, changer le nom et l'emplacement du fichier journal, ou forcer plusieurs composants à écrire dans un même fichier journal, procédez comme suit :

#### Pour modifier la journalisation pour un composant

1. Dans la console Configuration Manager, cliquez sur **Surveillance**, sélectionnez **État du système**, puis sélectionnez **État du site** ou **État du composant**.
2. Sous l'onglet **Accueil**, dans le groupe **Composant**, sélectionnez **Démarrer**, puis sélectionnez **Gestionnaire de service de Configuration Manager**.
3. Quand le Gestionnaire de service de Configuration Manager s'ouvre, connectez-vous au site que vous voulez gérer. Si le site que vous voulez gérer n'apparaît pas, sélectionnez **Site**, sélectionnez **Se connecter** et entrez le nom du serveur de site pour le site correct.
4. Développez le site et accédez à **Composants** ou à **Serveurs** selon l'emplacement où se trouvent les composants que vous voulez gérer.
5. Dans le volet de droite, sélectionnez un ou plusieurs composants.
6. Dans le menu **Composant**, sélectionnez **Journalisation**.
7. Dans la boîte de dialogue **Enregistrement du composant Configuration Manager** , choisissez les options de configuration disponibles pour votre sélection.
8. Cliquez sur **OK** pour enregistrer la configuration.

### Localiser les fichiers journaux de Configuration Manager

Configuration Manager stocke les fichiers journaux dans différents emplacements. Ces emplacements dépendent du processus qui crée le fichier journal et de la configuration de vos systèmes de site. L'emplacement du fichier journal pouvant varier sur un ordinateur, utilisez la fonction de recherche pour localiser les fichiers journaux appropriés sur votre ordinateur Configuration Manager si vous devez résoudre les problèmes pour un scénario spécifique.

## Journaux du client Configuration Manager

Les sections suivantes répertorient les fichiers journaux liés aux opérations et à l'installation du client.

### Opérations du client

Le tableau suivant répertorie les fichiers journaux qui se trouvent sur le client Configuration Manager.

| NOM DU FICHIER JOURNAL | DESCRIPTION |
|---|---|
| CAS.log | Service d'accès au contenu. Conserve le cache du package local sur le client. |
| Ccm32BitLauncher.log | Enregistre les actions liées au démarrage des applications sur le client marqué *run as 32 bit* (exécuter en 32 bits). |
| CcmEval.log | Enregistre des activités d'évaluation liées à l'état du client Configuration Manager et des détails sur les composants exigés par le client Configuration Manager. |
| CcmEvalTask.log | Enregistre des activités d'évaluation liées à l'état du client Configuration Manager lancées par la tâche planifiée d'évaluation. |

| NOM DU FICHIER JOURNAL | DESCRIPTION |
| --- | --- |
| CcmExec.log | Enregistre les activités du client et du service Hôte d'agent SMS. Ce fichier journal inclut également des informations sur l'activation et la désactivation du proxy de mise en éveil. |
| CcmMessaging.log | Enregistre les activités liées à la communication entre le client et les points de gestion. |
| CCMNotificationAgent.log | Enregistre les activités liées aux opérations de notification du client. |
| Ccmperf.log | Enregistre les activités liées à la maintenance et la capture de données relatives aux compteurs de performances du client. |
| CcmRestart.log | Enregistre les activités de redémarrage du client. |
| CCMSDKProvider.log | Enregistre les activités pour les interfaces du kit de développement logiciel (SDK) client. |
| CertificateMaintenance.log | Conserve les certificats pour les points de gestion et le service de domaine Active Directory. |
| CIDownloader.log | Enregistre des détails sur les téléchargements des définitions des éléments de configuration. |
| CITaskMgr.log | Enregistre les tâches lancées pour chaque type d'application et de déploiement, comme le téléchargement de contenu, et les actions d'installation ou de désinstallation. |
| ClientAuth.log | Enregistre l'activité de signature et d'authentification pour le client. |
| ClientIDManagerStartup.log | Crée et conserve le GUID du client et identifie les tâches effectuées pendant l'inscription et l'attribution des clients. |
| ClientLocation.log | Enregistre les tâches liées à l'attribution d'un site client. |
| CMHttpsReadiness.log | Enregistre les résultats de l'exécution de l'outil d'évaluation d'analyse HTTPS de Configuration Manager. Cet outil vérifie si les ordinateurs disposent d'un certificat d'authentification de client PKI qui peut être utilisé avec Configuration Manager. |
| CmRcService.log | Enregistre des informations pour le service de contrôle à distance. |
| ContentTransferManager.log | Planifie le service BITS (Background Intelligent Transfer Service) ou SMB (Server Message Block) pour leur permettre de télécharger des packages ou d'y accéder. |
| DataTransferService.log | Enregistre toutes les communications BITS relatives à l'accès aux stratégies ou aux packages. |
| EndpointProtectionAgent | Enregistre des informations concernant l'installation du client System Center Endpoint Protection et l'application de la stratégie anti-programme malveillant à ce client. |

| NOM DU FICHIER JOURNAL | DESCRIPTION |
| --- | --- |
| execmgr.log | Enregistre des détails concernant les packages et les séquences de tâches qui s'exécutent sur le client. |
| ExpressionSolver.log | Enregistre des informations détaillées concernant les méthodes de détection améliorées utilisées quand la journalisation détaillée ou de débogage est activée. |
| ExternalEventAgent.log | Enregistre l'historique de la détection des programmes malveillants par Endpoint Protection et des événements liés à l'état du client. |
| FileBITS.log | Enregistre toutes les tâches d'accès aux packages SMB. |
| FileSystemFile.log | Enregistre l'activité du fournisseur de l'infrastructure de gestion Windows (WMI) pour l'inventaire logiciel et le regroupement de fichiers. |
| FSPStateMessage.log | Enregistre l'activité des messages d'état envoyés par le client au point d'état de secours. |
| InternetProxy.log | Enregistre l'activité de configuration de proxy et d'utilisation réseau pour le client. |
| InventoryAgent.log | Enregistre les activités de l'inventaire matériel et logiciel et les actions de découverte par pulsations effectuées sur le client. |
| LocationCache.log | Enregistre l'activité d'utilisation de l'emplacement du cache et de maintenance pour le client. |
| LocationServices.log | Enregistre l'activité du client pour la localisation des points de gestion, des points de mise à jour logicielle et des points de distribution. |
| MaintenanceCoordinator.log | Enregistre l'activité des tâches de maintenance générale pour le client. |
| Mifprovider.log | Enregistre l'activité du fournisseur WMI pour les fichiers .MIF (Management Information Format). |
| mtrmgr.log | Surveille tous les processus de contrôle des logiciels. |
| PolicyAgent.log | Enregistre les demandes de stratégie effectuées via le service de transfert de données. |
| PolicyAgentProvider.log | Enregistre les changements de stratégie. |
| PolicyEvaluator.log | Enregistre des détails concernant l'évaluation des stratégies sur les ordinateurs clients, dont les stratégies de mises à jour logicielles. |
| PolicyPlatformClient.log | Enregistre le processus de correction et de conformité pour tous les fournisseurs dans %Program Files%\Microsoft Policy Platform, à l'exception du fournisseur de fichier. |

| NOM DU FICHIER JOURNAL | DESCRIPTION |
| --- | --- |
| PolicySdk.log | Enregistre les activités pour les interfaces du kit de développement logiciel (SDK) de système de stratégie. |
| Pwrmgmt.log | Enregistre les informations liées à l'activation ou à la désactivation et à la configuration des paramètres client du proxy de mise en éveil. |
| PwrProvider.log | Enregistre les activités du fournisseur de la gestion de l'alimentation (PWRInvProvider) hébergé dans le service WMI. Sur toutes les versions prises en charge de Windows, le fournisseur énumère les paramètres actuels sur les ordinateurs pendant l'inventaire matériel et applique des paramètres de mode d'alimentation. |
| SCClient<*domaine*>@<*nom_utilisateur*>_1.log | Enregistre l'activité dans le centre logiciel pour l'utilisateur spécifié sur l'ordinateur client. |
| SCClient<*domaine*>@<*nom_utilisateur*>_2.log | Enregistre l'historique des activités dans le centre logiciel pour l'utilisateur spécifié sur l'ordinateur client. |
| Scheduler.log | Enregistre les activités des tâches planifiées pour toutes les opérations du client. |
| SCNotify<*domaine*>@<*nom_utilisateur*>_1.log | Enregistre l'activité de notification des utilisateurs sur les logiciels pour l'utilisateur spécifié. |
| SCNotify<*domaine*>@<*nom_utilisateur*>_1-<*date_heure*>.log | Enregistre l'historique des informations de notification des utilisateurs sur les logiciels pour l'utilisateur spécifié. |
| setuppolicyevaluator.log | Enregistre la création de stratégies d'inventaire et de configuration dans WMI. |
| SleepAgent<*domaine*>@SYSTEM_0.log | Fichier journal principal pour le proxy de mise en éveil. |
| smscliui.log | Enregistre l'utilisation du client Configuration Manager dans le Panneau de configuration. |
| SrcUpdateMgr.log | Enregistre l'activité pour les applications Windows Installer installées, qui sont mises à jour avec les emplacements sources du point de distribution actuel. |
| StatusAgent.log | Enregistre les messages d'état créés par les composants des clients. |
| SWMTRReportGen.log | Génère un rapport des données d'utilisation collectées par l'agent de contrôle. Ces données sont enregistrées dans le fichier journal Mtrmgr.log. |
| UserAffinity.log | Enregistre les détails relatifs à l'affinité entre appareil et utilisateur. |
| VirtualApp.log | Enregistre des informations spécifiques à l'évaluation des types de déploiement App-V (Application Virtualization). |

| NOM DU FICHIER JOURNAL | DESCRIPTION |
| --- | --- |
| Wedmtrace.log | Enregistre les opérations liées aux filtres d'écriture sur les clients Windows Embedded. |
| wakeprxy-install.log | Enregistre les informations liées à l'installation quand les clients reçoivent l'option du paramètre client d'activation du proxy de mise en éveil. |
| wakeprxy-uninstall.log | Enregistre les informations liées à la désinstallation du proxy de mise en éveil quand les clients reçoivent l'option de désactivation du paramètre client du proxy de mise en éveil, si ce proxy a été précédemment activé. |

### Fichiers journaux de l'installation du client

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations relatives à l'installation du client Configuration Manager.

| NOM DU FICHIER JOURNAL | DESCRIPTION |
| --- | --- |
| ccmsetup.log | Enregistre les tâches de ccmsetup.exe liées au programme d'installation du client, à la mise à niveau du client et à la suppression de client. Permet de dépanner des problèmes d'installation du client. |
| ccmsetup-ccmeval.log | Enregistre les tâches de ccmsetup.exe liées à l'état et à la correction du client. |
| CcmRepair.log | Enregistre les activités de réparation de l'agent du client. |
| client.msi.log | Enregistre les tâches d'installation exécutées par client.msi. Permet de dépanner les problèmes d'installation ou de suppression du client. |

### Client pour Linux et UNIX

Le client Configuration Manager pour Linux et UNIX enregistre les informations dans les fichiers journaux suivants :

> **TIP**
> Utilisez CMTrace pour afficher les fichiers journaux du client pour Linux et UNIX.

> **NOTE**
> Lorsque vous utilisez la version initiale du client pour Linux et UNIX et faites référence à la documentation de cette section, remplacez les références suivantes pour chaque fichier ou processus :
>
> - Remplacez **omiserver.bin** par **nwserver.bin**
>   - Remplacez **omi** par **nanowbem**

| NOM DU FICHIER JOURNAL | DÉTAILS |
| --- | --- |

| NOM DU FICHIER JOURNAL | DÉTAILS |
| --- | --- |
| Scxcm.log | Fichier journal pour le service principal du client Configuration Manager pour Linux et UNIX (ccmexec.bin). Ce fichier journal contient des informations liées à l'installation et aux opérations en cours de ccmexec.bin.<br><br>Par défaut, ce fichier journal se trouve dans **/var/opt/microsoft/scxcm.log**<br><br>Pour définir un autre emplacement pour le fichier journal, modifiez **/opt/microsoft/configmgr/etc/scxcm.conf** et changez le champ **PATH** . Il n'est pas nécessaire de redémarrer l'ordinateur ou le service client pour appliquer la modification.<br><br>Vous pouvez définir le niveau de journalisation sur quatre valeurs différentes. |
| Scxcmprovider.log | Fichier journal pour le service CIM du client Configuration Manager pour Linux et UNIX (omiserver.bin). Ce fichier journal contient les informations liées aux opérations en cours de nwserver.bin.<br><br>Ce fichier journal se trouve dans **/var/opt/microsoft/configmgr/scxcmprovider.log**<br><br>Pour définir un autre emplacement pour le fichier journal, modifiez **/opt/microsoft/omi/etc/scxcmprovider.conf** et changez le champ **PATH** . Il n'est pas nécessaire de redémarrer l'ordinateur ou le service client pour appliquer la modification.<br><br>Vous pouvez définir le niveau de journalisation sur trois valeurs différentes. |

Les deux fichiers journaux prennent en charge plusieurs niveaux de journalisation :

- **scxcm.log**. Pour changer le niveau de journalisation, ouvrez **/opt/microsoft/configmgr/etc/scxcm.conf** et changez chaque instance de l'étiquette **MODULE** pour le niveau de journalisation souhaité :
  - ERROR : indique des problèmes nécessitant votre attention.
  - WARNING : indique des problèmes possibles pour les opérations du client.
  - INFO : une journalisation plus détaillée indiquant l'état de différents événements sur le client.
  - TRACE : une journalisation détaillée généralement utilisée pour diagnostiquer les problèmes.
- **scxcmprovider.log**. Pour définir un autre niveau de journal, modifiez **/opt/microsoft/omi/etc/scxcmprovider.conf** et changez chaque instance de la balise **MODULE** au niveau de journal souhaité :
  - ERROR : indique des problèmes nécessitant votre attention.
  - WARNING : indique des problèmes possibles pour les opérations du client.
  - INFO : une journalisation plus détaillée indiquant l'état de différents événements sur le client.

Dans des conditions de fonctionnement normales, utilisez le niveau de journalisation ERROR. Ce niveau de journalisation crée le fichier journal le plus petit. Au fil de l'augmentation du niveau de journalisation d'ERROR à WARNING, à INFO, puis à TRACE, un fichier journal à chaque fois plus volumineux est créé car plus de données

sont écrites dans le fichier journal.

#### Gérer les fichiers journaux du client Linux et UNIX

Le client pour Linux et UNIX ne limite pas la taille maximale des fichiers journaux du client. Il ne copie pas non plus automatiquement le contenu de ses fichiers .log dans un autre fichier, comme un fichier .lo_. Si vous voulez contrôler la taille maximale des fichiers journaux, implémentez un processus pour gérer les fichiers journaux indépendamment du client Configuration Manager pour Linux et UNIX.

Par exemple, vous pouvez utiliser la commande Linux et UNIX standard **logrotate** pour gérer la taille et la rotation des fichiers journaux du client. Le client Configuration Manager pour Linux et UNIX a une interface qui permet à **logrotate** de signaler au client le moment où la rotation des journaux est terminée. Le client peut ainsi reprendre la journalisation dans le fichier journal.

Pour plus d'informations sur **logrotate**, consultez la documentation des distributions Linux et UNIX que vous utilisez.

### Client pour ordinateurs Mac

Le client Configuration Manager pour les ordinateurs Mac enregistre les informations dans les fichiers journaux suivants :

| NOM DU FICHIER JOURNAL | DÉTAILS |
|---|---|
| CCMClient-<*date_heure*>.log | Enregistre les activités liées aux opérations du client Mac, notamment la gestion des applications, l'inventaire et la journalisation des erreurs.<br><br>Ce fichier journal se trouve dans le dossier /Library/Application Support/Microsoft/CCM/Logs sur l'ordinateur Mac. |
| CCMAgent-<*date_heure*>.log | Enregistre les informations liées aux opérations du client, notamment les opérations d'ouverture et de fermeture de session utilisateur et l'activité de l'ordinateurs Mac.<br><br>Ce fichier journal se trouve dans le dossier ~/Library/Logs sur l'ordinateur Mac. |
| CCMNotifications-<*date_heure*>.log | Enregistre les activités liées aux notifications Configuration Manage affichées sur l'ordinateur Mac.<br><br>Ce fichier journal se trouve dans le dossier ~/Library/Logs sur l'ordinateur Mac. |
| CCMPrefPane-<*date_heure*>.log | Enregistre les activités liées à la boîte de dialogue Préférences de Configuration Manager sur l'ordinateur Mac, ce qui inclut l'état général et la journalisation des erreurs.<br><br>Ce fichier journal se trouve dans le dossier ~/Library/Logs sur l'ordinateur Mac. |

Le fichier journal SMS_DM.log sur le serveur de système de site enregistre aussi les communications entre les ordinateurs Mac et le point de gestion configuré pour les appareils mobiles et les ordinateurs Mac.

## Fichiers journaux du serveur de site Configuration Manager

Les sections suivantes répertorient les fichiers journaux qui se trouvent sur le serveur de site ou qui sont liés à des rôles de système de site spécifiques.

### Journaux de serveur de site et de serveur de système de site

Le tableau suivant répertorie les fichiers journaux qui se trouvent sur le serveur de site et les serveurs de système de site Configuration Manager.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| adctrl.log | Enregistre les activités de traitement des inscriptions. | Serveur de site |
| ADForestDisc.log | Enregistre les actions de découverte de forêts Active Directory. | Serveur de site |
| ADService.log | Enregistre la création de compte et les détails des groupes de sécurité dans Active Directory. | Serveur de site |
| adsgdis.log | Enregistre les actions de découverte de groupe Active Directory. | Serveur de site |
| adsysdis.log | Enregistre les actions de découverte du système Active Directory. | Serveur de site |
| adusrdis.log | Enregistre les actions de découverte d'utilisateurs Active Directory. | Serveur de site |
| ccm.log | Enregistre les activités de l'installation poussée du client. | Serveur de site |
| CertMgr.log | Enregistre les activités de certificat pour la communication intra-site. | Serveur de système de site |
| chmgr.log | Enregistre les activités du gestionnaire d'intégrité du client. | Serveur de site |
| Cidm.log | Enregistre les modifications apportées aux paramètres du client par le Gestionnaire de données d'installation des clients (CIDM). | Serveur de site |
| colleval.log | Enregistre des détails concernant la création, la modification et la suppression de regroupements par l'Évaluateur de regroupements. | Serveur de site |
| compmon.log | Enregistre l'état des threads du composant surveillé pour le serveur de site. | Serveur de système de site |
| compsumm.log | Enregistre les tâches de l'Outil de synthèse d'état des composants. | Serveur de site |
| ComRegSetup.log | Enregistre l'installation initiale des résultats d'inscription COM d'un serveur de site. | Serveur de système de site |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| dataldr.log | Enregistre des informations sur le traitement des fichiers MIF et de l'inventaire matériel dans la base de données Configuration Manager. | Serveur de site |
| ddm.log | Enregistre les activités du gestionnaire de données de découverte. | Serveur de site |
| despool.log | Enregistre les transferts de communications entrantes de site à site. | Serveur de site |
| distmgr.log | Enregistre les détails concernant la création, la compression, la réplication delta et la mise à jour des informations des packages. | Serveur de site |
| EPCtrlMgr.log | Enregistre des informations concernant la synchronisation des informations sur les menaces de programmes malveillants à partir du serveur de rôle de système de site Endpoint Protection avec la base de données Configuration Manager. | Serveur de site |
| EPMgr.log | Enregistre l'état du rôle de système de site Endpoint Protection. | Serveur de système de site |
| EPSetup.log | Fournit des informations sur l'installation du rôle de système de site Endpoint Protection. | Serveur de système de site |
| EnrollSrv.log | Enregistre les activités du processus du service d'inscription. | Serveur de système de site |
| EnrollWeb.log | Enregistre les activités du processus du site Web d'inscription. | Serveur de système de site |
| fspmgr.log | Enregistre les activités du rôle de système de site d'un point d'état de secours. | Serveur de système de site |
| hman.log | Enregistre des informations sur les modifications de la configuration du site et sur la publication d'informations du site dans les services de domaine Active Directory. | Serveur de site |
| Inboxast.log | Enregistre les fichiers déplacés du point de gestion vers le dossier Boîtes de réception correspondant sur le serveur de site. | Serveur de site |
| inboxmgr.log | Enregistre les activités de transfert de fichier entre les dossiers des boîtes de réception. | Serveur de site |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| inboxmon.log | Enregistre le traitement des fichiers des boîtes de réception et des mises à jour du compteur de performances. | Serveur de site |
| invproc.log | Enregistre le transfert des fichiers MIF d'un site secondaire vers son site parent. | Serveur de site |
| migmctrl.log | Enregistre des informations sur les actions de migration qui impliquent des tâches de migration, des points de distribution partagés et des mises à niveau des points de distribution. | Site de plus haut niveau dans la hiérarchie Configuration Manager et chaque site principal enfant.<br><br>Dans une hiérarchie comportant plusieurs sites principaux, utilisez le fichier journal créé sur le site d'administration centrale. |
| mpcontrol.log | Enregistre l'inscription du point de gestion auprès de WINS (Windows Internet Name Service). Enregistre la disponibilité du point de gestion toutes les dix minutes. | Serveur de système de site |
| mpfdm.log | Enregistre les actions du composant du point de gestion qui déplace les fichiers du client vers le dossier Boîtes de réception correspondant sur le serveur de site. | Serveur de système de site |
| mpMSI.log | Enregistre des détails sur l'installation du point de gestion. | Serveur de site |
| MPSetup.log | Enregistre le processus de wrapper d'installation du point de gestion. | Serveur de site |
| netdisc.log | Enregistre les actions de découverte du réseau. | Serveur de site |
| ntsvrdis.log | Enregistre l'activité de découverte des serveurs de système de site. | Serveur de site |
| Objreplmgr | Enregistre le traitement des notifications de modification d'objet pour la réplication. | Serveur de site |
| offermgr.log | Enregistre les mises à jour des publications. | Serveur de site |
| offersum.log | Enregistre la synthèse des messages d'état du déploiement. | Serveur de site |
| OfflineServicingMgr.log | Enregistre les activités de mise à jour des fichiers d'image de systèmes d'exploitation. | Serveur de site |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| outboxmon.log | Enregistre le traitement des fichiers de la boîte d'envoi et des mises à jour du compteur de performances. | Serveur de site |
| PerfSetup.log | Enregistre les résultats de l'installation des compteurs de performance. | Serveur de système de site |
| PkgXferMgr.log | Enregistre les actions du composant SMS_Executive chargé de l'envoi de contenu d'un site principal vers un point de distribution distant. | Serveur de site |
| policypv.log | Enregistre les mises à jour des stratégies du client pour refléter les modifications apportées aux paramètres du client ou aux déploiements. | Serveur de site principal |
| rcmctrl.log | Enregistre les activités de réplication de la base de données entre les sites dans la hiérarchie. | Serveur de site |
| replmgr.log | Enregistre la réplication de fichiers entre les composants du serveur de site et le composant Planificateur. | Serveur de site |
| ResourceExplorer.log | Enregistre les erreurs, avertissements et informations liés à l'exécution de l'Explorateur de ressources. | Ordinateur qui exécute la console Configuration Manager |
| ruleengine.log | Enregistre des détails concernant les règles de déploiement automatique pour l'identification, le téléchargement de contenu et la création de groupe et de déploiement de mises à jour logicielles. | Serveur de site |
| schedule.log | Enregistre des détails concernant la réplication des travaux de site à site et de fichiers. | Serveur de site |
| Sender.log | Enregistre les fichiers qui sont transférés par réplication basée sur les fichiers entre les sites. | Serveur de site |
| sinvproc.log | Enregistre des informations sur le traitement des données d'inventaire logiciel vers la base de données de site. | Serveur de site |
| sitecomp.log | Enregistre des détails concernant la maintenance des composants du site installés sur tous les serveurs de système de site du site. | Serveur de site |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| sitectrl.log | Enregistre des modifications dans les paramètres du site apportées aux objets de contrôle de site dans la base de données. | Serveur de site |
| sitestat.log | Enregistre le processus de surveillance de la disponibilité et de l'espace disque de tous les systèmes de site. | Serveur de site |
| SMS_PhasedDeployment.log | Fichier journal pour les déploiements en plusieurs phases, une fonctionnalité en préversion à compter de Configuration Manager version 1802. | Site de niveau supérieur dans la hiérarchie Configuration Manager |
| SmsAdminUI.log | Enregistre l'activité de la console Configuration Manager. | Ordinateur qui exécute la console Configuration Manager |
| SMSAWEBSVCSetup.log | Enregistre les activités d'installation du service Web du catalogue des applications. | Serveur de système de site |
| smsbkup.log | Enregistre les résultats du processus de sauvegarde de site. | Serveur de site |
| smsdbmon.log | Enregistre les modifications de la base de données. | Serveur de site |
| SMSENROLLSRVSetup.log | Enregistre les activités d'installation du service Web d'inscription. | Serveur de système de site |
| SMSENROLLWEBSetup.log | Enregistre les activités d'installation du site Web d'inscription. | Serveur de système de site |
| smsexec.log | Enregistre le traitement de tous les threads du composant de serveur de site. | Serveur de site ou serveur de système de site |
| SMSFSPSetup.log | Enregistre les messages générés par l'installation d'un point d'état de secours. | Serveur de système de site |
| SMSPORTALWEBSetup.log | Enregistre les activités d'installation du site Web du catalogue des applications. | Serveur de système de site |
| SMSProv.log | Enregistre les accès du fournisseur WMI à la base de données du site. | Ordinateur sur lequel le fournisseur SMS est installé |
| srsrpMSI.log | Enregistre des résultats détaillés du processus d'installation du point de rapport à partir de la sortie MSI. | Serveur de système de site |
| srsrpsetup.log | Enregistre les résultats du processus d'installation du point de rapport. | Serveur de système de site |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| statesys.log | Enregistre le traitement des messages du système d'état. | Serveur de site |
| statmgr.log | Enregistre l'écriture de tous les messages d'état dans la base de données. | Serveur de site |
| swmproc.log | Enregistre le traitement des fichiers et des paramètres de contrôle. | Serveur de site |

### Fichiers journaux de l'installation du serveur de site

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations liées à l'installation du site.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| ConfigMgrPrereq.log | Enregistre les activités d'évaluation et d'installation des composants prérequis. | Serveur de site |
| ConfigMgrSetup.log | Enregistre les résultats détaillés de l'installation du serveur de site. | Serveur de site |
| ConfigMgrSetupWizard.log | Enregistre les informations liées à l'activité dans l'Assistant Installation. | Serveur de site |
| SMS_BOOTSTRAP.log | Enregistre des informations sur l'avancement du lancement du processus d'installation de site secondaire. Les détails du processus d'installation proprement dit sont donnés dans ConfigMgrSetup.log. | Serveur de site |
| smstsvc.log | Enregistre des informations sur l'installation, l'utilisation et la suppression d'un service Windows utilisé pour tester la connectivité du réseau et les autorisations entre les serveurs, en utilisant le compte d'ordinateur du serveur à l'origine de la connexion. | Serveur de site et serveur de système de site |

### Fichiers journaux du point de service de l'entrepôt de données

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations relatives au point de service de l'entrepôt de données.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| DWSSMSI.log | Enregistre les messages générés par l'installation d'un point de service de l'entrepôt de données. | Serveur de système de site |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| DWSSSetup.log | Enregistre les messages générés par l'installation d'un point de service de l'entrepôt de données. | Serveur de système de site |
| Microsoft.ConfigMgrDataWarehouse.log | Enregistre des informations sur la synchronisation des données entre la base de données de site et la base de données de l'entrepôt de données. | Serveur de système de site |

### Fichiers journaux du point d'état de secours

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations sur le point d'état de secours.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| FspIsapi | Enregistre des détails concernant les communications au point d'état de secours à partir de clients hérités d'appareils mobiles et d'ordinateurs clients. | Serveur de système de site |
| fspMSI.log | Enregistre les messages générés par l'installation d'un point d'état de secours. | Serveur de système de site |
| fspmgr.log | Enregistre les activités du rôle de système de site d'un point d'état de secours. | Serveur de système de site |

### Fichiers journaux du point de gestion

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations sur le point de gestion.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| CcmIsapi.log | Enregistre l'activité de la messagerie du client sur le point de terminaison. | Serveur de système de site |
| MP_CliReg.log | Enregistre l'activité de l'enregistrement du client traitée par le point de gestion. | Serveur de système de site |
| MP_Ddr.log | Enregistre la conversion d'enregistrements XML.ddr à partir des clients, puis les copie sur le serveur de site. | Serveur de système de site |
| MP_Framework.log | Enregistre les activités du point de gestion principal et des composants de l'infrastructure du client. | Serveur de système de site |
| MP_GetAuth.log | Enregistre les activités d'autorisation du client. | Serveur de système de site |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| MP_GetPolicy.log | Enregistre l'activité de demandes de stratégie des ordinateurs clients. | Serveur de système de site |
| MP_Hinv.log | Enregistre des détails concernant la conversion des enregistrements d'inventaire matériel XML à partir de clients ainsi que la copie de ces fichiers sur le serveur de site. | Serveur de système de site |
| MP_Location.log | Enregistre les demandes d'emplacement et les réponses données par les clients. | Serveur de système de site |
| MP_OOBMgr.log | Enregistre les activités du point de gestion liées à la réception d'un code secret à usage unique (OTP) de la part d'un client. | Serveur de système de site |
| MP_Policy.log | Enregistre la communication des stratégies. | Serveur de système de site |
| MP_Relay.log | Enregistre le transfert de fichiers qui sont collectés auprès du client. | Serveur de système de site |
| MP_Retry.log | Enregistre les processus des nouvelles tentatives d'inventaire matériel. | Serveur de système de site |
| MP_Sinv.log | Enregistre des détails concernant la conversion des enregistrements d'inventaire logiciel XML à partir de clients ainsi que la copie de ces fichiers sur le serveur de site. | Serveur de système de site |
| MP_SinvCollFile.log | Enregistre des détails concernant le regroupement de fichiers. | Serveur de système de site |
| MP_Status.log | Enregistre des détails concernant la conversion des fichiers de messages d'état XML.svf de clients et la copie de ces fichiers sur le serveur de site. | Serveur de système de site |
| mpcontrol.log | Enregistre l'inscription du point de gestion dans WINS. Enregistre la disponibilité du point de gestion toutes les dix minutes. | Serveur de site |
| mpfdm.log | Enregistre les actions du composant du point de gestion qui déplace les fichiers du client vers le dossier Boîtes de réception correspondant sur le serveur de site. | Serveur de système de site |
| mpMSI.log | Enregistre des détails sur l'installation du point de gestion. | Serveur de site |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| MPSetup.log | Enregistre le processus de wrapper d'installation du point de gestion. | Serveur de site |

### Fichiers journaux du point de mise à jour logicielle

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations relatives au point de mise à jour logicielle.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| objreplmgr.log | Enregistre les détails concernant la réplication des fichiers de notification de mises à jour logicielles, entre un site parent et des sites enfants. | Serveur de site |
| PatchDownloader.log | Enregistre des détails concernant le processus de téléchargement des mises à jour logicielles vers la destination de téléchargement, sur le serveur de site. | Ordinateur qui héberge la console Configuration Manager à partir de laquelle les téléchargements sont lancés |
| ruleengine.log | Enregistre des détails concernant les règles de déploiement automatique pour l'identification, le téléchargement de contenu et la création de groupe et de déploiement de mises à jour logicielles. | Serveur de site |
| SUPSetup.log | Enregistre des détails concernant l'installation du point de mise à jour logicielle. Lorsque l'installation d'un point de mise à jour logicielle se termine, la mention **Installation was successful** est consignée dans ce fichier journal. | Serveur de système de site |
| WCM.log | Enregistre les détails concernant la configuration du point de mise à jour logicielle et les connexions au serveur WSUS pour les catégories, les classifications et les langues des mises à jour souscrites. | Serveur de site qui se connecte au serveur WSUS |
| WSUSCtrl.log | Enregistre des détails concernant la configuration, la connectivité de la base de données et l'intégrité du serveur WSUS du site. | Serveur de système de site |
| wsyncmgr.log | Enregistre les détails concernant le processus de synchronisation des mises à jour logicielles. | Serveur de système de site |
| WUSSyncXML.log | Enregistre les détails concernant l'outil d'inventaire pour le processus de synchronisation de Microsoft Updates. | Ordinateur client configuré comme hôte de synchronisation pour l'outil d'inventaire de Microsoft Updates |

# Fichiers journaux pour les fonctionnalités de Configuration Manager

Les sections suivantes répertorient les fichiers journaux liés aux fonctions de Configuration Manager.

### Gestion des applications

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations liées à la gestion d'applications.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| AppIntentEval.log | Enregistre des détails concernant l'état actuel et prévu des applications, leur applicabilité, si les exigences ont été respectées, les types de déploiement et les dépendances. | Client |
| AppDiscovery.log | Enregistre les détails concernant la découverte ou la détection des applications sur les ordinateurs clients. | Client |
| AppEnforce.log | Enregistre des détails concernant les actions de mise en œuvre (installation et désinstallation) effectuées pour les applications sur le client. | Client |
| awebsctl.log | Enregistre les activités de surveillance du rôle de système de site du point de service web du catalogue d'applications. | Serveur de système de site |
| awebsvcMSI.log | Enregistre les informations d'installation détaillées sur le rôle du système de site du point de service Web du catalogue d'applications. | Serveur de système de site |
| CCMSDKProvider.log | Enregistre les activités de la gestion des applications SDK. | Client |
| colleval.log | Enregistre des détails concernant la création, la modification et la suppression de regroupements par l'Évaluateur de regroupements. | Serveur de système de site |
| ConfigMgrSoftwareCatalog.log | Enregistre l'activité du catalogue d'applications, dont l'utilisation de Silverlight. | Client |
| portlctl.log | Enregistre les activités de surveillance du rôle de système de site du point de site Web du catalogue d'applications. | Serveur de système de site |
| portlwebMSI.log | Enregistre l'activité d'installation MSI pour le rôle de site Web du catalogue d'applications. | Serveur de système de site |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| PrestageContent.log | Enregistre les détails concernant l'utilisation de l'outil ExtractContent.exe sur un point de distribution préparé distant. Cet outil extrait le contenu qui a été exporté vers un fichier. | Serveur de système de site |
| ServicePortalWebService.log | Enregistre l'activité du service Web du catalogue d'applications. | Serveur de système de site |
| ServicePortalWebSite.log | Enregistre l'activité du site Web du catalogue d'applications. | Serveur de système de site |
| SMSdpmon.log | Enregistre des détails concernant la tâche planifiée de surveillance de l'intégrité du point de distribution configurée sur un point de distribution. | Serveur de site |
| SoftwareCatalogUpdateEndpoint.log | Enregistre les activités de gestion de l'URL du catalogue d'applications indiquée dans le Centre logiciel. | Client |
| SoftwareCenterSystemTasks.log | Enregistre les activités liées à la validation des composants prérequis du Centre logiciel. | Client |

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations relatives au déploiement des packages et des programmes.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| colleval.log | Enregistre des détails concernant la création, la modification et la suppression de regroupements par l'Évaluateur de regroupements. | Serveur de site |
| execmgr.log | Enregistre des détails concernant les packages et les séquences de tâches qui s'exécutent. | Client |

### Asset Intelligence

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations relatives à Asset Intelligence.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| AssetAdvisor.log | Enregistre les activités des actions d'inventaire d'Asset Intelligence. | Client |
| aikbmgr.log | Enregistre des détails concernant le traitement des fichiers XML à partir de la boîte de réception, pour la mise à jour du catalogue Asset Intelligence. | Serveur de site |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| AIUpdateSvc.log | Enregistre l'interaction du point de synchronisation Asset Intelligence avec SCO (System Center Online), le service web en ligne. | Serveur de système de site |
| AIUSMSI.log | Enregistre les détails concernant l'installation du rôle de système de site du point de synchronisation Asset Intelligence. | Serveur de système de site |
| AIUSSetup.log | Enregistre les détails concernant l'installation du rôle de système de site du point de synchronisation Asset Intelligence. | Serveur de système de site |
| ManagedProvider.log | Enregistre des détails concernant la découverte de logiciels avec une balise d'identification logicielle associée. Enregistre également les activités liées à l'inventaire matériel. | Serveur de système de site |
| MVLSImport.log | Enregistre des détails concernant le traitement de fichiers de licence importés. | Serveur de système de site |

**Sauvegarde et récupération**

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations relatives aux actions de sauvegarde et de restauration, notamment la réinitialisation de site, et aux modifications apportées au fournisseur SMS.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| ConfigMgrSetup.log | Enregistre des informations sur les tâches d'installation et de restauration quand Configuration Manager restaure un site à partir d'une sauvegarde. | Serveur de site |
| smsbkup.log | Enregistre des détails concernant l'activité de sauvegarde du site. | Serveur de site |
| smssqlbkup.log | Enregistre les résultats du processus de sauvegarde de la base de données de site quand SQL Server est installé sur un serveur qui n'est pas le serveur de site. | Serveur de bases de données du site |
| Smswriter.log | Enregistre les informations sur l'état de l'enregistreur VSS Configuration Manager utilisé par le processus de sauvegarde. | Serveur de site |

**Inscription de certificats**

Le tableau suivant répertorie les fichiers journaux de Configuration Manager qui contiennent des informations relatives à l'inscription de certificats. L'inscription de certificats utilise le point d'inscription de certificats et le

module de stratégie de Configuration Manager sur le serveur qui exécute le service d'inscription de périphérique réseau.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| Crp.log | Enregistre les activités d'inscription. | Point d'enregistrement de certificat |
| Crpctrl.log | Enregistre le bon fonctionnement du point d'enregistrement de certificat. | Point d'enregistrement de certificat |
| Crpsetup.log | Enregistre des détails sur l'installation et la configuration du point d'enregistrement de certificat. | Point d'enregistrement de certificat |
| Crpmsi.log | Enregistre des détails sur l'installation et la configuration du point d'enregistrement de certificat. | Point d'enregistrement de certificat |
| NDESPlugin.log | Enregistre les activités de vérification des demandes d'accès et d'inscription des certificats. | Module de stratégie de Configuration Manager et service d'inscription d'appareils réseau |

En plus des fichiers journaux de Configuration Manager, consultez les journaux des applications Windows dans l'Observateur d'événements sur le serveur exécutant le service d'inscription d'appareils réseau et sur le serveur hébergeant le point d'enregistrement de certificat. Par exemple, recherchez des messages de la source **NetworkDeviceEnrollmentService** . Vous pouvez également utiliser les fichiers journaux suivants :

- Fichiers journaux IIS pour le service d'inscription d'appareils réseau : **<chemin>\inetpub\logs\LogFiles\W3SVC1**
- Fichiers journaux IIS pour le point d'inscription du certificat : **<chemin>\inetpub\logs\LogFiles\W3SVC1**
- Fichier journal de la stratégie d'inscription de périphérique réseau : **mscep.log**

> **NOTE**
> Ce fichier se trouve dans le dossier du profil de compte du service d'inscription de périphériques réseau, par exemple, dans C:\Users\SCEPSvc. Pour plus d'informations sur l'activation de la journalisation pour le service d'inscription de périphériques réseau, consultez la section Enable Logging (Activer la journalisation) dans l'article Network Device Enrollment Service (NDES) in Active Directory Certificate Services (AD CS) (Service d'inscription de périphériques réseau (NDES) dans les services de certificat Active Directory (AD CS)) sur le TechNet Wiki.

### Notification du client

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations liées à la notification du client.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| bgbmgr.log | Enregistre les détails concernant les activités du serveur de site liées aux tâches de notification du client et au traitement en ligne, ainsi qu'aux fichiers d'état des tâches. | Serveur de site |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| BGBServer.log | Enregistre les activités du serveur de notification, comme la communication client-serveur et l'envoi de tâches aux clients. Enregistre également les informations sur la génération de fichiers en ligne et de fichiers d'état de tâche à envoyer au serveur de site. | Point de gestion |
| BgbSetup.log | Enregistre les activités du processus de wrapper d'installation du serveur de notification lors de l'installation et de la désinstallation. | Point de gestion |
| bgbisapiMSI.log | Enregistre les détails concernant l'installation et la désinstallation du serveur de notification. | Point de gestion |
| BgbHttpProxy.log | Enregistre les activités du proxy HTTP de notification lors de la transmission des messages des clients via HTTP depuis et vers le serveur de notification. | Client |
| CCMNotificationAgent.log | Enregistre les activités de l'agent de notification, comme la communication client-serveur, et des informations concernant les tâches reçues et distribuées aux autres agents de client. | Client |

**Passerelle de gestion cloud**

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations liées à la passerelle de gestion cloud.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| CloudMgr.log | Enregistre les détails concernant le déploiement du service de passerelle de gestion cloud, l'état du service en cours et les données d'utilisation associées au service.<br>Vous pouvez configurer le niveau de journalisation en modifiant la valeur **Niveau de journalisation** dans la clé de Registre HKLM\SOFTWARE\ Microsoft\SMS\COMPONENTS\ SMS_CLOUD_ SERVICES_MANAGER | Le dossier *installdir* sur le serveur de site principal ou les autorités de certification. |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| CMGSetup.log[1] | Enregistre des détails concernant la deuxième phase du déploiement de la passerelle de gestion cloud (déploiement local dans Azure)<br>Vous pouvez configurer le niveau de journalisation à l'aide du paramètre **Niveau de suivi** (**Information** (par défaut), **Verbose**, **Error**) dans l'onglet de **configuration du portail Azure/services cloud**. | Le dossier **%approot%\logs** sur votre serveur Azure, ou le dossier SMS/Logs sur le serveur de système de site |
| CMGHttpHandler.log[1] | Enregistre des détails concernant la liaison du gestionnaire http de la passerelle de gestion cloud avec Internet Information Services dans Azure<br>Vous pouvez configurer le niveau de journalisation à l'aide du paramètre **Niveau de suivi** (**Information** (par défaut), **Verbose**, **Error**) dans l'onglet de **configuration du portail Azure/services cloud**. | Le dossier **%approot%\logs** sur votre serveur Azure, ou le dossier SMS/Logs sur le serveur de système de site |
| CMGService.log[1] | Enregistre des détails concernant le composant principal du service de passerelle de gestion cloud dans Azure<br>Vous pouvez configurer le niveau de journalisation à l'aide du paramètre **Niveau de suivi** (**Information** (par défaut), **Verbose**, **Error**) dans l'onglet de **configuration du portail Azure/services cloud**. | Le dossier **%approot%\logs** sur votre serveur Azure, ou le dossier SMS/Logs sur le serveur de système de site |
| SMS_Cloud_ ProxyConnector.log | Enregistre des détails sur la configuration des connexions entre le service de passerelle de gestion cloud et le point de connexion de passerelle de gestion cloud. | Serveur de système de site |

[1] Il s'agit des fichiers journaux Configuration Manager locaux que le gestionnaire de services cloud synchronise toutes les cinq minutes à partir du stockage Azure. La passerelle de gestion cloud transfère (par opération push) les journaux vers le stockage Azure toutes les 5 minutes. Le délai maximal est donc de 10 minutes. Les commutateurs Verbose affectent les journaux locaux et distants. Les noms des fichiers réels incluent le nom du service et l'identificateur de l'instance de rôle. Par exemple, CMG-*NomService*-*IDInstanceRôle*-CMGSetup.log

- Pour résoudre les problèmes de déploiement, utilisez **CloudMgr.log** et **CMGSetup.log**
- Pour la résolution des problèmes d'intégrité du service, utilisez **CMGService.log** et **SMS_Cloud_ProxyConnector.log**.
- Pour résoudre les problèmes de trafic client, utilisez **CMGHttpHandler.log**, **CMGService.log** et **SMS_Cloud_ProxyConnector.log**.

**Paramètres de conformité et accès aux ressources d'entreprise**

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations relatives aux paramètres de compatibilité et à l'accès aux ressources de l'entreprise.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| CIAgent.log | Enregistre des détails concernant le processus de correction et de compatibilité pour les paramètres de compatibilité, les mises à jour logicielles et la gestion d'applications. | Client |
| CITaskManager.log | Enregistre des informations sur la planification des tâches des éléments de configuration. | Client |
| DCMAgent.log | Enregistre les informations principales concernant l'évaluation, les rapports de conflit et la correction des éléments de configuration et des applications. | Client |
| DCMReporting.log | Enregistre des informations sur les rapports des résultats de la plateforme de stratégie sous forme de messages d'état pour les éléments de configuration. | Client |
| DcmWmiProvider.log | Enregistre des informations sur la lecture des synclets d'élément de configuration provenant de WMI. | Client |

### Accès conditionnel

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations relatives à l'accès conditionnel.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| ADALOperationProvider.log | Enregistre des détails concernant l'acquisition du jeton AAD. | Client |
| cloudusersync.log | Enregistre l'activation des licences des utilisateurs. | Ordinateur avec le point de connexion de service |
| ComplRelayAgent.log | Reçoit l'état de conformité global à partir de DCM, acquiert le jeton MP, acquiert le jeton AAD et transmet la conformité à Intune (le service de relais d'autorité de certification). | Client |
| DcmWmiProvider.log | Enregistre des informations sur la lecture des synclets d'élément de configuration provenant de WMI. | Client |
| dmpdownloader.log | Enregistre les détails concernant les téléchargements à partir de Microsoft Intune. | Ordinateur avec le point de connexion de service |
| dmpuploader.log | Enregistre les détails concernant le chargement des modifications de la base de données sur Microsoft Intune. | Ordinateur avec le point de connexion de service |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| MP_Token.log | Enregistre les demandes de jeton des clients. | Serveur de système de site |

### Console Configuration Manager

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations relatives à la console Configuration Manager.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| ConfigMgrAdminUISetup.log | Enregistre l'installation de la console Configuration Manager. | Ordinateur qui exécute la console Configuration Manager |
| SmsAdminUI.log | Enregistre des informations relatives au fonctionnement de la console Configuration Manager. | Ordinateur qui exécute la console Configuration Manager |
| SMSProv.log | Enregistre les activités effectuées par le fournisseur SMS. Les activités de la console Configuration Manager utilisent le fournisseur SMS. | Serveur de site ou serveur de système de site |

### Gestion de contenu

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations liées à la gestion de contenu.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| CloudDP-<guid>.log | Enregistre les détails d'un point de distribution cloud spécifique, y compris des informations sur le stockage et l'accès au contenu. | Serveur de système de site |
| CloudMgr.log | Enregistre les détails concernant l'approvisionnement du contenu, sur la collecte de statistiques de stockage et de bande passante, et sur les actions lancées par l'administrateur pour arrêter ou démarrer le service cloud qui exécute un point de distribution cloud. | Serveur de système de site |
| DataTransferService.log | Enregistre toutes les communications BITS relatives à l'accès aux stratégies ou aux packages. Ce journal est également utilisé pour la gestion de contenu par les points de distribution d'extraction. | Ordinateur configuré comme point de distribution d'extraction |
| PullDP.log | Enregistre des détails concernant le contenu que le point de distribution d'extraction transfère à partir de points de distribution source. | Ordinateur configuré comme point de distribution d'extraction |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| PrestageContent.log | Enregistre les détails concernant l'utilisation de l'outil ExtractContent.exe sur un point de distribution préparé distant. Cet outil extrait le contenu qui a été exporté vers un fichier. | Rôle de système de site |
| SMSdpmon.log | Enregistre les détails concernant les tâches planifiées de surveillance de l'intégrité du point de distribution configurées sur un point de distribution. | Rôle de système de site |
| smsdpprov.log | Enregistre des détails concernant l'extraction des fichiers compressés reçus à partir d'un site principal. Ce journal est généré par le fournisseur WMI du point de distribution distant. | Ordinateur de point de distribution n'est pas au même emplacement que le serveur de site |

### Découverte

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations liées à la détection.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| adsgdis.log | Enregistre les actions de la découverte du groupe de sécurité Active Directory. | Serveur de site |
| adsysdis.log | Enregistre les actions de découverte du système Active Directory. | Serveur de site |
| adusrdis.log | Enregistre les actions de découverte d'utilisateurs Active Directory. | Serveur de site |
| ADForestDisc.log | Enregistre les actions de découverte de forêts Active Directory. | Serveur de site |
| ddm.log | Enregistre les activités du gestionnaire de données de découverte. | Serveur de site |
| InventoryAgent.log | Enregistre les activités de l'inventaire matériel et logiciel et les actions de découverte par pulsations effectuées sur le client. | Client |
| netdisc.log | Enregistre les actions de découverte du réseau. | Serveur de site |

### Endpoint Protection

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations liées à Endpoint Protection.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| EndpointProtectionAgent.log | Enregistre des détails concernant l'installation du client Endpoint Protection et l'application de la stratégie anti-programme malveillant à ce client. | Client |
| EPCtrlMgr.log | Enregistre les détails concernant la synchronisation des informations sur les menaces de programmes malveillants à partir du serveur de rôle Endpoint Protection avec la base de données Configuration Manager. | Serveur de système de site |
| EPMgr.log | Surveille l'état du rôle de système de site Endpoint Protection. | Serveur de système de site |
| EPSetup.log | Fournit des informations sur l'installation du rôle de système de site Endpoint Protection. | Serveur de système de site |

### Extensions

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations liées aux extensions.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| AdminUI.ExtensionInstaller.log | Enregistre des informations sur le téléchargement des extensions de Microsoft et sur l'installation et la désinstallation de toutes les extensions. | Ordinateur qui exécute la console Configuration Manager |
| FeatureExtensionInstaller.log | Enregistre des informations sur l'installation et la suppression d'extensions individuelles quand elles sont activées ou désactivées dans la console Configuration Manager. | Ordinateur qui exécute la console Configuration Manager |
| SmsAdminUI.log | Enregistre l'activité de la console Configuration Manager. | Ordinateur qui exécute la console Configuration Manager |

### Inventaire

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations relatives au traitement des données d'inventaire.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| dataldr.log | Enregistre des informations sur le traitement des fichiers MIF et de l'inventaire matériel dans la base de données Configuration Manager. | Serveur de site |
| invproc.log | Enregistre le transfert des fichiers MIF d'un site secondaire vers son site parent. | Serveur de site secondaire |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| sinvproc.log | Enregistre des informations sur le traitement des données d'inventaire logiciel vers la base de données de site. | Serveur de site |

### Contrôle

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations liées au contrôle.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| mtrmgr.log | Surveille tous les processus de contrôle des logiciels. | Serveur de site |

### Migration

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations liées à la migration.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| migmctrl.log | Enregistre des informations sur les actions de migration qui impliquent des tâches de migration, des points de distribution partagés et des mises à niveau des points de distribution. | Site de plus haut niveau dans la hiérarchie Configuration Manager et chaque site principal enfant.<br><br>Dans une hiérarchie comportant des sites principaux multiples, utilisez le fichier journal créé sur le site d'administration centrale. |

### Appareils mobiles

Les sections suivantes répertorient les fichiers journaux qui contiennent des informations relatives à la gestion des appareils mobiles.

#### Inscription

Le tableau suivant répertorie les journaux qui contiennent des informations relatives à l'inscription d'appareils mobiles.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| DMPRP.log | Enregistre les communications entre les points de gestion activés pour les appareils mobiles et les points de terminaison du point de gestion. | Serveur de système de site |
| dmpmsi.log | Enregistre les données Windows Installer pour la configuration d'un point de gestion activé pour les appareils mobiles. | Serveur de système de site |
| DMPSetup.log | Enregistre la configuration du point de gestion lorsqu'il est activé pour les appareils mobiles. | Serveur de système de site |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| enrollsrvMSI.log | Enregistre les données Windows Installer pour la configuration d'un point d'inscription. | Serveur de système de site |
| enrollmentweb.log | Enregistre la communication entre les appareils mobiles et le point proxy d'inscription. | Serveur de système de site |
| enrollwebMSI.log | Enregistre les données Windows Installer pour la configuration d'un point proxy d'inscription. | Serveur de système de site |
| enrollmentservice.log | Enregistre la communication entre un point proxy d'inscription et un point d'inscription. | Serveur de système de site |
| SMS_DM.log | Enregistre les communications entre les appareils mobiles, les ordinateurs Mac et le point de gestion activé pour les appareils mobiles et les ordinateurs Mac. | Serveur de système de site |

**Connecteur Exchange Server**

Les journaux suivants contiennent des informations relatives au connecteur Exchange Server.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| easdisc.log | Enregistre les activités et l'état du connecteur Exchange Server. | Serveur de site |

**Client hérité d'appareil mobile**

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations relatives au client hérité de l'appareil mobile.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| DmCertEnroll.log | Enregistre des détails concernant l'inscription de certificats sur les clients hérités d'appareils mobiles. | Client |
| DMCertResp.htm | Enregistre la réponse HTML du serveur de certificats lorsque le programme d'inscription de client hérité d'appareil mobile demande un certificat PKI. | Client |
| DmClientHealth.log | Enregistre les GUID de tous les clients hérités des appareils mobiles qui communiquent avec le point de gestion activé pour les appareils mobiles. | Serveur de système de site |
| DmClientRegistration.log | Enregistre les demandes d'inscription et leurs réponses de et vers les clients hérités d'appareils mobiles. | Serveur de système de site |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| DmClientSetup.log | Enregistre les données d'installation du client pour les clients hérités d'appareils mobiles. | Client |
| DmClientXfer.log | Enregistre les données de transfert de client pour les clients hérités d'appareils mobiles et les déploiements ActiveSync. | Client |
| DmCommonInstaller.log | Enregistre l'installation des fichiers de transfert du client pour configurer les fichiers de transfert de clients hérités d'appareils mobiles. | Client |
| DmInstaller.log | Enregistre si DMInstaller appelle DmClientSetup correctement et si DmClientSetup se termine avec ou sans erreur pour les clients hérités d'appareils mobiles. | Client |
| DmpDatastore.log | Enregistre toutes les connexions aux bases de données de site et les requêtes effectuées par le point de gestion activé pour les appareils mobiles. | Serveur de système de site |
| DmpDiscovery.log | Enregistre toutes les données de découverte provenant des clients hérités d'appareils mobiles sur le point de gestion activé pour les appareils mobiles. | Serveur de système de site |
| DmpHardware.log | Enregistre des données d'inventaire matériel provenant de clients hérités d'appareils mobiles sur le point de gestion activé pour les appareils mobiles. | Serveur de système de site |
| DmpIsapi.log | Enregistre les communications du client hérité d'appareil mobile avec un point de gestion activé pour les appareils mobiles. | Serveur de système de site |
| dmpmsi.log | Enregistre les données Windows Installer pour la configuration d'un point de gestion activé pour les appareils mobiles. | Serveur de système de site |
| DMPSetup.log | Enregistre la configuration du point de gestion lorsqu'il est activé pour les appareils mobiles. | Serveur de système de site |
| DmpSoftware.log | Enregistre des données de la distribution logicielle provenant de clients hérités d'appareils mobiles sur un point de gestion activé pour les appareils mobiles. | Serveur de système de site |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| DmpStatus.log | Enregistre les données de messages d'état à partir de clients d'appareils mobiles sur un point de gestion activé pour les appareils mobiles. | Serveur de système de site |
| DmSvc.log | Enregistre les communications provenant de clients hérités d'appareils mobiles avec un point de gestion activé pour les appareils mobiles. | Client |
| FspIsapi.log | Enregistre des détails concernant les communications au point d'état de secours à partir de clients hérités d'appareils mobiles et d'ordinateurs clients. | Serveur de système de site |

**Déploiement du système d'exploitation**

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations relatives au déploiement du système d'exploitation.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| CAS.log | Enregistre des détails lorsque des points de distribution sont trouvés pour le contenu référencé. | Client |
| ccmsetup.log | Enregistre les tâches ccmsetup liées au programme d'installation client, à la mise à niveau du client et à la suppression de client. Permet de dépanner des problèmes d'installation du client. | Client |
| CreateTSMedia.log | Enregistre les détails sur la création de médias de séquence de tâches. | Ordinateur qui exécute la console Configuration Manager |
| DeployToVhd.log | Enregistre les détails concernant le processus de création et de modification de disque dur virtuel. | Ordinateur qui exécute la console Configuration Manager |
| Dism.log | Enregistre les actions d'installation de pilotes ou les actions d'application de mises à jour pour la maintenance hors connexion. | Serveur de système de site |
| distmgr.log | Enregistre les détails concernant la configuration de l'activation d'un point de distribution pour PXE (Preboot Execution Environment). | Serveur de système de site |
| DriverCatalog.log | Enregistre des détails concernant les pilotes de périphérique importés dans le catalogue de pilotes. | Serveur de système de site |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| mcsisapi.log | Enregistre les informations pour les transferts de packages en multidiffusion et les réponses aux demandes des clients. | Serveur de système de site |
| mcsexec.log | Enregistre les actions relatives au contrôle de l'intégrité, à l'espace de noms, à la création de sessions et à la vérification des certificats. | Serveur de système de site |
| mcsmgr.log | Enregistre les modifications apportées à la configuration, au mode de sécurité et à la disponibilité. | Serveur de système de site |
| mcsprv.log | Enregistre l'interaction du fournisseur de multidiffusion avec les services de déploiement Windows (WDS). | Serveur de système de site |
| MCSSetup.log | Enregistre des détails concernant l'installation du rôle de serveur de multidiffusion. | Serveur de système de site |
| MCSMSI.log | Enregistre des détails concernant l'installation du rôle de serveur de multidiffusion. | Serveur de système de site |
| Mcsperf.log | Enregistre des détails concernant les mises à jour du compteur de performance de multidiffusion. | Serveur de système de site |
| MP_ClientIDManager.log | Enregistre les réponses du point de gestion aux demandes d'ID client que les séquences de tâches lancent à partir de PXE ou du support de démarrage. | Serveur de système de site |
| MP_DriverManager.log | Enregistre les réponses du point de gestion aux demandes d'actions de la séquence de tâches Appliquer automatiquement les pilotes. | Serveur de système de site |
| OfflineServicingMgr.log | Enregistre les détails de la planification de la maintenance hors connexion et des actions d'application de mises à jour sur les fichiers WIM. | Serveur de système de site |
| Setupact.log | Enregistre des détails sur Windows Sysprep et les journaux d'installation. | Client |
| Setupapi.log | Enregistre des détails sur Windows Sysprep et les journaux d'installation. | Client |
| Setuperr.log | Enregistre des détails sur Windows Sysprep et les journaux d'installation. | Client |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| smpisapi.log | Enregistre des détails concernant les actions de capture de l'état du client et de restauration, et les informations de seuil. | Client |
| Smpmgr.log | Enregistre des détails concernant les résultats des modifications de configuration et des vérifications de l'intégrité du point de migration de l'état. | Serveur de système de site |
| smpmsi.log | Enregistre les détails d'installation et de configuration du point de migration d'état. | Serveur de système de site |
| smpperf.log | Enregistre les mises à jour du compteur de performances du point de migration d'état. | Serveur de système de site |
| smspxe.log | Enregistre les détails concernant les réponses aux clients qui effectuent un démarrage PXE et les détails concernant l'expansion d'images de démarrage et des fichiers de démarrage. | Serveur de système de site |
| smssmpsetup.log | Enregistre les détails d'installation et de configuration du point de migration d'état. | Serveur de système de site |
| SMS_PhasedDeployment.log | Fichier journal pour les déploiements en plusieurs phases, une fonctionnalité en préversion à compter de Configuration Manager version 1802. | Site de niveau supérieur dans la hiérarchie Configuration Manager |
| Smsts.log | Enregistre les activités de séquences de tâches. | Client |
| TSAgent.log | Enregistre le résultat des dépendances des séquences de tâche avant de démarrer une séquence de tâches. | Client |
| TaskSequenceProvider.log | Enregistre des détails concernant les séquences de tâches importées, exportées ou modifiées. | Serveur de système de site |
| loadstate.log | Enregistre des détails concernant l'outil de migration de l'état utilisateur (USMT) et la restauration des données d'état de l'utilisateur. | Client |
| scanstate.log | Enregistre des détails concernant l'outil de migration de l'état utilisateur (USMT) et la capture des données d'état de l'utilisateur. | Client |

**Gestion de l'alimentation**

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations liées à la gestion de l'alimentation.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| Pwrmgmt.log | Enregistre les détails concernant les activités de gestion de l'alimentation sur l'ordinateur client, notamment la surveillance et l'application de paramètres par l'agent du client de gestion de l'alimentation. | Client |

### Contrôle à distance

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations relatives au contrôle à distance.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| CMRcViewer.log | Enregistre des détails concernant l'activité de l'observateur de contrôle à distance. | Sur l'ordinateur qui exécute l'observateur de contrôle à distance, dans le dossier %temp%. |

### Rapports

Le tableau suivant répertorie les fichiers journaux de Configuration Manager qui contiennent des informations relatives à la création de rapports.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| srsrp.log | Enregistre des informations sur l'activité et l'état du point de Reporting Services. | Serveur de système de site |
| srsrpMSI.log | Enregistre les résultats détaillés du processus d'installation du point de Reporting Services à partir des données fournies par MSI. | Serveur de système de site |
| srsrpsetup.log | Enregistre les résultats du processus d'installation du point de Reporting Services. | Serveur de système de site |

### Administration basée sur des rôles

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations relatives à la gestion de l'administration basée sur des rôles.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| hman.log | Enregistre les informations concernant les modifications de la configuration du site et la publication d'informations du site sur les services de domaine Active Directory. | Serveur de site |
| SMSProv.log | Enregistre les accès du fournisseur WMI à la base de données du site. | Ordinateur sur lequel le fournisseur SMS est installé |

### Point de connexion de service

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations relatives au point de connexion de service.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| CertMgr.log | Enregistre des informations concernant les certificats et le compte proxy. | Serveur de site |
| Colleval.log | Enregistre des détails concernant la création, la modification et la suppression de regroupements par l'Évaluateur de regroupements. | Site principal et site d'administration centrale |
| Cloudusersync.log | Enregistre l'activation des licences des utilisateurs. | Ordinateur avec le point de connexion de service |
| dataldr.log | Enregistre des informations sur le traitement des fichiers MIF. | Serveur de site |
| ddm.log | Enregistre les activités du gestionnaire de données de découverte. | Serveur de site |
| distmgr.log | Enregistre des détails concernant les requêtes de distribution de contenu. | Serveur de site de niveau supérieur |
| Dmpdownloader.log | Enregistre les détails concernant les téléchargements à partir de Microsoft Intune. | Ordinateur avec le point de connexion de service |
| Dmpuploader.log | Enregistre les détails concernant le chargement des modifications de la base de données sur Microsoft Intune. | Ordinateur avec le point de connexion de service |
| hman.log | Enregistre des informations concernant le transfert des messages. | Serveur de site |
| objreplmgr.log | Enregistre le traitement des stratégies et des affectations. | Serveur de site principal |
| Policypv.log | Enregistre la génération de stratégie de toutes les stratégies. | Serveur de site |
| outgoingcontentmanager.log | Enregistre le contenu chargé vers Microsoft Intune. | Ordinateur avec le point de connexion de service |
| sitecomp.log | Enregistre les détails de l'installation du point de connexion de service. | Serveur de site |
| SmsAdminUI.log | Enregistre l'activité de la console Configuration Manager. | Ordinateur qui exécute la console Configuration Manager |
| SMSProv.log | Enregistre les activités effectuées par le fournisseur SMS. Les activités de la console Configuration Manager utilisent le fournisseur SMS. | Ordinateur sur lequel le fournisseur SMS est installé |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| SrvBoot.log | Enregistre les détails du service d'installation du point de connexion de service. | Ordinateur avec le point de connexion de service |
| Statesys.log | Enregistre le traitement des messages de gestion d'appareil mobile. | Site principal et site d'administration centrale |

### Mises à jour logicielles

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations relatives aux mises à jour logicielles.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| Ccmperf.log | Enregistre les activités liées à la maintenance et la capture de données relatives aux compteurs de performances du client. | Client |
| PatchDownloader.log | Enregistre des détails concernant le processus de téléchargement des mises à jour logicielles vers la destination de téléchargement, sur le serveur de site. | Ordinateur qui héberge la console Configuration Manager à partir de laquelle les téléchargements sont lancés |
| PolicyEvaluator.log | Enregistre des détails concernant l'évaluation des stratégies sur les ordinateurs clients, dont les stratégies de mises à jour logicielles. | Client |
| RebootCoordinator.log | Enregistre des détails concernant la coordination des redémarrages du système sur des ordinateurs clients après l'installation de mises à jour logicielles. | Client |
| ScanAgent.log | Enregistre des détails concernant les demandes d'analyse pour les mises à jour logicielles, l'emplacement de WSUS et des actions connexes. | Client |
| SdmAgent.log | Enregistre les détails concernant le suivi des corrections et de la conformité. Cependant, le fichier journal des mises à jour logicielles, Updateshandler.log, fournit plus d'informations sur l'installation des mises à jour logicielles nécessaires pour la conformité.<br><br>Ce fichier journal est partagé avec les paramètres de compatibilité. | Client |
| ServiceWindowManager.log | Enregistre des détails concernant l'évaluation des fenêtres de maintenance. | Client |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| SmsWusHandler.log | Enregistre des détails concernant le processus d'analyse pour l'outil d'inventaire de Microsoft Updates. | Client |
| StateMessage.log | Enregistre les détails concernant les messages d'état des mises à jour logicielles qui sont créés et envoyés au point de gestion. | Client |
| SUPSetup.log | Enregistre des détails concernant l'installation du point de mise à jour logicielle. Lorsque l'installation d'un point de mise à jour logicielle se termine, la mention **Installation was successful** est consignée dans ce fichier journal. | Serveur de système de site |
| UpdatesDeployment.log | Enregistre des détails concernant les déploiements sur le client, y compris l'activation, l'évaluation et l'application des mises à jour logicielles. La journalisation documentée contient des informations supplémentaires sur l'interaction avec l'interface utilisateur du client. | Client |
| UpdatesHandler.log | Enregistre des détails concernant l'analyse de la compatibilité des mises à jour logicielles, ainsi que le téléchargement et l'installation des mises à jour logicielles sur le client. | Client |
| UpdatesStore.log | Enregistre des détails concernant l'état de compatibilité des mises à jour logicielles qui ont été évaluées au cours du cycle d'analyse de la compatibilité. | Client |
| WCM.log | Enregistre les détails concernant la configuration du point de mise à jour logicielle et les connexions au serveur WSUS pour les catégories, les classifications et les langues des mises à jour avec abonnement. | Serveur de site |
| WSUSCtrl.log | Enregistre des détails concernant la configuration, la connectivité de la base de données et l'intégrité du serveur WSUS du site. | Serveur de système de site |
| wsyncmgr.log | Enregistre les détails concernant le processus de synchronisation des mises à jour logicielles. | Serveur de site |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| WUAHandler.log | Enregistre des détails concernant l'agent Windows Update sur le client, lors de la recherche des mises à jour logicielles. | Client |

### Wake On LAN

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations relatives à l'utilisation de Wake On LAN.

> **NOTE**
>
> Quand vous complétez l'éveil par appel réseau (Wake On LAN) en utilisant le proxy de mise en éveil, cette activité est journalisée sur le client. Par exemple, consultez CcmExec.log et SleepAgent<*domaine*>*@SYSTEM_0.log dans la section Opérations du client de cet article.*

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| wolcmgr.log | Enregistre des détails concernant les clients auxquels des paquets de mise en éveil doivent être envoyés, le nombre de paquets de mise en éveil envoyés et le nombre de nouvelles tentatives. | Serveur de site |
| wolmgr.log | Enregistre des détails concernant les procédures de mise en éveil, notamment le moment opportun pour déclencher le réveil des déploiements configurés pour Wake On LAN. | Serveur de site |

### Maintenance de Windows 10

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations relatives à la maintenance de Windows 10.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| Ccmperf.log | Enregistre les activités liées à la maintenance et la capture de données relatives aux compteurs de performances du client. | Client |
| CcmRepair.log | Enregistre les activités de réparation de l'agent du client. | Client |
| PatchDownloader.log | Enregistre des détails concernant le processus de téléchargement des mises à jour logicielles vers la destination de téléchargement, sur le serveur de site. | Ordinateur qui héberge la console Configuration Manager à partir de laquelle les téléchargements sont lancés |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| PolicyEvaluator.log | Enregistre des détails concernant l'évaluation des stratégies sur les ordinateurs clients, dont les stratégies de mises à jour logicielles. | Client |
| RebootCoordinator.log | Enregistre des détails concernant la coordination des redémarrages du système sur des ordinateurs clients après l'installation de mises à jour logicielles. | Client |
| ScanAgent.log | Enregistre des détails concernant les demandes d'analyse pour les mises à jour logicielles, l'emplacement de WSUS et des actions connexes. | Client |
| SdmAgent.log | Enregistre les détails concernant le suivi des corrections et de la conformité. Cependant, le fichier journal des mises à jour logicielles, Updateshandler.log, fournit plus d'informations sur l'installation des mises à jour logicielles nécessaires pour la conformité.<br><br>Ce fichier journal est partagé avec les paramètres de compatibilité. | Client |
| ServiceWindowManager.log | Enregistre des détails concernant l'évaluation des fenêtres de maintenance. | Client |
| setupact.log | Fichier journal principal pour la plupart des erreurs qui se produisent pendant le processus d'installation de Windows. Le fichier journal se trouve dans le dossier %windir%$Windows.~BT\sources\panther. | Client |
| SmsWusHandler.log | Enregistre des détails concernant le processus d'analyse pour l'outil d'inventaire de Microsoft Updates. | Client |
| StateMessage.log | Enregistre des détails sur les messages d'état des mises à jour logicielles créés et envoyés au point de gestion. | Client |
| SUPSetup.log | Enregistre des détails concernant l'installation du point de mise à jour logicielle. Lorsque l'installation d'un point de mise à jour logicielle se termine, la mention **Installation was successful** est consignée dans ce fichier journal. | Serveur de système de site |

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| UpdatesDeployment.log | Enregistre des détails concernant les déploiements sur le client, y compris l'activation, l'évaluation et l'application des mises à jour logicielles. La journalisation documentée contient des informations supplémentaires sur l'interaction avec l'interface utilisateur du client. | Client |
| Updateshandler.log | Enregistre des détails concernant l'analyse de la compatibilité des mises à jour logicielles, ainsi que le téléchargement et l'installation des mises à jour logicielles sur le client. | Client |
| UpdatesStore.log | Enregistre des détails concernant l'état de compatibilité des mises à jour logicielles qui ont été évaluées au cours du cycle d'analyse de la compatibilité. | Client |
| WCM.log | Enregistre les détails concernant la configuration du point de mise à jour logicielle et les connexions au serveur WSUS pour les catégories, les classifications et les langues des mises à jour avec abonnement. | Serveur de site |
| WSUSCtrl.log | Enregistre des détails concernant la configuration, la connectivité de la base de données et l'intégrité du serveur WSUS du site. | Serveur de système de site |
| wsyncmgr.log | Enregistre les détails concernant le processus de synchronisation des mises à jour logicielles. | Serveur de site |
| WUAHandler.log | Enregistre des détails concernant l'agent Windows Update sur le client, lors de la recherche des mises à jour logicielles. | Client |

### Agent Windows Update

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations relatives à l'agent Windows Update.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| WindowsUpdate.log | Enregistre les détails concernant les connexions de l'agent Windows Update au serveur WSUS et la récupération des mises à jour logicielles pour l'évaluation de la conformité, et s'il existe des mises à jour pour les composants de l'agent. | Client |

### Serveur WSUS

Le tableau suivant répertorie les fichiers journaux qui contiennent des informations relatives au serveur WSUS.

| NOM DU FICHIER JOURNAL | DESCRIPTION | ORDINATEUR SUR LEQUEL SE TROUVE LE FICHIER JOURNAL |
|---|---|---|
| Change.log | Enregistre les détails concernant les informations de la base de données du serveur WSUS qui ont été modifiées. | Serveur WSUS |
| SoftwareDistribution.log | Enregistre les détails concernant les mises à jour logicielles qui sont synchronisées depuis la source de mise à jour configurée vers la base de données du serveur WSUS. | Serveur WSUS |

# Ports utilisés dans System Center Configuration Manager

09/05/2018 • 43 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

System Center Configuration Manager est un système client/serveur distribué. Du fait de la nature distribuée de Configuration Manager, il est possible d'établir des connexions entre les serveurs de site, les systèmes de site et les clients. Certaines connexions utilisent des ports qui ne sont pas configurables et certaines prennent en charge des ports personnalisés que vous spécifiez. Si vous utilisez des technologies de filtrage de port, par exemple, des pare-feu, des routeurs, des serveurs proxy ou IPsec, vérifiez que les ports requis sont disponibles.

> **NOTE**
> Si vous prenez en charge les clients Internet par pontage SSL, parallèlement aux exigences de port, vous devrez peut-être également autoriser certains verbes et en-têtes HTTP pour traverser le pare-feu.

Les listes de ports ci-après sont utilisées par Configuration Manager et ne comportent aucune information relative aux services Windows standard, tels que les paramètres Stratégie de groupe pour les services de domaine Active Directory ou l'authentification Kerberos. Pour plus d'informations sur les ports et les services de Windows Server, voir Vue d'ensemble des services et exigences du port réseau pour le système Windows Server.

## Ports configurables

Configuration Manager vous permet de configurer les ports pour les types de communication suivants :

- Point du site web du catalogue des applications vers point de service web du catalogue des applications
- Point proxy d'inscription vers point d'inscription
- Client vers systèmes de site exécutant IIS
- Client à Internet (sous forme de paramètres du serveur proxy)
- Point de mise à jour logicielle à Internet (sous forme de paramètres du serveur proxy)
- Point de mise à jour logicielle à serveur WSUS
- Serveur de site à serveur de base de données de site
- Points de Reporting Services

> **NOTE**
> Les ports qui sont utilisés pour le rôle de système de site du point de Reporting Services sont configurés dans SQL Server Reporting Services. Ces ports sont ensuite utilisés par Configuration Manager pendant les communications à destination du point de Reporting Services. Veillez à passer en revue les ports qui définissent les informations de filtre IP pour les stratégies IPsec ou pour la configuration des pare-feu.

Par défaut, le port HTTP utilisé pour la communication entre le client et le système de site est le port 80, et le port HTTPS par défaut est le port 443. Vous pouvez modifier les ports HTTP ou HTTPS de communication entre

le client et le système de site pendant l'installation ou dans les propriétés de votre site Configuration Manager.

Les ports qui sont utilisés pour le rôle de système de site du point de Reporting Services sont configurés dans SQL Server Reporting Services. Ces ports sont ensuite utilisés par Configuration Manager pendant les communications à destination du point de Reporting Services. Veillez à passer en revue ces ports quand vous définissez les informations de filtre IP pour les stratégies IPsec ou pour la configuration des pare-feu.

## Ports non configurables

Configuration Manager ne vous autorise pas à configurer des ports pour les types de communication suivants :

- Site à site
- Serveur de site à système de site
- Console Configuration Manager vers le fournisseur SMS
- Console Configuration Manager vers Internet
- Connexions aux services cloud tels que Microsoft Intune et les points de distribution cloud

## Ports utilisés par les clients Configuration Manager et les systèmes de site

Les sections suivantes détaillent les ports qui sont utilisés pour la communication dans Configuration Manager. Les flèches figurant dans les titres des sections indiquent le sens de la communication :

- -- > indique qu'un ordinateur initie la communication et que l'autre ordinateur répond toujours ;
- < -- > indique que les deux ordinateurs peuvent initier la communication.

**Point de synchronisation Asset Intelligence -- > Microsoft**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| HTTPS (Secure Hypertext Transfer Protocol) | -- | 443 |

**Point de synchronisation Asset Intelligence -- > SQL Server**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SQL sur TCP | -- | 1433 (voir note 2, **autre port disponible**) |

**Point de service Web du catalogue des applications -- > SQL Server**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SQL sur TCP | -- | 1433 (voir note 2, **Autre port disponible**) |

**Point du site Web du catalogue des applications -- > Point de service Web du catalogue des applications**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| HTTP (Hypertext Transfer Protocol) | -- | 80 (voir note 2, **Autre port disponible**) |

| DESCRIPTION | UDP | TCP |
| --- | --- | --- |
| HTTPS (Secure Hypertext Transfer Protocol) | -- | 443 (voir note 2, **Autre port disponible**) |

**Client -- > Point du site Web du catalogue des applications**

| DESCRIPTION | UDP | TCP |
| --- | --- | --- |
| HTTP (Hypertext Transfer Protocol) | -- | 80 (voir note 2, **Autre port disponible**) |
| HTTPS (Secure Hypertext Transfer Protocol) | -- | 443 (voir note 2, **Autre port disponible**) |

**Client -- > Client**

En plus des ports répertoriés dans le tableau ci-dessous, le proxy de mise en éveil utilise également des messages de demande d'écho ICMP (Internet Control Message Protocol) d'un client à un autre, lorsque ceux-ci sont configurés pour utiliser le proxy de mise en éveil.

Cette communication permet de savoir si l'autre ordinateur client est en éveil sur le réseau. ICMP est parfois appelé commandes ping TCP/IP. ICMP ne disposant pas d'un numéro de protocole UDP ou TCP, il ne figure pas dans le tableau ci-dessous. Toutefois, les pare-feu d'hôte de ces ordinateurs clients ou les appareils réseau intervenant sur le sous-réseau doivent autoriser le trafic ICMP pour que la communication avec le proxy de mise en éveil aboutisse.

| DESCRIPTION | UDP | TCP |
| --- | --- | --- |
| Éveil par appel réseau | 9 (voir note 2, **Autre port disponible**) | -- |
| Proxy de mise en éveil | 25536 (voir note 2, **Autre port disponible**) | -- |

**Client --> Module de stratégie de Configuration Manager (service d'inscription d'appareils réseau)**

| DESCRIPTION | UDP | TCP |
| --- | --- | --- |
| HTTP (Hypertext Transfer Protocol) | | 80 |
| HTTPS (Secure Hypertext Transfer Protocol) | -- | 443 |

**Client -- > Point de distribution cloud**

| DESCRIPTION | UDP | TCP |
| --- | --- | --- |
| HTTPS (Secure Hypertext Transfer Protocol) | -- | 443 |

**Client -- > Point de distribution**

| DESCRIPTION | UDP | TCP |
| --- | --- | --- |

| DESCRIPTION | UDP | TCP |
| --- | --- | --- |
| HTTP (Hypertext Transfer Protocol) | -- | 80 (voir note 2, **Autre port disponible**) |
| HTTPS (Secure Hypertext Transfer Protocol) | -- | 443 (voir note 2, **Autre port disponible**) |

### Client -- > Point de distribution configuré pour la multidiffusion

| DESCRIPTION | UDP | TCP |
| --- | --- | --- |
| SMB (Server Message Block) | -- | 445 |
| Protocole de multidiffusion | 63000-64000 | -- |

### Client -- > Point de distribution configuré pour PXE

| DESCRIPTION | UDP | TCP |
| --- | --- | --- |
| DHCP (Dynamic Host Configuration Protocol) | 67 et 68 | -- |
| TFTP (Trivial File Transfer Protocol) | 69 (voir note 4, **Service Trivial FTP (TFTP)**) | -- |
| BINL (Boot Information Negotiation Layer) | 4011 | -- |

### Client -- > Point d'état de secours

| DESCRIPTION | UDP | TCP |
| --- | --- | --- |
| HTTP (Hypertext Transfer Protocol) | -- | 80 (voir note 2, **Autre port disponible**) |

### Client -- > Contrôleur de domaine de catalogue global

Un client Configuration Manager ne contacte pas de serveur de catalogue global lorsqu'il s'agit d'un ordinateur d'un groupe de travail ou lorsqu'il est configuré pour les communications Internet uniquement.

| DESCRIPTION | UDP | TCP |
| --- | --- | --- |
| LDAP de catalogue global | -- | 3268 |

### Client -- > Point de gestion

| DESCRIPTION | UDP | TCP |
| --- | --- | --- |
| Notification du client (communication par défaut avant le basculement en HTTP ou HTTPS) | -- | 10123 (voir note 2, **Autre port disponible**) |
| HTTP (Hypertext Transfer Protocol) | -- | 80 (voir note 2, **Autre port disponible**) |

| DESCRIPTION | UDP | TCP |
| --- | --- | --- |
| HTTPS (Secure Hypertext Transfer Protocol) | -- | 443 (voir note 2, **Autre port disponible**) |

**Client -- > Point de mise à jour logicielle**

| DESCRIPTION | UDP | TCP |
| --- | --- | --- |
| HTTP (Hypertext Transfer Protocol) | -- | 80 ou 8530 (Voir la remarque 3, **Windows Server Update Services**) |
| HTTPS (Secure Hypertext Transfer Protocol) | -- | 443 ou 8531 (Voir la remarque 3, **Windows Server Update Services**) |

**Client -- > Point de migration d'état**

| DESCRIPTION | UDP | TCP |
| --- | --- | --- |
| HTTP (Hypertext Transfer Protocol) | -- | 80 (voir note 2, **Autre port disponible**) |
| HTTPS (Secure Hypertext Transfer Protocol) | -- | 443 (voir note 2, **Autre port disponible**) |
| SMB (Server Message Block) | -- | 445 |

**Console Configuration Manager -- > Client**

| DESCRIPTION | UDP | TCP |
| --- | --- | --- |
| Contrôle à distance (contrôle) | -- | 2701 |
| Assistance à distance (RDP et RTC) | -- | 3389 |

**Console Configuration Manager -- > Internet**

| DESCRIPTION | UDP | TCP |
| --- | --- | --- |
| HTTP (Hypertext Transfer Protocol) | -- | 80 |
| HTTPS (Secure Hypertext Transfer Protocol) | -- | 443 |

La console de Configuration Manager utilise l'accès à Internet pour les éléments suivants :

- le téléchargement des mises à jour de logiciels à partir de Microsoft Update pour les packages de déploiement ;
- l'élément Commentaires dans le ruban ;
- les liens vers la documentation dans la console.

**Console Configuration Manager -- > Point de Reporting Services**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| HTTP (Hypertext Transfer Protocol) | -- | 80 (voir note 2, **Autre port disponible**) |
| HTTPS (Secure Hypertext Transfer Protocol) | -- | 443 (voir note 2, **Autre port disponible**) |

**Console Configuration Manager -- > Serveur de site**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| RPC (connexion initiale à WMI pour localiser le système fournisseur) | -- | 135 |

**Console Configuration Manager -- > Fournisseur SMS**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| Mappeur de point de terminaison RPC | 135 | 135 |
| RPC | -- | DYNAMIQUE (voir la note 6, **Ports dynamiques**) |

**Module de stratégie de Configuration Manager (service d'inscription de périphériques réseau) -- > Point d'enregistrement de certificat**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| HTTPS (Secure Hypertext Transfer Protocol) | -- | 443 (voir note 2, **Autre port disponible**) |

**Point de distribution -- > Point de gestion**

Un point de distribution communique avec le point de gestion dans les scénarios suivants :

- Pour signaler l'état du contenu préparé
- Pour signaler les données de synthèse d'utilisation
- Pour signaler la validation du contenu
- Pour signaler l'état des téléchargements de packages (point de distribution d'extraction)

| DESCRIPTION | UDP | TCP |
|---|---|---|
| HTTP (Hypertext Transfer Protocol) | -- | 80 (voir note 2, **Autre port disponible**) |
| HTTPS (Secure Hypertext Transfer Protocol) | -- | 443 (voir note 2, **Autre port disponible**) |

**Point Endpoint Protection -- > Internet**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| HTTP (Hypertext Transfer Protocol) | -- | 80 |

### Point Endpoint Protection -- > SQL Server

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SQL sur TCP | -- | 1433 (voir note 2, **Autre port disponible**) |

### Point proxy d'inscription -- > Point d'inscription

| DESCRIPTION | UDP | TCP |
|---|---|---|
| HTTPS (Secure Hypertext Transfer Protocol) | -- | 443 (voir note 2, **Autre port disponible**) |

### Point d'inscription -- > SQL Server

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SQL sur TCP | -- | 1433 (voir note 2, **Autre port disponible**) |

### Connecteur du serveur Exchange Server -- > Exchange Online

| DESCRIPTION | UDP | TCP |
|---|---|---|
| Gestion à distance de Windows via HTTPS | -- | 5986 |

### Connecteur du serveur Exchange Server -- > Serveur Exchange Server local

| DESCRIPTION | UDP | TCP |
|---|---|---|
| Gestion à distance de Windows via HTTP | -- | 5985 |

### Ordinateur Mac -- > Point proxy d'inscription

| DESCRIPTION | UDP | TCP |
|---|---|---|
| HTTPS (Secure Hypertext Transfer Protocol) | -- | 443 |

### Point de gestion -- > Contrôleur de domaine

| DESCRIPTION | UDP | TCP |
|---|---|---|
| LDAP (Lightweight Directory Access Protocol) | -- | 389 |
| LDAP de catalogue global | -- | 3268 |
| Mappeur de point de terminaison RPC | 135 | 135 |
| RPC | -- | DYNAMIQUE (voir la note 6, **Ports dynamiques**) |

**Point de gestion < -- > Serveur de site**

(Voir remarque 5, **Communications entre le serveur de site et les systèmes de site**)

| DESCRIPTION | UDP | TCP |
|---|---|---|
| Mappeur de point de terminaison RPC | -- | 135 |
| RPC | -- | DYNAMIQUE (voir la note 6, **Ports dynamiques**) |
| SMB (Server Message Block) | -- | 445 |

**Point de gestion -- > SQL Server**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SQL sur TCP | -- | 1433 (voir note 2, **Autre port disponible**) |

**Appareil mobile -- > Point proxy d'inscription**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| HTTPS (Secure Hypertext Transfer Protocol) | -- | 443 |

**Appareil mobile -- > Microsoft Intune**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| HTTPS (Secure Hypertext Transfer Protocol) | -- | 443 |

**Point de Reporting Services -- > SQL Server**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SQL sur TCP | -- | 1433 (voir note 2, **Autre port disponible**) |

**Point de connexion de service -- > Microsoft Intune**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| HTTPS (Secure Hypertext Transfer Protocol) | -- | 443 |

Pour plus d'informations, consultez la section Conditions requises pour l'accès à Internet du point de connexion de service.

**Serveur de site < -- > Point de service Web du catalogue des applications**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SMB (Server Message Block) | -- | 445 |

| DESCRIPTION | UDP | TCP |
|---|---|---|
| Mappeur de point de terminaison RPC | 135 | 135 |
| RPC | -- | DYNAMIQUE (voir la note 6, **Ports dynamiques**) |

**Serveur de site < -- > Point du site Web du catalogue des applications**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SMB (Server Message Block) | -- | 445 |
| Mappeur de point de terminaison RPC | 135 | 135 |
| RPC | -- | DYNAMIQUE (voir la note 6, **Ports dynamiques**) |

**Serveur de site < -- > Point de synchronisation Asset Intelligence**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SMB (Server Message Block) | -- | 445 |
| Mappeur de point de terminaison RPC | 135 | 135 |
| RPC | -- | DYNAMIQUE (voir la note 6, **Ports dynamiques**) |

**Serveur de site -- > Client**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| Éveil par appel réseau | 9 (voir note 2, **Autre port disponible**) | -- |

**Serveur de site -- > Point de distribution cloud**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| HTTPS (Secure Hypertext Transfer Protocol) | -- | 443 |

**Serveur de site -- > Point de distribution**

(Voir remarque 5, **Communications entre le serveur de site et les systèmes de site**)

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SMB (Server Message Block) | -- | 445 |
| Mappeur de point de terminaison RPC | 135 | 135 |
| RPC | -- | DYNAMIQUE (voir la note 6, **Ports dynamiques**) |

### Serveur de site -- > Contrôleur de domaine

| DESCRIPTION | UDP | TCP |
|---|---|---|
| LDAP (Lightweight Directory Access Protocol) | -- | 389 |
| LDAP de catalogue global | -- | 3268 |
| Mappeur de point de terminaison RPC | 135 | 135 |
| RPC | -- | DYNAMIQUE (voir la note 6, **Ports dynamiques**) |

### Serveur de site < -- > Point d'enregistrement de certificat

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SMB (Server Message Block) | -- | 445 |
| Mappeur de point de terminaison RPC | 135 | 135 |
| RPC | -- | DYNAMIQUE (voir la note 6, **Ports dynamiques**) |

### Serveur de site < -- > Point Endpoint Protection

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SMB (Server Message Block) | -- | 445 |
| Mappeur de point de terminaison RPC | 135 | 135 |
| RPC | -- | DYNAMIQUE (voir la note 6, **Ports dynamiques**) |

### Serveur de site < -- > Point d'inscription

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SMB (Server Message Block) | -- | 445 |
| Mappeur de point de terminaison RPC | 135 | 135 |
| RPC | -- | DYNAMIQUE (voir la note 6, **Ports dynamiques**) |

### Serveur de site < -- > Point proxy d'inscription

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SMB (Server Message Block) | -- | 445 |
| Mappeur de point de terminaison RPC | 135 | 135 |

| DESCRIPTION | UDP | TCP |
|---|---|---|
| RPC | -- | DYNAMIQUE (voir la note 6, **Ports dynamiques**) |

**Serveur de site < -- > Point d'état de secours**

(Voir remarque 5, **Communications entre le serveur de site et les systèmes de site**)

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SMB (Server Message Block) | -- | 445 |
| Mappeur de point de terminaison RPC | 135 | 135 |
| RPC | -- | DYNAMIQUE (voir la note 6, **Ports dynamiques**) |

**Serveur de site -- > Internet**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| HTTP (Hypertext Transfer Protocol) | -- | 80 (voir note 1, **Port de serveur proxy**) |

**Serveur de site < -- > Autorité de certification (CA) émettrice**

Cette communication est utilisée lorsque vous déployez des profils de certificat à l'aide du point d'enregistrement de certificat. La communication n'est pas utilisée pour chaque serveur de site de la hiérarchie. En fait, elle est utilisée uniquement pour le serveur de site situé en haut de la hiérarchie.

| DESCRIPTION | UDP | TCP |
|---|---|---|
| Mappeur de point de terminaison RPC | 135 | 135 |
| RPC (DCOM) | -- | DYNAMIQUE (voir la note 6, **Ports dynamiques**) |

**Serveur de site < -- > Point de Reporting Services**

(Voir remarque 5, **Communications entre le serveur de site et les systèmes de site**)

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SMB (Server Message Block) | -- | 445 |
| Mappeur de point de terminaison RPC | 135 | 135 |
| RPC | -- | DYNAMIQUE (voir la note 6, **Ports dynamiques**) |

**Serveur de site < -- > Serveur de site**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SMB (Server Message Block) | -- | 445 |

**Serveur de site -- > SQL Server**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SQL sur TCP | -- | 1433 (voir note 2, **Autre port disponible**) |

Lors de l'installation d'un site utilisant une instance SQL Server distante pour héberger la base de données de site, vous devez ouvrir les ports suivants entre le serveur de site et l'instance SQL Server :

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SMB (Server Message Block) | -- | 445 |
| Mappeur de point de terminaison RPC | 135 | 135 |
| RPC | -- | DYNAMIQUE (voir la note 6, **Ports dynamiques**) |

**Serveur de site -- > Fournisseur SMS**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SMB (Server Message Block) | -- | 445 |
| Mappeur de point de terminaison RPC | 135 | 135 |
| RPC | -- | DYNAMIQUE (voir la note 6, **Ports dynamiques**) |

**Serveur de site < -- > Point de mise à jour logicielle**

(Voir remarque 5, **Communications entre le serveur de site et les systèmes de site**)

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SMB (Server Message Block) | -- | 445 |
| HTTP (Hypertext Transfer Protocol) | -- | 80 ou 8530 (Voir la remarque 3, **Windows Server Update Services**) |
| HTTPS (Secure Hypertext Transfer Protocol) | -- | 443 ou 8531 (Voir la remarque 3, **Windows Server Update Services**) |

**Serveur de site < -- > Point de migration d'état**

(Voir remarque 5, **Communications entre le serveur de site et les systèmes de site**)

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SMB (Server Message Block) | -- | 445 |
| Mappeur de point de terminaison RPC | 135 | 135 |

**Fournisseur SMS -- > SQL Server**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SQL sur TCP | -- | 1433 (voir note 2, **Autre port disponible**) |

**Point de mise à jour logicielle -- > Internet**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| HTTP (Hypertext Transfer Protocol) | -- | 80 (voir note 1, **Port de serveur proxy**) |

**Point de mise à jour logicielle -- > Serveur WSUS en amont**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| HTTP (Hypertext Transfer Protocol) | -- | 80 ou 8530 (Voir la remarque 3, **Windows Server Update Services**) |
| HTTPS (Secure Hypertext Transfer Protocol) | -- | 443 ou 8531 (Voir la remarque 3, **Windows Server Update Services**) |

**SQL Server --> SQL Server**

La réplication inter-sites de base de données exige que le serveur SQL Server d'un site communique directement avec le serveur SQL Server de son site parent ou enfant.

| DESCRIPTION | UDP | TCP |
|---|---|---|
| Service SQL Server | -- | 1433 (voir note 2, **Autre port disponible**) |
| Service Broker SQL Server | -- | 4022 (voir note 2, **Autre port disponible**) |

> **TIP**
> Configuration Manager ne nécessite pas le navigateur SQL Server, qui utilise le port UDP 1434.

**Point de migration d'état -- > SQL Server**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SQL sur TCP | -- | 1433 (voir note 2, **Autre port disponible**) |

**Notes pour les ports utilisés par les clients Configuration Manager et les systèmes de site**

1. **Port de serveur proxy** : ce port ne peut pas être configuré, mais il peut être routé via un serveur proxy configuré.
2. **Autre port disponible** : un autre port peut être défini dans Configuration Manager pour cette valeur. Si un port personnalisé a été défini, remplacez-le lorsque vous définissez les informations de filtre IP pour les stratégies IPsec ou pour configurer les pare-feu.
3. **Windows Server Update Services (WSUS)** : WSUS peut être installé pour utiliser les ports 80/443 ou

8530/8531 pour la communication client. Quand vous exécutez WSUS dans Windows Server 2012 ou Windows Server 2016, WSUS est configuré par défaut pour utiliser le port 8530 pour HTTP et le port 8531 pour HTTPS.

Ce port peut être modifié après l'installation. Vous n'avez pas à utiliser le même numéro de port dans l'ensemble de la hiérarchie du site.

- Si le numéro de port HTTP est 80, le numéro de port HTTPS doit être 443.
- Si le port HTTP a un autre numéro, le port HTTPS doit avoir le numéro 1 ou plus (par exemple 8530 et 8531).

> **NOTE**
> Quand vous configurez le point de mise à jour logicielle pour utiliser HTTPS, le port HTTP doit également être ouvert. Les données non chiffrées, telles que le CLUF pour les mises à jour spécifiques, utilisent le port HTTP.

4. **Service Trivial FTP (TFTP)** : le service système Trivial FTP ne nécessite pas de nom d'utilisateur ni de mot de passe, et il fait partie intégrante des services de déploiement Windows (WDS). Le service Trivial FTP met en œuvre la prise en charge du protocole TFTP qui est défini par les normes RFC suivantes :

   - RFC 350 : TFTP
   - RFC 2347 : extension d'option
   - RFC 2348 : option de taille de bloc
   - RFC 2349 : options d'intervalle de délai d'attente et de taille de transfert

   Le protocole Trivial FTP est conçu pour prendre en charge les environnements de démarrage sans disque. Les services Trivial FTP écoutent au port UDP 69 mais répondent à partir d'un port à numéro élevé alloué de manière dynamique. Ainsi, l'activation de ce port permet au service TFTP de recevoir les demandes TFTP entrantes mais n'autorise pas le serveur sélectionné à répondre à ces demandes. Vous ne pouvez pas permettre au serveur sélectionné de répondre aux demandes TFTP entrantes, à moins que le serveur TFTP soit configuré de manière à répondre à partir du port 69.

5. **Communications entre le serveur de site et les systèmes de site**: par défaut, les communications entre le serveur de site et les systèmes de site sont bidirectionnelles. Le serveur de site initialise la communication pour configurer le système de site, puis la plupart des systèmes de site se connectent à leur tour au serveur de site pour envoyer des informations d'état. Les points de Reporting Services et les points de distribution n'envoient pas d'informations d'état. Si vous sélectionnez **Exiger que le serveur de site démarre les connexions vers ce système de site** dans les propriétés du système de site, après l'installation du système de site, ce dernier n'établit pas la communication vers le système de site. Au lieu de cela, le serveur de site initie la communication et utilise le compte d'installation du système de site pour l'authentification auprès du serveur de système de site.

6. **Ports dynamiques** : les ports dynamiques (également appelés ports éphémères) utilisent une plage de numéros de port qui est définie par la version du système d'exploitation. Pour plus d'informations sur les plages de port par défaut, voir Vue d'ensemble des services et exigences de ports réseau pour le système Windows Server.

## Listes de ports supplémentaires

Les sections suivantes fournissent des informations supplémentaires sur les ports utilisés par Configuration Manager.

**Client vers partages serveur**

Les clients utilisent le protocole SMB (Server Message Block) à chaque fois qu'ils se connectent à des partages UNC. Par exemple :

- Installation manuelle du client spécifiant la propriété de ligne de commande CCMSetup.exe **/source:**
- Clients Endpoint Protection qui téléchargent des fichiers de définition à partir d'un chemin UNC

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SMB (Server Message Block) | -- | 445 |

**Connexions à Microsoft SQL Server**

Pour la communication vers le moteur de base de données SQL Server et pour la réplication intersite, vous pouvez utiliser le port de SQL Server par défaut ou spécifier des ports personnalisés :

- Utilisation des communications intersites :
  - SQL Server Service Broker, qui utilise par défaut le port TCP 4022.
  - Service SQL Server, qui utilise par défaut le port TCP 1433.
- Les communications intrasites entre le moteur de base de données SQL Server et divers rôles de système de site Configuration Manager utilisent par défaut le port TCP 1433.
- Configuration Manager utilise les mêmes ports et protocoles pour communiquer avec chaque réplica du groupe de disponibilité SQL qui héberge la base de données comme si le réplica était une instance SQL Server autonome.

Quand vous utilisez Azure et que la base de données de site se trouve derrière un équilibreur de charge interne ou externe, configurez les exceptions de pare-feu suivantes sur chaque réplica et ajoutez des règles d'équilibrage de charge pour les ports suivants :

- SQL sur TCP : TCP 1433
- SQL Server Service Broker : TCP 4022
- Server Message Block (SMB) : TCP 445
- Mappeur de point de terminaison RPC : TCP 135

> **WARNING**
> Configuration Manager ne prend pas en charge les ports dynamiques. Étant donné que les instances nommées de SQL Server utilisent par défaut des ports dynamiques pour les connexions au moteur de base de données, lorsque vous utilisez une instance nommée, vous devez configurer manuellement le port statique que vous souhaitez utiliser pour la communication intrasite.

Les rôles de système de site suivants communiquent directement avec la base de données SQL Server :

- Point de service web du catalogue des applications
- Rôle de point d'enregistrement de certificat
- Rôle de point d'inscription
- Point de gestion
- Serveur de site
- Point de Reporting Services

- fournisseur SMS
- SQL Server --> SQL Server

Lorsqu'un SQL Server héberge une base de données provenant de plusieurs sites, chaque base de données doit utiliser une instance distincte de SQL Server, et chaque instance doit être configurée avec un ensemble de ports unique.

Si un pare-feu est activé sur l'ordinateur SQL Server, assurez-vous qu'il est configuré pour autoriser les ports utilisés par votre déploiement. Configurez également les pare-feu situés à d'autres emplacements sur le réseau, entre les ordinateurs qui communiquent avec le serveur SQL Server, de manière à autoriser ces ports.

Pour obtenir un exemple montrant comment configurer SQL Server pour utiliser un port spécifique, consultez Configurer un serveur pour écouter un port TCP spécifique (Gestionnaire de configuration SQL Server) dans la bibliothèque TechNet relative à SQL Server.

**Découverte et publication**

Les ports suivants sont utilisés pour la découverte et la publication d'informations de site :

- LDAP (Lightweight Directory Access Protocol) : 389
- LDAP de catalogue global : 3268
- Mappeur de point de terminaison RPC : 135
- RPC : ports TCP à numéro élevé alloués dynamiquement
- TCP : 1024 : 5000
- TCP : 49152 : 65535

**Connexions externes effectuées par Configuration Manager**

Les clients ou les systèmes de site Configuration Manager peuvent établir les connexions externes suivantes :

- Point de synchronisation Asset Intelligence -- > Microsoft
- Point Endpoint Protection -- > Internet
- Client -- > Contrôleur de domaine de catalogue global
- Console Configuration Manager -- > Internet
- Point de gestion -- > Contrôleur de domaine
- Serveur de site -- > Contrôleur de domaine
- Serveur de site < -- > Autorité de certification (CA) émettrice
- Point de mise à jour logicielle -- > Internet
- Point de mise à jour logicielle -- > Serveur WSUS en amont
- Point de connexion de service -- > Microsoft Intune

**Configuration requise pour les systèmes de site qui prennent en charge les clients Internet**

Les points de gestion et les points de distribution qui prennent en charge les clients Internet, le point de mise à jour logicielle et le point d'état de secours utilisent les ports suivants pour l'installation et la réparation :

- Serveur de site --> Système de site : mappeur de point de terminaison RPC utilisant le port UDP et TCP 135
- Serveur de site --> Système de site : ports TCP RPC dynamiques
- Serveur de site < --> Système de site : protocole SMB (Server Message Blocks) utilisant le port TCP 445

Les installations d'applications et de packages sur les points de distribution nécessitent les ports RPC suivants :

- Serveur de site --> Point de distribution : mappeur de point de terminaison RPC utilisant le port UDP et TCP 135
- Serveur de site --> Point de distribution : ports TCP RPC dynamiques

Utilisez IPsec pour sécuriser le trafic entre le serveur de site et les systèmes de site. Si vous devez restreindre les ports dynamiques utilisés par RPC, vous pouvez employer l'outil de configuration Microsoft RPC (rpccfg.exe) pour configurer une plage de ports limitée à ces paquets RPC. Pour plus d'informations sur l'outil de configuration RPC, voir Comment configurer RPC pour qu'il utilise certains ports et comment sécuriser ces ports à l'aide d'IPsec.

> **IMPORTANT**
> Avant d'installer ces systèmes de site, vérifiez que le service d'accès à distance au Registre est en cours d'exécution sur le serveur de système de site et que vous avez spécifié un compte d'installation du système de site si le système de site est situé dans une autre forêt Active Directory sans relation d'approbation.

**Ports utilisés par l'installation du client Configuration Manager**

Les ports utilisés lors de l'installation du client dépendent de la méthode de déploiement du client. Pour obtenir la liste des ports utilisés par chaque méthode de déploiement de clients, consultez la section **Ports utilisés lors du déploiement de clients de Configuration Manager** de l'article Paramètres de port et de Pare-feu Windows pour les clients dans System Center Configuration Manager. Pour plus d'informations sur la configuration du Pare-feu Windows sur le client pour l'installation du client et la communication après l'installation, consultez Paramètres de port et de pare-feu Windows pour les clients dans System Center Configuration Manager.

**Ports utilisés par la migration**

Le serveur de site qui exécute la migration utilise plusieurs ports pour se connecter aux sites applicables dans la hiérarchie source, pour recueillir des données à partir des bases de données SQL Server des sites sources et pour partager des points de distribution.

Pour plus d'informations sur ces ports, consultez la section Configurations requises pour la migration de l'article Prérequis de la migration dans System Center Configuration Manager.

**Ports utilisés par Windows Server**

Le tableau suivant répertorie certains ports principaux utilisés par Windows Server, ainsi que leurs fonctions respectives. Pour une liste plus complète des services Windows Server et les exigences des ports réseau, voir Vue d'ensemble des services et exigences du port réseau pour le système Windows Server.

| DESCRIPTION | UDP | TCP |
|---|---|---|
| DNS (Domain Name System) | 53 | 53 |
| DHCP (Dynamic Host Configuration Protocol) | 67 et 68 | -- |
| Résolution de noms Netbios | 137 | -- |
| Service de datagramme NetBIOS | 138 | -- |
| Service de session NETBIOS | -- | 139 |

# Prise en charge du serveur proxy dans System Center Configuration Manager

22/06/2018 • 7 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les clients aussi bien que les serveurs de système de site System Center Configuration Manager peuvent utiliser un serveur proxy.

## Serveurs de système de site

Quand les rôles de système de site doivent se connecter à Internet, vous pouvez les configurer pour qu'ils utilisent un serveur proxy.

- Un ordinateur qui héberge un serveur de système de site prend en charge une configuration de serveur proxy unique partagée par tous les rôles de système de site sur ce même ordinateur. Si vous avez besoin de serveurs proxy distincts pour les différents rôles ou les différentes instances d'un rôle, vous devez placer ces rôles sur des serveurs de système de site distincts.
- Quand vous configurez de nouveaux paramètres de serveur proxy pour un serveur de système de site qui possède déjà une configuration de serveur proxy, la configuration d'origine est remplacée.
- Les connexions au serveur proxy utilisent le compte **Système** de l'ordinateur qui héberge le rôle de système de site.

Les rôles de système de site suivants se connectent à Internet et peuvent nécessiter un serveur proxy. À une exception près, les rôles de système de site qui peuvent utiliser un proxy le font sans aucune configuration supplémentaire. Cette exception concerne le point de mise à jour logicielle. La liste suivante contient des informations sur les configurations supplémentaires exigées par un point de mise à jour logicielle :

**Point de synchronisation Asset Intelligence** : ce rôle de système de site se connecte à Microsoft et utilise une configuration de serveur proxy sur l'ordinateur hébergeant le point de synchronisation Asset Intelligence.

**Point de distribution cloud** : pour configurer un serveur proxy pour un point de distribution cloud, configurez le proxy sur le site principal qui gère le point de distribution cloud.

Pour cette configuration, le serveur de site principal :

- doit pouvoir se connecter à Microsoft Azure pour configurer le contenu, le surveiller et le distribuer au point de distribution ;
- utilise le compte Système de cet ordinateur pour établir la connexion ;
- utilise le navigateur web par défaut de cet ordinateur.

Vous ne pouvez pas configurer un serveur proxy sur le point de distribution cloud dans Microsoft Azure.

**Point de connexion cloud** : ce rôle de système de site se connecte au service cloud de Configuration Manager pour télécharger des mises à jour de version de Configuration Manager, et utilise un serveur proxy configuré sur l'ordinateur hébergeant le point de connexion de service.

**Connecteur du serveur Exchange Server** : ce rôle de système de site se connecte à un serveur Exchange Server et utilise une configuration de serveur proxy sur l'ordinateur hébergeant le connecteur Exchange Server.

**Point de connexion de service** : ce rôle de système de site se connecte à Microsoft Intune et utilise une configuration de serveur proxy sur l'ordinateur hébergeant le point de connexion de service.

**Point de mise à jour logicielle** : ce rôle de système de site peut utiliser le proxy quand il se connecte à Microsoft Update pour télécharger des correctifs et synchroniser les informations sur les mises à jour. Les points de mise à jour logicielle utilisent un proxy uniquement pour les options suivantes, quand vous activez cette option au moment de la configuration du point de mise à jour logicielle :

- **Utiliser un serveur proxy lors de la synchronisation des mises à jour logicielles**
- **Utiliser un serveur proxy lors du téléchargement du contenu avec des règles de déploiement automatiques** (Bien que disponible, ce paramètre n'est pas utilisé par les points de mise à jour logicielle sur des sites secondaires).

Configurez les paramètres du serveur proxy dans la page Point de mise à jour logicielle actif de l'Assistant Ajout des rôles de système de site ou sous l'onglet **Général** des **Propriétés du composant du point de mise à jour logicielle**.

- Les paramètres du serveur proxy sont associés uniquement au point de mise à jour logicielle au niveau du site.
- Les options de serveur proxy sont disponibles uniquement quand un serveur proxy est déjà configuré pour le serveur de système de site qui héberge le point de mise à jour logicielle.

> **NOTE**
>
> Par défaut, le compte **Système** pour le serveur sur lequel une règle de déploiement automatique a été créée est utilisé pour se connecter à Internet et télécharger les mises à jour logicielles lors de l'exécution des règles de déploiement automatique.
>
> Si ce compte n'a pas accès à Internet, les mises à jour logicielles ne peuvent pas être téléchargées et l'entrée suivante est consignée dans le fichier ruleengine.log : **Échec du téléchargement de la mise à jour sur Internet. Erreur = 12007.**

**Pour configurer le serveur proxy d'un serveur de système de site**

1. Dans la console Configuration Manager, choisissez **Administration**, développez **Configuration du site**, puis choisissez **Serveurs et rôles de système de site**.
2. Sélectionnez le serveur de système de site à modifier, puis dans le volet d'informations, cliquez avec le bouton droit sur **Système de site**, puis choisissez **Propriétés**.
3. Dans Propriétés du système de site, sélectionnez l'onglet **Proxy**, puis configurez les paramètres de proxy de ce serveur de site principal.
4. Cliquez sur **OK** pour enregistrer la nouvelle configuration de serveur proxy.

# Notes de publication de System Center Configuration Manager

22/06/2018 • 7 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Avec Configuration Manager, les notes de publication de produit se limitent aux problèmes urgents. Ces problèmes ne sont pas encore résolus dans le produit ni traités dans un article de la Base de connaissances Microsoft.

La documentation spécifique aux fonctionnalités inclut des informations sur les problèmes connus qui affectent les scénarios de base.

> **TIP**
> Cette rubrique contient les notes de publication pour l'édition actuelle de Configuration Manager. Pour obtenir des informations sur l'édition Technical Preview, consultez Technical Preview pour System Center Configuration Manager

Pour plus d'informations sur les nouvelles fonctionnalités introduites dans les différentes versions, consultez les articles suivants :

- Nouveautés de la version 1802
- Nouveautés dans la version 1710
- Nouveautés dans la version 1706

## Installation et mise à niveau

**Lors de l'utilisation de fichiers redistribuables à partir du dossier CD.Latest, le programme d'installation échoue avec une erreur de vérification du manifeste**

Quand vous exécutez le programme d'installation à partir du dossier CD.Latest créé pour la version 1606 et que vous utilisez les fichiers redistribuables fournis avec ce dossier CD.Latest, le programme d'installation échoue avec les erreurs suivantes dans le journal d'installation de Configuration Manager :

```
ERROR: File hash check failed for defaultcategories.dll
ERROR: Manifest verification failed. Wrong version of manifest?
```

**Solution de contournement**

Utilisez l'une des options suivantes :

- Pendant l'installation, choisissez de télécharger les fichiers redistribuables de Microsoft les plus récents. Utilisez les fichiers redistribuables les plus récents à la place des fichiers inclus dans le dossier CD.Latest.
- Supprimez manuellement le dossier *cd.latest\redist\languagepack\zhh*, puis réexécutez le programme d'installation.

**L'option de la ligne de commande du programme d'installation JoinCEIP doit être spécifiée**

*S'applique à : Configuration Manager version 1802*

Depuis Configuration Manager version 1802, la fonctionnalité du programme d'amélioration de l'expérience utilisateur (CEIP) ne figure plus dans le produit. Lors de l'automatisation de l'installation d'un nouveau site à partir d'un script de ligne de commande ou sans assistance, le programme d'installation retourne une erreur indiquant qu'un paramètre requis est manquant.

#### Solution de contournement

Alors qu'il n'a aucun effet sur le résultat du processus d'installation, incluez le paramètre **JoinCEIP** dans la ligne de commande de l'installation.

> **NOTE**
> Le paramètre EnableSQM pour l'installation de la console n'est pas obligatoire.

## Mise à niveau et déploiement du client

### Les clients compatibles Azure AD ne peuvent pas communiquer avec le point de gestion

*S'applique à : Configuration Manager version 1706*

Dans le scénario pour installer et attribuer des clients Configuration Manager exécutant Windows 10 avec Azure AD pour l'authentification, les communications du client échouent quand le point de gestion HTTPS utilise d'autres informations d'identification de base de données.

#### Solution de contournement

Pour atténuer ce problème, effectuez l'une des actions suivantes :

- Mettez à jour le site vers la dernière version et appliquez le dernier correctif
- Modifiez les informations d'identification utilisées par le point de gestion.

## Mises à jour logicielles

### Les plans de maintenance créent un grand nombre de groupes et de déploiements de mises à jour logicielles en double

Par défaut, l'Assistant Créer un plan de maintenance s'exécute actuellement après chaque synchronisation des mises à jour logicielles. Chaque fois que l'Assistant s'exécute, il crée un groupe et un déploiement de mises à jour logicielles. Si vous avez une planification de la synchronisation des mises à jour logicielles qui s'exécute plusieurs fois par jour, l'Assistant Créer un plan de maintenance génère quotidiennement plusieurs groupes et déploiements de mises à jour logicielles.

#### Solution de contournement

après avoir créé un plan de maintenance, ouvrez les propriétés de celui-ci, accédez à l'onglet **Calendrier d'évaluation**, sélectionnez **Exécuter la règle dans un calendrier**, cliquez sur **Personnaliser**, puis créez un calendrier personnalisé. Par exemple, vous pouvez faire en sorte que le plan de maintenance s'exécute tous les 60 jours.

### Le changement du paramètre client Office 365 ne s'applique pas

*S'applique à : Configuration Manager version 1802*

Déployez un paramètre client avec **Activer la gestion de l'agent Office 365 Client** configuré sur `Yes`. Changez ensuite ce paramètre en `No` ou `Not Configured`. Après la mise à jour de la stratégie sur les clients ciblés, les mises à jour Office 365 continuent d'être gérées par Configuration Manager.

#### Solution de contournement

Changez la valeur de Registre suivante en `0` et redémarrez le **service Microsoft Office « Démarrer en un clic »** (ClickToRunSvc) :

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\office\16.0\Common\officeupdate]
"OfficeMgmtCOM"=dword:00000000
```

# Gestion des appareils mobiles

### Vous ne pouvez plus déployer de profils VPN Windows Phone 8.1 sur Windows 10

*S'applique à : Configuration Manager version 1710*

Vous ne pouvez pas créer de profil VPN à l'aide du workflow Windows Phone 8.1, ce qui s'applique aussi aux appareils Windows 10. Pour ces profils, l'Assistant de création n'affiche plus la page Plateformes prises en charge. Windows Phone 8.1 est sélectionné automatiquement sur le serveur principal. La page Plateformes prises en charge est disponible dans les propriétés du profil, mais n'affiche pas les options de Windows 10.

#### Solution de contournement

Utilisez le workflow du profil VPN Windows 10 pour les appareils Windows 10. Si ce n'est pas possible pour votre environnement, contactez le support technique. Le support technique peut vous aider à ajouter le ciblage Windows 10.

# Prise en charge Unicode et ASCII dans System Center Configuration Manager

22/06/2018 • 6 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

System Center Configuration Manager crée la plupart des objets à l'aide de caractères Unicode. Cependant, plusieurs objets prennent en charge uniquement des caractères ASCII ou disposent d'autres limitations.

Les sections suivantes répertorient les objets qui ne doivent utiliser que les caractères du jeu de caractères ASCII, ou qui ont des limitations supplémentaires.



## Objets qui utilisent des caractères ASCII

Configuration Manager prend en charge le jeu de caractères ASCII uniquement lorsque vous créez les objets suivants :

- Code de site
- Tous les noms des ordinateurs serveurs du système de site
- Les comptes de Configuration Manager suivants :

  > **NOTE**
  > Ces comptes prennent en charge les caractères ASCII et RUS sur un site qui s'exécute en russe.

  - Compte d'installation Push du client
  - Compte de publication de la référence d'état d'intégrité
  - Compte d'interrogation de référence d'état d'intégrité
  - Compte de connexion à la base de données du point de gestion
  - Compte d'accès réseau
  - Compte d'accès au package
  - Compte expéditeur standard
  - Compte d'installation du système de site
  - Compte de connexion de point de mise à jour logicielle
  - Compte du serveur proxy du point de mise à jour logicielle

> **NOTE**
>
> Les comptes que vous spécifiez pour l'administration basée sur des rôles prennent en charge Unicode.
>
> Le compte du point de Reporting Services prend en charge Unicode, à l'exception des caractères RUS.

- Nom de domaine complet (FQDN) pour les serveurs de site et les systèmes de site
- Chemin d'installation de Configuration Manager
- Noms d'instance SQL Server
- Le chemin d'accès pour les rôles de système de site suivants :
  - Point de service web du catalogue des applications
  - Point du site web du catalogue des applications
  - Point d'inscription
  - Point proxy d'inscription
  - Point de Reporting Services
  - Point de migration d'état
- Chemin d'accès pour les dossiers suivants :
  - Le dossier qui stocke les données de migration d'état du client
  - Le dossier qui contient les rapports Configuration Manager
  - Le dossier qui stocke la sauvegarde de Configuration Manager
  - Le dossier qui stocke les fichiers sources d'installation pour la configuration de site
  - Le dossier qui stocke les téléchargements requis par le programme d'installation
- Le chemin d'accès pour les objets suivants :
  - Site Web IIS
  - Chemin d'installation de l'application virtuelle
  - Nom de l'application virtuelle
- Les objets suivants pour AMT et la gestion hors bande :
  - Le nom de domaine complet de l'ordinateur basé sur AMT
  - Le nom d'ordinateur de l'ordinateur basé sur AMT
  - Le nom NetBIOS du domaine
  - Le nom du profil sans fil et SSID
  - Le nom de l'autorité de certification racine de confiance
  - Le nom de l'autorité de certification (CA) et les noms de modèle
  - Le nom de fichier et le chemin du fichier image de redirection IDE
  - Le contenu du stockage de données AMT
- Les noms des fichiers ISO des supports de démarrage

## Limitations supplémentaires

Voici les limitations supplémentaires pour les versions de langue et les jeux de caractères pris en charge :

- Configuration Manager ne prend pas en charge la modification des paramètres régionaux de l'ordinateur serveur de site.
- Une autorité de certification (CA) d'entreprise ne gère pas les noms des ordinateurs clients qui utilisent des jeux de caractères codés sur deux octets (DBCS). Les noms d'ordinateur client que vous pouvez utiliser sont limités par la limitation PKI du jeu de caractères IA5. En outre, Configuration Manager ne prend pas en charge les noms d'autorité de certification ou les valeurs de nom d'objet qui utilisent un jeu de caractères DBCS.

## Objets Configuration Manager non localisés

La base de données Configuration Manager prend en charge le format Unicode pour la plupart des objets qu'elle stocke, et lorsque cela est possible, elle affiche ces informations dans la langue du système d'exploitation correspondant aux paramètres régionaux d'un ordinateur. Pour que l'interface client ou la console Configuration Manager affichent des informations dans la langue du système d'exploitation de l'ordinateur, les paramètres régionaux de l'ordinateur doivent correspondre à la langue du client ou du serveur que vous installez sur un site.

Toutefois, plusieurs objets Configuration Manager ne prennent pas en charge le format Unicode et ils sont stockés dans la base de données à l'aide du jeu de caractères ASCII, ou bien les langues supplémentaires sont limitées. Ces informations s'affichent toujours à l'aide du jeu de caractères ASCII défini ou dans la langue utilisée lors de la création de l'objet.

# Insights de gestion dans System Center Configuration Manager

22/06/2018 • 7 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les insights de gestion dans System Center Configuration Manager fournissent des informations sur l'état actuel de votre environnement. Les informations sont basées sur l'analyse des données provenant de la base de données du site. Ces informations vous aident à mieux comprendre votre environnement et à prendre des mesures en fonction de ces renseignements. Cette fonctionnalité a été publiée dans Configuration Manager version 1802.

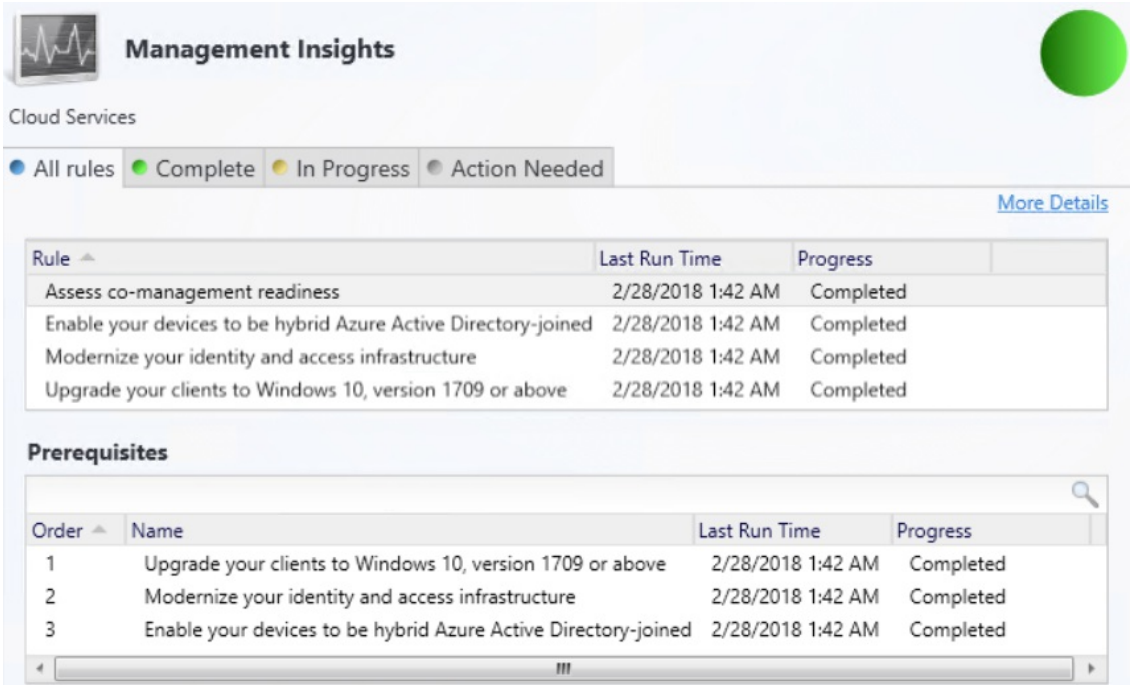
## Examiner les insights de gestion dans la console Configuration Manager

L'autorisation de **lecture sur le site** est nécessaire pour afficher les règles.

1. Ouvrez la console Configuration Manager.
2. Accédez au nœud **Administration** et cliquez sur **Insights de gestion**.
3. Sélectionnez **Tous les insights**
4. Double-cliquez sur le **Nom du groupe d'insights de gestion** que vous souhaitez examiner. Vous pouvez également le mettre en surbrillance et cliquer sur **Afficher les insights** dans le ruban.
5. Quatre onglets sont disponibles pour l'examen, ainsi que les prérequis nécessaires pour exécuter la règle.

   - **Toutes les règles** : affiche la liste complète des règles pour le groupe d'insights de gestion choisi.
   - **Terminé** : liste les règles quand aucune action n'est nécessaire.
   - **En cours** : affiche les règles quand certains prérequis, mais pas tous, sont remplis.
   - **Action nécessaire** : les règles nécessitant la prise de mesures sont listées. Cliquez avec le bouton droit et sélectionnez **Plus de détails** pour récupérer des éléments spécifiques quand une action est nécessaire.
   - **Prérequis** : si une règle a besoin d'éléments terminés avant qu'ils ne puissent être exécutés, les éléments nécessaires sont affichés ici.

     **Ensemble des règles et prérequis pour le groupe de services cloud**




## Réévaluation et journalisation des insights de gestion

Les règles des insights de gestion réévaluent leur mise en application selon une planification hebdomadaire. Vous pouvez réévaluer une règle à la demande en cliquant avec le bouton droit sur la règle et en sélectionnant **Réévaluer**.

**Fichier journal pour les règles des insights de gestion** : SMS_DataEngine.log

## Règles et groupes d'insights de gestion

Les règles sont organisées en différents groupes d'insights de gestion. Le cas échéant, les groupes et les règles sont ajoutés à la liste suivante :

**Applications** : insights pour la gestion de votre application.

- **Applications sans déploiements** : répertorie les applications de votre environnement qui n'ont pas de déploiements actifs. Cette règle facilite la recherche et la suppression des applications inutilisées pour simplifier la liste des applications affichées dans la console.

**Services cloud** : vous permet d'intégrer de nombreux services cloud ; activation de la gestion moderne de vos appareils.

- **Évaluer la préparation de la cogestion** : vous aide à comprendre les étapes nécessaires pour activer la cogestion. Cette règle comporte des prérequis.
- **Permettre à vos appareils d'être hybrides joints à Azure Active Directory** : les appareils joints à Azure AD permettent aux utilisateurs de se connecter avec leurs informations d'identification de domaine tout en garantissant que les appareils répondent aux normes de conformité et de sécurité de l'organisation.
- **Moderniser votre infrastructure d'identité et d'accès** : le service cloud Azure AD avec l'authentification multifacteur intégrée protège les données sensibles et les applications à la fois localement et dans le cloud.
- **Mettre à niveau vos clients vers Windows 10, version 1709 ou ultérieure** : Windows 10 version 1709 ou ultérieure améliore et modernise l'expérience informatique de vos utilisateurs.

**Regroupements** : insights qui permettent de simplifier la gestion par le nettoyage et la reconfiguration de regroupements.

- **Regroupements vides** : répertorie les regroupements de votre environnement qui n'ont aucun membre.

**Gestion simplifiée** : insights qui permettent de simplifier la gestion quotidienne de votre environnement.

- **Versions des clients obsolètes** : répertorie tous les clients dont les versions sont antérieures à deux ans.

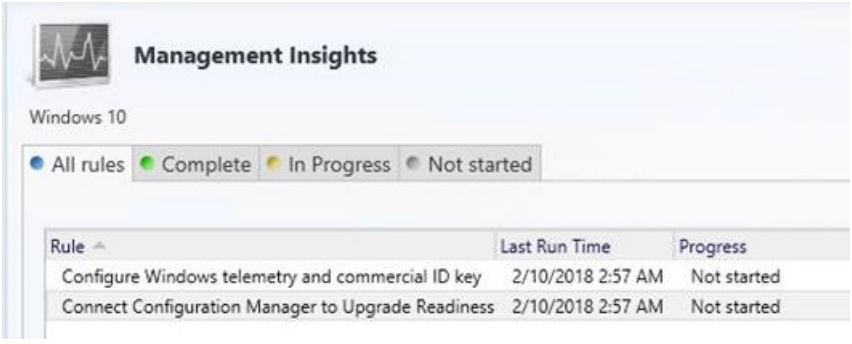
**Centre logiciel** : insights pour la gestion du Centre logiciel.

- **Diriger les utilisateurs vers le Centre logiciel au lieu du catalogue d'applications** : vérifiez si les utilisateurs ont installé ou demandé des applications provenant du catalogue d'applications au cours des 14 derniers jours. La fonctionnalité principale du catalogue d'applications est désormais incluse dans le Centre logiciel. La prise en charge du site web du catalogue d'applications prend fin avec la première mise à jour publiée après le 1er juin 2018
- **Utiliser la nouvelle version du Centre logiciel** : la version précédente du Centre logiciel n'est plus prise en charge. Configurez les clients pour qu'ils utilisent le nouveau Centre logiciel en activant le paramètre client **Agent ordinateur** > **Utiliser le nouveau Centre logiciel**.

**Windows 10** : insights sur le déploiement et la maintenance de Windows 10. Le groupe d'insights de gestion Windows 10 est disponible quand plus de la moitié des clients exécutent Windows 7, Windows 8 ou Windows 8.1.

- **Configurer la télémétrie et la clé d'ID commercial de Windows** : pour utiliser des données d'Upgrade Readiness, les appareils doivent être configurés avec une clé d'ID commercial et la télémétrie doit être activée. Les appareils Windows 10 doivent avoir un niveau de télémétrie supérieur ou égal à Avancé (limité).
- **Connecter Configuration Manager à Upgrade Readiness** : tirez parti d'Upgrade Readiness pour accélérer vos déploiements de Windows 10 avant la fin de la prise en charge de Windows 7. **Configurer la télémétrie et la clé d'ID commercial de Windows** est un prérequis.

**Règles d'insights de gestion Windows 10**



# Tâches de maintenance pour System Center Configuration Manager

22/06/2018 • 14 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les sites et hiérarchies System Center Configuration Manager exigent une maintenance et une surveillance régulières pour fournir en permanence des services efficaces. Une maintenance régulière garantit que le matériel, les logiciels et la base de données Configuration Manager fonctionnent toujours correctement et efficacement. Lorsque les performances sont optimales, les risques de défaillance sont considérablement réduits.

Pour configurer des alertes et utiliser le système d'état pour surveiller l'intégrité de Configuration Manager, consultez Utiliser des alertes et le système d'état pour System Center Configuration Manager.



## Tâches de maintenance

Une maintenance régulière est essentielle pour assurer le bon fonctionnement du site. Tenez un journal des tâches de maintenance pour y documenter les dates, les auteurs et tout commentaire de maintenance sur les tâches.

**Quand effectuer les tâches de maintenance courantes ?**

Pour maintenir votre site, envisagez une maintenance quotidienne ou hebdomadaire. Certaines tâches peuvent nécessiter une planification différente. Une maintenance courante peut inclure les tâches de maintenance prédéfinies, ainsi que d'autres tâches, telles que la gestion des comptes pour conserver la conformité aux stratégies de l'entreprise.

Utilisez les informations suivantes comme guide pour mieux planifier quand effectuer les différentes tâches de maintenance. Utilisez ces listes comme point de départ et ajoutez les tâches éventuellement requises.

**Tâches quotidiennes**

Tâches de maintenance que vous pouvez envisager d'effectuer quotidiennement :

- Vérifiez que les tâches de maintenance prédéfinies devant être exécutées quotidiennement s'exécutent correctement.
- Vérifiez l'état de la base de données Configuration Manager.
- Vérifiez l'état du serveur de site.
- Vérifiez les boîtes de réception de système de site Configuration Manager pour chercher des backlogs de fichiers.
- Vérifiez l'état des systèmes de site.
- Vérifiez les journaux d'événements du système d'exploitation sur les systèmes de site.
- Vérifiez le journal des erreurs de SQL Server sur l'ordinateur de la base de données de site.
- Vérifiez les performances du système.
- Vérifiez les alertes Configuration Manager.

**Tâches hebdomadaires**

Tâches de maintenance que vous pouvez envisager d'effectuer chaque semaine :

- Vérifiez que les tâches de maintenance prédéfinies devant être exécutées chaque semaine s'exécutent correctement.
- Supprimez les fichiers inutiles des systèmes de sites.
- Si nécessaire, rédigez et distribuez des rapports destinés aux utilisateurs finaux.
- Sauvegardez les journaux des applications, de sécurité et des événements système, et effacez-les.
- Vérifiez la taille de la base de données du site et assurez-vous que l'espace disque disponible sur le serveur de bases de données du site est suffisant pour permettre à la base de données de grandir.
- Effectuez la maintenance de la base de données du site, conformément à votre plan de maintenance de base de données SQL Server.
- Vérifiez que tous les systèmes de site disposent d'espace disque disponible.
- Exécutez les outils de défragmentation sur tous les systèmes de site.

**Tâches périodiques**

Certaines tâches qui ne nécessitent pas de maintenance quotidienne ni hebdomadaire sont importantes pour garantir l'intégrité globale du site. Ces tâches garantissent également que les plans de récupération d'urgence et de sécurité sont à jour. Tâches de maintenance que vous pouvez envisager d'effectuer plus régulièrement que les tâches quotidiennes ou hebdomadaires :

- Modifier les comptes et les mots de passe, si nécessaire, en fonction de votre plan de sécurité.
- Passez en revue le plan de maintenance pour vérifier si les tâches de maintenance prévues sont planifiées correctement et efficacement en fonction des paramètres de site configurés.
- Passez en revue la conception de la hiérarchie Configuration Manager pour repérer toute modification requise.
- Vérifiez les performances du réseau pour vous assurer qu'aucune modification effectuée n'affecte le fonctionnement du site.
- Vérifiez que les paramètres Active Directory affectant le fonctionnement du site n'ont pas été modifiés. Par exemple, vérifiez que les sous-réseaux qui sont attribués aux sites Active Directory et utilisés comme limites du site Configuration Manager n'ont pas changé.
- Examiner dans votre plan de reprise après incident toute modification nécessaire.
- Récupérez un site selon le plan de récupération d'urgence dans un laboratoire de test en utilisant une copie de sauvegarde de la dernière sauvegarde créée par la tâche de maintenance Serveur de site de sauvegarde.
- Examiner les erreurs liées au matériel ou vérifier si des mises à jour matérielles sont disponibles.
- Vérifier l'état d'intégrité global du site.

**Garantir l'intégrité opérationnelle de votre base de données de site**

Quand votre site et hiérarchie Configuration Manager effectuent les tâches que vous planifiez et configurez, les composants de site ajoutent continuellement des données à la base de données Configuration Manager. Les performances de la base de données et l'espace de stockage disponible dans la base de données diminuent au fur et à mesure que la quantité de données augmente. Vous pouvez configurer des tâches de maintenance de site pour supprimer les données anciennes dont vous n'avez plus besoin.

Configuration Manager propose des tâches de maintenance prédéfinies que vous pouvez utiliser pour garantir l'intégrité de la base de données Configuration Manager. Toutes les tâches de maintenance ne sont pas disponibles sur chaque site, par défaut. Certaines tâches sont activées alors que d'autres ne le sont pas, et toutes

prennent en charge une planification que vous pouvez configurer.

La plupart des tâches de maintenance prédéfinies suppriment régulièrement les données périmées de la base de données Configuration Manager. La réduction de la taille de la base de données obtenue en supprimant les données inutiles permet d'améliorer les performances et l'intégrité de la base de données, ce qui améliore l'efficacité du site et de la hiérarchie. D'autres tâches, telles que **Reconstruire les index**, aident à maintenir l'efficacité de la base de données. D'autres tâches, telles que la tâche **Serveur de site de sauvegarde**, vous aident à préparer la récupération d'urgence.

> **IMPORTANT**
> Lorsque vous planifiez l'exécution d'une tâche qui supprime des données, examinez l'utilisation de ces données dans la hiérarchie. Quand une tâche qui supprime des données s'exécute sur un site, les informations sont supprimées de la base de données Configuration Manager, et cette modification est répliquée sur tous les sites dans la hiérarchie. Cette suppression peut affecter d'autres tâches reposant sur ces données. Par exemple, sur le site d'administration centrale, vous pouvez configurer une exécution mensuelle de la découverte afin d'identifier les ordinateurs non clients. Vous planifiez d'installer le client Configuration Manager sur ces ordinateurs dans un délai de deux semaines à compter de leur découverte. Toutefois, sur un site de la hiérarchie, un administrateur configure une exécution hebdomadaire de la tâche Supprimer les données de découverte anciennes. Il en résulte qu'une semaine après la découverte des ordinateurs non clients, ils sont supprimés de la base de données Configuration Manager. De retour sur le site d'administration centrale, vous préparez l'installation push du client Configuration Manager sur ces nouveaux ordinateurs au bout du dixième jour. Toutefois, étant donné que la tâche Supprimer les données de découverte anciennes a récemment été exécutée pour supprimer les données de sept jours ou plus, les ordinateurs récemment découverts ne sont plus disponibles dans la base de données.

Après l'installation d'un site Configuration Manager, passez en revue les tâches de maintenance disponibles et activez celles nécessaire pour vos opérations. Passez en revue la planification par défaut de chaque tâche et, si nécessaire, modifiez la planification pour ajuster la tâche de maintenance en fonction de votre hiérarchie et de votre environnement. Bien que la planification par défaut de chaque tâche s'adapte à la plupart des environnements, surveillez les performances de vos sites et de votre base de données, et envisagez de reconfigurer ces tâches afin d'optimiser l'efficacité de votre déploiement. Planifiez d'examiner régulièrement les performances du site et de la base de données, ainsi que de reconfigurer les tâches de maintenance et leurs planifications afin de maintenir l'efficacité.

#### Configurer les tâches de maintenance

Chaque site Configuration Manager prend en charge des tâches de maintenance qui contribuent à garantir le fonctionnement optimal de la base de données du site. Par défaut, plusieurs tâches de maintenance sont activées pour chaque site, et toutes les tâches prennent en charge des planifications indépendantes. Les tâches de maintenance sont configurées individuellement pour chaque site et s'appliquent à la base de données sur le site. Toutefois, certaines tâches, telles que **Supprimer les données de découverte anciennes**, affectent les informations disponibles dans tous les sites d'une hiérarchie.

La console Configuration Manager affiche uniquement les tâches de maintenance que vous pouvez configurer sur un site. Pour obtenir la liste complète des tâches de maintenance par type de site, consultez Référence des tâches de maintenance pour System Center Configuration Manager.

Utilisez la procédure suivante pour mieux configurer les paramètres courants des tâches de maintenance.

##### Pour configurer les tâches de maintenance pour Configuration Manager

1. Dans la console Configuration Manager, accédez à **Administration** > **Configuration de site** >**Sites**.
2. Choisissez le site avec la tâche de maintenance que vous souhaitez configurer.
3. Sous l'onglet **Accueil**, dans le groupe **Paramètres**, choisissez **Maintenance de site**, puis choisissez la tâche de maintenance que vous souhaitez configurer.

> **TIP**
> Seules les tâches disponibles sur le site sélectionné sont affichées.

4. Pour configurer la tâche, choisissez **Modifier**, veillez à ce que la case **Activer cette tâche** soit cochée, et planifiez l'exécution de la tâche. Si la tâche supprime également les données anciennes, configurez l'ancienneté des données à supprimer de la base de données lors de l'exécution de la tâche. Choisissez **OK** pour fermer les **Propriétés** de la tâche.

   > **NOTE**
   > Pour **Supprimer les messages d'état anciens**, vous devez configurer l'ancienneté des données à supprimer lorsque vous configurez des règles de filtre d'état.

5. Pour activer ou désactiver la tâche sans modifier les propriétés de la tâche, choisissez le bouton **Activer** ou **Désactiver**. L'étiquette du bouton change en fonction de la configuration actuelle de la tâche.

6. Une fois que vous avez terminé de configurer les tâches de maintenance, choisissez **OK** pour terminer la procédure.

# Référence des tâches de maintenance pour System Center Configuration Manager

22/06/2018 • 32 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cette rubrique répertorie les détails de chaque tâche de maintenance de site de System Center Configuration Manager et spécifie les types de sites sur lesquels la tâche est disponible. Chaque entrée indique également si la tâche est activée ou non par défaut. Pour plus d'informations sur la planification et la configuration de sites pour exécuter des tâches de maintenance, consultez Tâches de maintenance pour System Center Configuration Manager.

**Serveur de site de sauvegarde** : cette tâche permet de préparer la récupération des données critiques. Vous pouvez créer une sauvegarde de vos informations critiques pour restaurer un site et la base de données Configuration Manager. Pour plus d'informations, consultez Sauvegarde et récupération pour System Center Configuration Manager.

- **Site d'administration centrale** : activé
- **Site principal**non activé
- Site secondaire : non disponible

**Vérifier le titre de l'application à l'aide des informations d'inventaire** : cette tâche permet de maintenir la cohérence entre les titres de logiciels rapportés dans l'inventaire logiciel et les titres de logiciels du catalogue Asset Intelligence. Pour plus d'informations, consultez Présentation d'Asset Intelligence dans System Center Configuration Manager.

- **Site d'administration centrale** : activé
- **Site principal** : activé
- Site secondaire : non disponible

**Remettre à zéro l'indicateur d'installation** : cette tâche permet de supprimer l'indicateur installé pour les clients qui n'envoient pas d'enregistrement de découverte par pulsations d'inventaire durant la période de **Redécouverte du client**. L'indicateur installé empêche l'installation push automatique du client sur un ordinateur pouvant disposer d'un client Configuration Manager actif.

- Site d'administration centrale : non disponible
- **Site principal**non activé
- Site secondaire : non disponible

**Supprimer les anciennes données de demande d'application** : cette tâche permet de supprimer les demandes d'application anciennes de la base de données. Pour plus d'informations sur les demandes d'application, consultez Créer et déployer une application avec System Center Configuration Manager.

- Site d'administration centrale : non disponible
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer l'historique de téléchargement de clients anciens** : utilisez cette tâche pour supprimer les données historiques relatives à la source de téléchargement utilisée par les clients. Les informations relatives à la source du téléchargement permettent de remplir le tableau de bord Sources de données du client.

- Site d'administration centrale : non disponible
- **Site principal** - Activée
- Site secondaire - Non disponible

**Supprimer les anciennes opérations des clients** : cette tâche permet de supprimer de la base de données de site toutes les anciennes données pour les opérations des clients. Cela comprend par exemple les données pour les notifications des clients anciennes ou ayant expiré (comme les demandes de téléchargement pour les stratégies utilisateur ou ordinateur) et pour Endpoint Protection (comme les demandes effectuées par un utilisateur administratif pour que les clients exécutent une analyse ou téléchargent des définitions mises à jour).

- **Site d'administration centrale** : activé
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer historique de présence de clients anciens** : cette tâche permet de supprimer les informations d'historique sur le statut de connexion des clients, enregistrées par la notification client, qui sont antérieures à l'heure spécifiée. Pour plus d'informations sur la notification client, consultez Comment surveiller des clients dans System Center Configuration Manager.

- **Site d'administration centrale** : activé
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer les anciennes données de trafic de la passerelle de gestion cloud** : cette tâche permet de supprimer toutes les anciennes données sur le trafic de la base de données du site qui transite via la passerelle de gestion cloud. Cela inclut par exemple les données sur le nombre de demandes, le nombre total d'octets des demandes et des réponses, ainsi que le nombre de demandes ayant échoué et le nombre maximum de demandes simultanées.

- **Site d'administration centrale** - Activée
- **Site principal** - Activée
- Site secondaire - Non disponible

**Supprimer les fichiers collectés anciens** : cette tâche permet de supprimer de la base de données d'anciennes informations sur les fichiers collectés. Cette tâche supprime également les fichiers collectés à partir de la structure de dossier du serveur de site sur le site sélectionné. Par défaut, les cinq copies les plus récentes des fichiers collectés sont stockées sur le serveur de site dans le répertoire **Inboxes\sinv.box\FileCol**. Pour plus d'informations, consultez Présentation de l'inventaire logiciel dans System Center Configuration Manager.

- Site d'administration centrale : non disponible
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer les données d'associations d'ordinateurs anciennes** : cette tâche permet de supprimer de la base de données d'anciennes données d'associations d'ordinateur du déploiement de système d'exploitation. Ces informations sont utilisées dans le cadre de l'exécution de restaurations de l'état utilisateur. Pour plus d'informations sur les associations d'ordinateurs, consultez Gérer l'état utilisateur dans System Center Configuration Manager.

- Site d'administration centrale : non disponible
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer les données de détection de suppression anciennes** : cette tâche permet de supprimer de la base de données d'anciennes données ayant été créées par Extraction Views. Par défaut, Extraction Views est désactivé.

Vous pouvez uniquement l'activer à l'aide du SDK Configuration Manager. Sauf si Extraction Views est activé, il n'y a pas de données à supprimer pour cette tâche.

- **Site d'administration centrale** : activé
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer l'ancien enregistrement de réinitialisation de périphérique** : cette tâche permet de supprimer de la base de données d'anciennes données d'actions de réinitialisation d'appareils mobiles. Pour plus d'informations sur la réinitialisation des appareils mobiles, consultez Protéger les données à l'aide de la réinitialisation à distance, du verrouillage à distance ou de la réinitialisation du code d'accès en utilisant System Center Configuration Manager.

- Site d'administration centrale : non disponible
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer les anciens périphériques gérés par le connecteur du serveur Exchange Server** : cette tâche permet de supprimer d'anciennes données d'appareils mobiles gérés par le connecteur Exchange Server. Ces données sont supprimées en fonction de l'intervalle configuré pour l'option **Ignorer les appareils mobiles inactifs depuis plus de (jours)** sous l'onglet **Découverte** des propriétés du connecteur Exchange Server. Pour plus d'informations, consultez Gérer les appareils mobiles avec System Center Configuration Manager et Exchange.

- Site d'administration centrale : non disponible
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer les données de découverte anciennes** : cette tâche permet de supprimer de la base de données d'anciennes données de découverte. Ces données peuvent inclure les enregistrements résultant des méthodes de découverte par pulsations, de découverte réseau et de découverte Active Directory Domain Services (Système, Utilisateur et Groupe). Cette tâche supprime également les anciens appareils marqués comme étant désactivés. Lorsque cette tâche s'exécute sur un site, les données associées à celui-ci sont supprimées, et ces modifications sont répliquées vers d'autres sites. Pour plus d'informations sur la découverte, voir Exécuter la découverte pour System Center Configuration Manager.

- Site d'administration centrale : non disponible
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer les données d'utilisation de l'ancien point de distribution** : cette tâche permet de supprimer de la base de données d'anciennes données des points de distribution ayant été stockées plus longtemps que la durée spécifiée.

- **Site d'administration centrale** : activé
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer les anciennes données de l'historique de l'état d'intégrité Endpoint Protection** : cette tâche permet de supprimer de la base de données d'anciennes informations d'état Endpoint Protection. Pour plus d'informations sur les informations d'état Endpoint Protection, consultez Comment surveiller Endpoint Protection dans System Center Configuration Manager.

- Site d'administration centrale : non disponible
- **Site principal** : activé

- Site secondaire : non disponible

**Supprimer les anciens périphériques inscrits** : à compter de la mise à jour pour la version 1602, cette tâche est désactivée par défaut. Vous pouvez utiliser cette tâche pour supprimer de la base de données de site d'anciennes données concernant les appareils mobiles qui n'ont signalé aucune information au site pendant une durée spécifiée.

Cette tâche s'applique aux appareils qui sont inscrits à l'aide de Microsoft Intune (hybride) ou de la gestion des appareils mobiles locale de Configuration Manager. Pour plus d'informations sur les systèmes d'exploitation des appareils inscrits à l'aide de Configuration Manager ou d'Intune, consultez la section Appareils mobiles inscrits par Microsoft Intune dans Systèmes d'exploitation pris en charge pour les clients et les appareils pour System Center Configuration Manager.

- Site d'administration centrale : non disponible
- **Site principal**non activé
- Site secondaire : non disponible

**Supprimer les historiques d'inventaire anciens** : cette tâche permet de supprimer des données d'inventaire ayant été stockées dans la base de données pendant une durée plus longue que celle spécifiée. Pour plus d'informations sur l'historique d'inventaire, consultez Comment utiliser l'Explorateur de ressources pour afficher l'inventaire matériel dans System Center Configuration Manager.

- Site d'administration centrale : non disponible
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer les anciennes données de journal** : cette tâche permet de supprimer d'anciennes données de journal utilisées pour le dépannage de la base de données. Ces données ne sont pas liées à des opérations de composants Configuration Manager.

> **IMPORTANT**
> Par défaut, cette tâche s'exécute quotidiennement sur chaque site. Au niveau du site d'administration centrale et des sites principaux, la tâche supprime les données datant de plus de 30 jours. Quand vous utilisez SQL Server Express sur un site secondaire, veillez à ce que cette tâche soit exécutée chaque jour et à ce qu'elle supprime bien les données inactives depuis sept jours.

- **Site d'administration centrale** : activé
- **Site principal** : activé
- **Site secondaire** : activé

**Supprimer l'historique d'anciennes tâches de notification** : cette tâche permet de supprimer de la base de données du site des informations sur des tâches de notification client quand elles n'ont pas été mises à jour pendant une période spécifiée. Pour plus d'informations sur la notification client, consultez Tâches de déploiement du client pour System Center Configuration Manager.

- Site d'administration centrale : non disponible
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer les anciennes données de synthèse de la réplication** : cette tâche permet de supprimer de la base de données du site d'anciennes données de synthèse de la réplication quand elles n'ont pas été mises à jour pendant une période spécifiée. Pour plus d'informations, voir la section How to monitor database replication links and replication status dans la rubrique Monitor hierarchy and replication infrastructure in System Center Configuration Manager.

- **Site d'administration centrale** : activé
- **Site principal** : activé
- **Site secondaire** : activé

**Supprimer les anciens enregistrements de code secret** : utilisée sur le site de niveau supérieur de votre hiérarchie, cette tâche permet de supprimer d'anciennes données de réinitialisation de code d'accès pour des appareils Android et Windows Phone. Les données de réinitialisation de code secret sont chiffrées, mais n'incluent pas le code confidentiel des appareils. Par défaut, cette tâche est activée et supprime les données datant de plus d'un jour.

- **Site d'administration centrale** : activé
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer les anciennes données de suivi de réplication** : cette tâche permet de supprimer de la base de données d'anciennes données sur la réplication de base de données entre sites Configuration Manager. Lorsque vous modifiez la configuration de cette tâche de maintenance, la configuration s'applique à chaque site concerné de la hiérarchie. Pour plus d'informations, voir la section How to monitor database replication links and replication status dans la rubrique Monitor hierarchy and replication infrastructure in System Center Configuration Manager.

- **Site d'administration centrale** : activé
- **Site principal** : activé
- **Site secondaire** : activé

**Supprimer les données de contrôle de logiciel anciennes** : cette tâche permet de supprimer de la base de données d'anciennes données du contrôle de logiciel ayant été stockées plus longtemps que la durée spécifiée. Pour plus d'informations, consultez Contrôle de logiciel dans System Center Configuration Manager.

- Site d'administration centrale : non disponible
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer les données de résumé de contrôle de logiciel anciennes** : cette tâche permet de supprimer de la base de données d'anciennes données de résumé du contrôle de logiciel ayant été stockées plus longtemps que la durée spécifiée. Pour plus d'informations, consultez Contrôle de logiciel dans System Center Configuration Manager.

- Site d'administration centrale : non disponible
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer les messages d'état anciens** : cette tâche permet de supprimer de la base de données d'anciennes données de message d'état en fonction de la configuration des règles de filtre d'état. Pour plus d'informations, consultez la section « Surveiller l'état du système de Configuration Manager » dans la rubrique Utiliser des alertes et le système d'état pour System Center Configuration Manager.

- **Site d'administration centrale** : activé
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer les anciennes données de menace** : cette tâche permet de supprimer de la base de données d'anciennes données de menace Endpoint Protection ayant été stockées plus longtemps que la période spécifiée. Pour plus d'informations sur Endpoint Protection, consultez Endpoint Protection dans System Center Configuration Manager.

- Site d'administration centrale : non disponible
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer les anciens ordinateurs inconnus** : cette tâche permet de supprimer de la base de données de site des informations sur des ordinateurs inconnus quand elles n'ont pas été mises à jour pendant une période spécifiée. Pour plus d'informations, consultez Préparer les déploiements d'ordinateurs inconnus dans System Center Configuration Manager.

- Site d'administration centrale : non disponible
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer les anciennes données d'affinité entre périphérique et utilisateur** : cette tâche permet de supprimer de la base de données d'anciennes données d'affinité entre appareil et utilisateur. Pour plus d'informations, consultez Lier des utilisateurs et des appareils avec l'affinité entre utilisateur et appareil dans System Center Configuration Manager.

- Site d'administration centrale : non disponible
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer les enregistrements de package d'inscription en bloc MDM expirés** : utilisez cette tâche pour supprimer les anciens certificats d'inscription en bloc et les profils correspondants après l'expiration du certificat d'inscription. Pour plus d'informations, consultez Créer des profils de certificat.

- **Site d'administrations centrales** : activé
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer les données de découverte des clients inactifs** : cette tâche permet de supprimer de la base de données des données de découverte de clients inactifs. Les clients sont marqués comme inactifs quand le client est marqué comme obsolète et par les configurations effectuées pour l'état du client.

Cette tâche ne fonctionne que sur les ressources qui des clients Configuration Manager. Elle est différente de la tâche **Supprimer les données de découverte anciennes** qui supprime tous les anciens enregistrements de données de découverte. Lorsque cette tâche s'exécute sur un site, elle supprime les données de la base de données de tous les sites d'une hiérarchie. Pour plus d'informations, voir Guide pratique pour configurer l'état du client dans System Center Configuration Manager.

> **IMPORTANT**
> Quand elle est activée, configurez cette tâche pour qu'elle s'exécute à un intervalle plus important que celui planifié pour la **Découverte par pulsations d'inventaire**. Les clients actifs peuvent ainsi envoyer un enregistrement de type Découverte par pulsations d'inventaire pour marquer leur enregistrement de client comme actif, de sorte que cette tâche ne les supprime pas.

- Site d'administration centrale : non disponible
- **Site principal**non activé
- Site secondaire : non disponible

**Supprimer les alertes obsolètes** : cette tâche permet de supprimer de la base de données des alertes expirées ayant été stockées pendant une période plus longue que celle spécifiée. Pour plus d'informations, voir Utiliser des alertes et le système d'état pour System Center Configuration Manager.

- **Site d'administration centrale** : activé
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer les données obsolètes de découverte des clients** : cette tâche permet de supprimer de la base de données des enregistrements de client obsolètes. Un enregistrement marqué comme obsolète a généralement été remplacé par un enregistrement plus récent pour le même client. L'enregistrement plus récent devient l'enregistrement actuel du client. Pour plus d'informations sur la découverte, voir Exécuter la découverte pour System Center Configuration Manager.

> **IMPORTANT**
> Quand elle est activée, configurez cette tâche pour qu'elle s'exécute à un intervalle plus important que celui planifié pour la Découverte par pulsations d'inventaire. Cela permet au client d'envoyer un enregistrement de découverte par pulsations d'inventaire qui définit l'état obsolète correctement.

- Site d'administration centrale : non disponible
- **Site principal**non activé
- Site secondaire : non disponible

**Supprimer les sites et sous-réseaux de découverte de forêts obsolètes** : cette tâche permet de supprimer des données de sites, de sous-réseaux et de domaines Active Directory n'ayant pas été découverts par la méthode de découverte de forêt Active Directory au cours des 30 derniers jours. Cela supprime les données de découverte, mais n'affecte pas les limites créées à partir de ces données de découverte. Pour plus d'informations, voir Exécuter la découverte pour System Center Configuration Manager.

- **Site d'administration centrale** : activé
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer les enregistrements d'état du déploiement des clients orphelins** : cette tâche permet de purger régulièrement la table qui contient les informations sur l'état du déploiement d'un client. Cette tâche nettoie les enregistrements associés aux appareils obsolètes ou désactivés.

- **Site d'administration centrale** : activé
- **Site principal** : activé
- Site secondaire : non disponible

**Supprimer les révisions d'application inutilisées** : cette tâche permet de supprimer les révisions d'application qui ne sont plus référencées. Pour plus d'informations, consultez Comment modifier et remplacer des applications dans System Center Configuration Manager.

- Site d'administration centrale : non disponible
- **Site principal** : activé
- Site secondaire : non disponible

**Évaluer les membres du regroupement** : vous configurez l'évaluation de l'appartenance au regroupement comme composant de site. Pour plus d'informations sur les composants de site, voir Site components for System Center Configuration Manager.

- Site d'administration centrale : non disponible
- **Site principal** : activé
- Site secondaire : non disponible

**Contrôler les clés** : cette tâche permet de surveiller l'intégrité des clés primaires de la base de données Configuration Manager. Une clé primaire est une colonne (ou une combinaison de colonnes) qui identifie de manière unique une ligne et la distingue des autres lignes dans une table de base données Microsoft SQL Server.

- **Site d'administration centrale** : activé
- **Site principal** : activé
- Site secondaire : non disponible

**Reconstruire les index** : cette tâche permet de reconstruire les index des bases de données Configuration Manager. Un index désigne une structure de base de données créée dans une table de base de données pour accélérer le processus d'extraction des données. Par exemple, il est souvent plus rapide d'effectuer une recherche dans une colonne indexée que dans une colonne qui ne l'est pas.

Pour des performances optimales, les index de base de données Configuration Manager sont mis à jour fréquemment pour être synchronisés avec les données changeant constamment stockées dans la base de données. Cette tâche permet de créer et de placer des index dans des colonnes de base de données uniques à moins de 50 % et de reconstruire tous les index existants conformes aux critères d'unicité des données.

- **Site d'administration centrale** : non activé
- **Site principal**non activé
- **Site secondaire** : non activé

**Résumer les données du logiciel installé** : cette tâche permet de synthétiser les données de logiciels installés de plusieurs enregistrements en un seul enregistrement général. La synthèse des données permet de compresser la quantité de données stockées dans la base de données Configuration Manager. Pour plus d'informations, consultez Présentation de l'inventaire logiciel dans System Center Configuration Manager.

- Site d'administration centrale : non disponible
- **Site principal** : activé
- Site secondaire : non disponible

**Résumer les données d'utilisation de fichier de contrôle de logiciel** : cette tâche permet de synthétiser les données de plusieurs enregistrements pour l'utilisation de fichier de contrôle logiciel en un seul enregistrement général. La synthèse des données permet de compresser la quantité de données stockées dans la base de données Configuration Manager.

Vous pouvez utiliser cette tâche avec la tâche **Résumer les données d'utilisation mensuelle de contrôle de logiciel** pour synthétiser les données de contrôle de logiciel et pour préserver de l'espace disque dans la base de données Configuration Manager. Pour plus d'informations, consultez Contrôle de logiciel dans System Center Configuration Manager.

- Site d'administration centrale : non disponible
- **Site principal** : activé
- Site secondaire : non disponible

**Résumer les données d'utilisation mensuelle de contrôle de logiciel** : cette tâche permet de synthétiser les données de plusieurs enregistrements pour l'utilisation mensuelle du contrôle de logiciel en un seul enregistrement général. La synthèse des données permet de compresser la quantité de données stockées dans la base de données Configuration Manager.

Vous pouvez utiliser cette tâche avec la tâche **Résumer les données d'utilisation de fichier de contrôle de logiciel** pour synthétiser les données de contrôle de logiciel et pour préserver de l'espace dans la base de données Configuration Manager. Pour plus d'informations, consultez Contrôle de logiciel dans System Center Configuration Manager.

- Site d'administration centrale : non disponible

- **Site principal** : activé
- Site secondaire : non disponible

**Mettre à jour le ciblage disponible de l'application** : cette tâche permet de faire en sorte que Configuration Manager recalcule le mappage des déploiements de stratégies et d'applications aux ressources dans des regroupements. Quand vous déployez une stratégie ou des applications dans un regroupement, Configuration Manager crée un mappage initial entre les objets que vous déployez et les membres du regroupement.

Ces mappages sont stockés dans une table à des fins de référence rapide. Quand l'appartenance à un regroupement change, ces mappages stockés sont mis à jour afin de refléter ces modifications. Toutefois, il est possible que ces mappages soient désynchronisés. Par exemple, si le site ne parvient pas à traiter correctement un fichier de notification, il se peut que cette modification ne soit pas reflétée dans une modification des mappages. Cette tâche actualise ce mappage en fonction de l'appartenance au regroupement actuel.

- Site d'administration centrale : non disponible
- **Site principal** : activé
- Site secondaire : non disponible

**Mettre à jour les tables du catalogue des applications** : cette tâche permet de synchroniser le cache de base de données du site web du catalogue des applications avec les dernières informations sur les applications. Lorsque vous modifiez la configuration de cette tâche de maintenance, la configuration s'applique à tous les sites principaux de la hiérarchie.

- Site d'administration centrale : non disponible
- **Site principal** : activé
- Site secondaire : non disponible

# Modifier votre infrastructure System Center Configuration Manager

22/06/2018 • 39 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Après avoir installé un ou plusieurs sites, vous pouvez être amené à modifier les configurations ou à effectuer des actions qui affectent l'infrastructure que vous avez déployée.

## Gérer le fournisseur SMS

Le fournisseur SMS (fichier de bibliothèque de liens dynamiques smsprov.dll) procure le point de contact administratif pour une ou plusieurs consoles Configuration Manager. Lorsque vous installez plusieurs fournisseurs SMS, vous pouvez fournir une redondance pour l'administration de votre site et hiérarchie par des points de contact.

Sur chaque site Configuration Manager, vous pouvez réexécuter le programme d'installation pour :

- ajouter une instance du fournisseur SMS (chaque instance supplémentaire du fournisseur SMS doit se trouver sur un ordinateur distinct) ;
- supprimer une instance du fournisseur SMS (pour supprimer le dernier fournisseur SMS pour un site, vous devez désinstaller le site).

  Vous pouvez surveiller le processus d'installation ou de suppression du fournisseur SMS en consultant le fichier **ConfigMgrSetup.log** dans le dossier racine du serveur du site sur lequel vous exécutez le programme d'installation.

  Avant de modifier le fournisseur SMS sur un site, familiarisez-vous avec les informations contenues dans Planifier le fournisseur SMS pour System Center Configuration Manager.

**Pour gérer la configuration du fournisseur SMS pour un site**

1. Exécutez **Installation de Configuration Manager** à partir de **<dossier_installation_du_site_Configuration_Manager>\BIN\X64\setup.exe**.
2. Sur la page **Mise en route** , sélectionnez **Effectuer une maintenance de site ou réinitialiser ce site**, puis cliquez sur **Suivant**.
3. Sur la page **Maintenance de site** , sélectionnez **Modifier la configuration du fournisseur SMS**, puis cliquez sur **Suivant**.
4. Sur la page **Gérer les fournisseurs SMS** , sélectionnez l'une des options suivantes et effectuez toutes les étapes de l'Assistant comme indiqué :

   - Pour ajouter un fournisseur SMS supplémentaires sur ce site :

     Sélectionnez **Ajouter un nouveau fournisseur SMS**, spécifiez le nom de domaine complet d'un ordinateur qui hébergera le fournisseur SMS mais qui n'héberge aucun fournisseur SMS actuellement, puis cliquez sur **Suivant**.

   - Pour supprimer un fournisseur SMS d'un serveur :

     Sélectionnez **Désinstaller le fournisseur SMS spécifié**, sélectionnez le nom de l'ordinateur dont vous souhaitez supprimer le fournisseur SMS, cliquez sur **Suivant**, puis confirmez l'action.

> **TIP**
> Pour déplacer le fournisseur SMS entre deux ordinateurs, vous devez installer le fournisseur SMS sur le nouvel ordinateur et supprimer le fournisseur SMS de l'emplacement d'origine. Il n'existe aucune option spéciale pour déplacer le fournisseur SMS entre les ordinateurs en un seul processus.

Une fois toutes les étapes de l'Assistant Installation effectuées, la configuration du fournisseur SMS est terminée. Dans l'onglet **Général** dans la boîte de dialogue **Propriétés** du site, vous pouvez vérifier les ordinateurs disposant d'un fournisseur SMS installé pour un site.

# Gérer la console Configuration Manager

Voici les tâches que vous pouvez effectuer pour gérer la console Configuration Manager :

- **Modifier la langue qui s'affiche dans la console Configuration Manager** – Pour modifier les langues installées, consultez Gérer la langue de la console Configuration Manager dans cette rubrique.
- **Installer d'autres consoles** – Pour installer des consoles supplémentaires, consultez Installer des consoles System Center Configuration Manager.
- **Configurer DCOM** – Pour configurer une autorisation DCOM pour permettre aux consoles distantes du serveur de site de se connecter, consultez Configurer les autorisations DCOM pour les consoles Configuration Manager distantes dans cette rubrique.
- **Modifier les autorisations pour limiter ce que voient les utilisateurs administratifs dans la console** – Pour modifier les autorisations d'administration qui limitent ce que les utilisateurs peuvent voir et faire dans la console, consultez Modifier l'étendue administrative d'un utilisateur administratif.

**Gérer la langue de la console Configuration Manager**

Lors de l'installation du serveur de site, les fichiers d'installation de la console Configuration Manager et les modules linguistiques pris en charge pour le site sont copiés dans le sous-dossier **<chemin_installation_Configuration_Manager>\Tools\ConsoleSetup** du serveur de site.

- Quand vous démarrez l'installation de la console Configuration Manager à partir de ce dossier sur le serveur de site, les fichiers de la console Configuration Manager et du module linguistique pris en charge sont copiés sur l'ordinateur.
- Si le module linguistique correspondant au paramètre de langue défini sur l'ordinateur est disponible, la console Configuration Manager s'ouvre dans cette langue.
- Si le module linguistique associé n'est pas disponible pour la console Configuration Manager, la console s'ouvre en anglais.

Par exemple, considérez un scénario dans lequel vous installez la console Configuration Manager à partir d'un serveur de site prenant en charge l'anglais, l'allemand et le français. Si vous ouvrez la console Configuration Manager sur un ordinateur avec un paramètre de langue configuré pour le français, la console s'ouvre en français. Par contre, si vous ouvrez la console Configuration Manager sur un ordinateur avec un paramètre de langue configuré pour le japonais, la console s'ouvre en anglais, car le module linguistique japonais n'est pas disponible.

Chaque fois que la console Configuration Manager s'ouvre, les paramètres configurés pour la langue de l'ordinateur sont déterminés, la disponibilité d'un module linguistique associé pour la console Configuration Manager est vérifiée et le module linguistique correspondant est utilisé. Si vous voulez ouvrir la console Configuration Manager en anglais sans tenir compte des paramètres de langue configurés sur l'ordinateur, vous devez supprimer ou renommer manuellement les fichiers du module linguistique sur l'ordinateur.

Utilisez les procédures suivantes pour démarrer la console Configuration Manager en anglais quels que soient les paramètres régionaux configurés sur l'ordinateur.

#### Pour installer une version en anglais uniquement de la console Configuration Manager sur des ordinateurs

1. Dans l'Explorateur Windows, accédez à **<chemin_installation_Configuration_Manager>\Tools\ConsoleSetup\LanguagePack**.
2. Renommez les fichiers **.msp** et **.mst** . Par exemple, vous pouvez remplacer **<nom_fichier>.MSP** par **<nom_fichier>.MSP.disabled**.
3. Installez la console Configuration Manager sur l'ordinateur.

> **IMPORTANT**
> Une fois les nouvelles langues de serveur configurées pour le serveur de site, les fichiers .msp et .mst sont recopiés dans le dossier **LanguagePack**. Vous devez répéter cette procédure pour installer de nouvelles consoles Configuration Manager en anglais uniquement.

#### Pour désactiver temporairement la langue d'une console sur une installation existante de la console Configuration Manager

1. Sur l'ordinateur qui exécute la console Configuration Manager, fermez la console Configuration Manager.
2. Dans l'Explorateur Windows, accédez à <*chemin_installation_console*>\Bin\ sur l'ordinateur de la console Configuration Manager.
3. Renommez le dossier de langue approprié selon la langue configurée sur l'ordinateur. Par exemple, si les paramètres de langue pour l'ordinateur sont configurés pour l'allemand, renommez le dossier **de** , **de.disabled**.
4. Pour ouvrir la console Configuration Manager dans la langue configurée pour l'ordinateur, rétablissez le nom d'origine du dossier. Par exemple, renommez **de.disabled** , **de**.

## Configurer les autorisations DCOM pour les consoles Configuration Manager distantes

Le compte d'utilisateur exécutant la console Configuration Manager exige des autorisations pour accéder à la base de données de site par le biais du fournisseur SMS. Toutefois, chaque utilisateur administratif qui utilise une console Configuration Manager distante doit posséder également des autorisations DCOM d'**activation à distance** sur :

- L'ordinateur de serveur de site ;
- chaque ordinateur qui héberge une instance du fournisseur SMS.

  Le groupe de sécurité nommé **Administrateurs SMS** accorde des autorisations d'accès au fournisseur SMS sur un ordinateur et permet également d'accorder les autorisations DCOM requises. (Quand le fournisseur SMS s'exécute sur un serveur membre, il s'agit d'un groupe local dans l'ordinateur. Quand le fournisseur SMS s'exécute sur un contrôleur de domaine, il s'agit d'un groupe de domaine local.)

> **IMPORTANT**
> La console Configuration Manager utilise WMI (Windows Management Instrumentation) pour se connecter au fournisseur SMS, et WMI utilise DCOM en interne. Par conséquent, lorsque la console Configuration Manager est exécutée sur un ordinateur autre que le fournisseur SMS, Configuration Manager exige des autorisations pour activer un serveur DCOM sur l'ordinateur fournisseur SMS. Par défaut, l'activation à distance est accordée uniquement aux membres du groupe Administrateurs intégré. Accorder une autorisation d'activation à distance au groupe Administrateurs SMS reviendrait à permettre à un membre de ce groupe d'effectuer des attaques DCOM à l'encontre de l'ordinateur du fournisseur SMS. La surface d'attaque de l'ordinateur s'en trouverait également augmentée. Vous pouvez réduire l'étendue de cette menace en surveillant attentivement les membres du groupe Administrateurs SMS.

Utilisez la procédure ci-après pour configurer chaque site d'administration centrale, serveur de site principal et ordinateur sur lequel est installé le fournisseur SMS pour accorder l'accès à distance à la console Configuration Manager aux utilisateurs administratifs.

**Pour configurer des autorisations DCOM pour les connexions à distance à la console Configuration Manager**

1. Ouvrez **Services de composants** en exécutant **Dcomcnfg.exe**.
2. Dans **Services de composants**, cliquez sur **Racine de la console** > **Services de composants** > **Ordinateurs**, puis cliquez sur **Poste de travail**. Dans le menu **Action** , cliquez sur **Propriétés**.
3. Dans la boîte de dialogue **Propriétés du poste de travail** , sous l'onglet **Sécurité COM** , dans la section **Autorisations d'exécution et d'activation** , cliquez sur **Modifier les limites**.
4. Dans la boîte de dialogue **Autorisations d'exécution et d'activation** , cliquez sur **Ajouter**.
5. Dans la boîte de dialogue **Sélectionner Utilisateur, ordinateurs, comptes de service ou groupes** , dans la zone **Entrez les noms d'objets à sélectionner (exemples)** , tapez **SMS Admins**, puis cliquez sur **OK**.

   > **NOTE**
   > Vous devrez peut-être modifier la valeur du paramètre de **À partir de cet emplacement** pour localiser le groupe Administrateurs SMS. Lorsque le fournisseur SMS s'exécute sur un serveur membre, il s'agit d'un groupe local dans l'ordinateur. Lorsque le fournisseur SMS s'exécute sur un contrôleur de domaine, il s'agit d'un groupe de domaine local.

6. Dans la section **Autorisations pour les administrateurs SMS** , sélectionnez la case à cocher **Activation à distance** pour autoriser l'activation à distance.
7. Cliquez sur **OK** , cliquez de nouveau sur **OK** , puis fermez **Gestion de l'ordinateur**. Votre ordinateur est maintenant configuré pour autoriser l'accès à distance à la console Configuration Manager aux membres du groupe Administrateurs SMS.

   Répétez cette procédure sur chaque ordinateur de fournisseur SMS pouvant prendre en charge les consoles Configuration Manager à distance.

## Modifier la configuration de base de données de site

Après avoir installé un site, vous pouvez modifier la configuration de la base de données de site et le serveur de base de données de site en exécutant l'installation sur un serveur de site d'administration centrale ou un serveur de site principal. Vous pouvez déplacer la base de données de site vers une nouvelle instance de SQL Server sur le même ordinateur ou vers un autre ordinateur exécutant une version de SQL Server prise en charge. Ces modifications et les modifications associées ne sont pas prises en charge pour la configuration de base de données sur des sites secondaires.

Pour plus d'informations sur les limites de prise en charge, consultez Support policy for manual database changes in a Configuration Manager environment.

> **NOTE**
> Lorsque vous modifiez la configuration de la base de données pour un site, Configuration Manager redémarre ou réinstalle les services Configuration Manager sur le serveur de site et les serveurs de système de site distants qui communiquent avec la base de données.

**Pour modifier la configuration de la base de données**, vous devez exécuter le programme d'installation sur le serveur de site, puis sélectionner l'option **Effectuer une maintenance de site ou réinitialiser ce site**. Ensuite, sélectionnez l'option **Modifier la configuration de SQL Server** . Vous pouvez modifier les configurations de base de données de site suivantes :

- Le serveur Windows qui héberge la base de données.
- L'instance de SQL Server en cours d'utilisation sur un serveur qui héberge la base de données SQL Server.
- Nom de la base de données.
- Port SQL Server utilisé par Configuration Manager
- Port SQL Server Service Broker utilisé par Configuration Manager

**Si vous déplacez la base de données de site, vous devez configurer les éléments suivants :**

- **Configurer l'accès :** quand vous déplacez la base de données de site vers un nouvel ordinateur, ajoutez le compte d'ordinateur du serveur de site au groupe **Administrateurs locaux** sur l'ordinateur exécutant SQL Server. Si vous utilisez un cluster SQL Server pour la base de données de site, vous devez ajouter le compte d'ordinateur au groupe **Administrateurs locaux** de chaque ordinateur du nœud de cluster Windows Server.
- **Activer l'intégration du CLR (Common Language Runtime) :** quand vous déplacez la base de données vers une nouvelle instance de SQL Server ou vers un nouvel ordinateur SQL Server, vous devez activer l'intégration du CLR. Pour activer le CLR, utilisez **SQL Server Management Studio** pour vous connecter à l'instance de SQL Server qui héberge la base de données de site, puis exécutez la procédure stockée suivante en tant que requête : **sp_configure 'clr enabled',1; reconfigure**.
- **Garantir que le nouvel ordinateur SQL Server a accès à l'emplacement de sauvegarde :** quand vous utilisez un chemin UNC pour le stockage de la sauvegarde de la base de données de site, après avoir déplacé la base de données vers un nouveau serveur, dont un déplacement vers un groupe de disponibilité SQL Server AlwaysOn ou un cluster SQL Server, vérifiez que le compte d'ordinateur du nouvel ordinateur SQL Server a des autorisations en **écriture** sur l'emplacement UNC.

> **IMPORTANT**
> Avant de déplacer une base de données possédant un ou plusieurs réplicas de base de données de points de gestion, vous devez supprimer les réplicas de base de données. Une fois la base de données déplacée, vous pouvez reconfigurer les réplicas de base de données. Pour plus d'informations, consultez Database replicas for management points for System Center Configuration Manager.

## Gérer le SPN pour le serveur de base de données de site

Vous pouvez choisir le compte exécutant les services SQL pour la base de données du site :

- Quand les services s'exécutent avec le compte système d'ordinateurs, le SPN est enregistré automatiquement pour vous.
- Quand les services s'exécutent avec un compte d'utilisateur local de domaine, vous devez enregistrer manuellement le SPN pour vous assurer que les clients SQL et autre système de site peuvent effectuer l'authentification Kerberos. Sans l'authentification Kerberos, la communication avec la base de données peut échouer.

La documentation de SQL Server peut vous aider à enregistrer manuellement le SPNet fournit des informations supplémentaires sur les SPN et les connexions Kerberos.

> **IMPORTANT**
> - Quand vous créez un SPN pour un serveur SQL Server en cluster, vous devez spécifier le nom virtuel du cluster SQL Server comme nom d'ordinateur SQL Server.
>   - La commande permettant d'enregistrer un SPN pour une instance nommée de SQL Server est la même que celle utilisée pour l'enregistrement du SPN d'une instance par défaut, la seule différence étant que le numéro de port doit correspondre au port utilisé par l'instance nommée.

Vous pouvez enregistrer un SPN pour le compte de service SQL Server du serveur de base de données de site à l'aide de l'outil **Setspn** . Vous devez exécuter l'outil Setspn sur un ordinateur qui réside dans le domaine de SQL Server et qui doit utiliser les informations d'identification de l'administrateur de domaine pour pouvoir l'exécuter.

Les procédures suivantes sont des exemples de gestion de SPN pour le compte de service SQL Server qui utilise l'outil Setspn sur Windows Server 2008 R2. Pour obtenir des instructions spécifiques à propos de Setspn, voir Présentation de Setspnou une documentation similaire, spécifique à votre système d'exploitation.

> **NOTE**
> Les procédures suivantes font référence à l'outil en ligne de commande Setspn. L'outil en ligne de commande Setspn est inclus lorsque vous installez les outils de support Windows Server 2003 à partir du CD du produit ou depuis le Centre de téléchargement Microsoft. Pour plus d'informations sur l'installation des outils de support Windows à partir du CD du produit, voir Installer des outils de support Windows.

**Pour créer manuellement un nom principal de service (SPN) d'utilisateur de domaine pour le compte du service SQL Server**

1. Dans le menu **Démarrer** , cliquez sur **Exécuter**et entrez **cmd** dans la boîte de dialogue Exécuter.
2. Sur la ligne de commande, accédez au répertoire d'installation des outils de support de Windows Server. Par défaut, ces outils se trouvent dans le répertoire **C:\Program Files\Support Tools** .
3. Entrez une commande valide pour créer le SPN. Pour créer le SPN, vous pouvez utiliser le nom NetBIOS ou le nom de domaine complet (FQDN) de l'ordinateur exécutant SQL Server. Toutefois, vous devez créer un SPN pour le nom NetBIOS et le nom de domaine complet.

   > **IMPORTANT**
   > Lorsque vous créez un SPN pour un SQL Server en cluster, vous devez spécifier le nom virtuel du cluster SQL Server comme nom d'ordinateur SQL Server.

   - Pour créer un SPN pour le nom NetBIOS de l'ordinateur SQL Server, tapez la commande suivante : **setspn -A MSSQLSvc/<nom_ordinateur_SQL_Server>:1433 <Domaine\Compte>**
   - Pour créer un SPN pour le nom de domaine complet de l'ordinateur SQL Server, tapez la

commande suivante : **setspn -A MSSQLSvc/<nom_de_domaine_complet_SQL_Server>:1433 <Domaine\Compte**

> **NOTE**
> La commande permettant d'enregistrer un SPN pour une instance nommée de SQL Server est la même que celle utilisée pour l'enregistrement du SPN d'une instance par défaut, sauf que le numéro de port doit correspondre au port utilisé par l'instance nommée.

**Pour vérifier si le SPN d'utilisateur de domaine est inscrit correctement en utilisant la commande Setspn**

1. Dans le menu **Démarrer** , cliquez sur **Exécuter**et entrez **cmd** dans la boîte de dialogue **Exécuter** .
2. À l'invite de commandes, entrez la commande suivante : **setspn -L <domaine\compte_de_service_SQL>**.
3. Examinez le **Nom principal de service** inscrit pour vous assurer qu'un SPN valide a été créé pour SQL Server.

**Pour vérifier que le SPN d'utilisateur de domaine est enregistré correctement lors de l'utilisation de la console MMC ADSIEdit**

1. Dans le menu **Démarrer** , cliquez sur **Exécuter**, puis entrez **adsiedit.msc** pour démarrer la console MMC ADSIEdit.
2. Si nécessaire, connectez-vous au domaine du serveur de site.
3. Dans le volet de la console, développez le domaine du serveur de site, développez **DC=<nom_serveur_unique>**, développez **CN=Users**, cliquez avec le bouton droit sur **CN=<utilisateur_compte_de_service>**, puis cliquez sur **Propriétés**.
4. Dans la boîte de dialogue **Propriétés CN=<utilisateur_compte_de_service>**, consultez la valeur de **servicePrincipalName** pour vérifier qu'un SPN valide a été créé et associé à l'ordinateur SQL Server approprié.

**Pour indiquer un compte d'utilisateur de domaine à la place du système local comme compte du service SQL Server**

1. Créez ou sélectionnez un compte d'utilisateur de domaine ou de système local en tant que compte du service SQL Server.
2. Ouvrez le **Gestionnaire de configuration SQL Server**.
3. Cliquez sur **Services SQL Server**, puis double-cliquez sur **SQL Server<NOM_INSTANCE>**.
4. Dans l'onglet **Ouvrir une session** , sélectionnez **Ce compte**et entrez le nom et le mot de passe du compte d'utilisateur de domaine créé à l'étape 1. Vous pouvez également cliquer sur **Parcourir** pour rechercher le compte d'utilisateur dans les services de domaine Active Directory, puis cliquer sur **Appliquer**.
5. Cliquez sur **Oui** dans la boîte de dialogue **Confirmer la modification du compte** pour confirmer le changement de compte de service et redémarrer le service SQL Server.
6. Cliquez sur **OK** après modification du compte de service.

## Exécuter une réinitialisation de site

Quand une réinitialisation de site s'exécute sur un site d'administration centrale ou sur un site principal, le site :

- réapplique les autorisations de fichiers et de Registre Configuration Manager par défaut ;
- réinstalle tous les composants de site et tous les rôles de système de site sur le site.

Les sites secondaires ne prennent pas en charge la réinitialisation du site.

Les réinitialisations de site peuvent être exécutées manuellement, quand vous le souhaitez, mais peuvent également s'exécuter automatiquement une fois que vous avez modifié la configuration du site.

Par exemple, si les comptes utilisés par les composants Configuration Manager ont été modifiés, vous devez envisager de réinitialiser le site manuellement ; ainsi mis à jour, les composants de site peuvent utiliser les nouvelles informations de compte. Toutefois, si vous modifiez les langues du client ou du serveur sur un site, Configuration Manager réinitialise automatiquement le site, car cette action est nécessaire avant que le site puisse utiliser cette modification.

> **NOTE**
> La réinitialisation d'un site ne réinitialise pas les autorisations d'accès aux objets non-Configuration Manager.

Quand une réinitialisation de site s'exécute :

1. L'installation s'arrête et redémarre le service **SMS_SITE_COMPONENT_MANAGER** ainsi que les composants de thread du service **SMS_EXECUTIVE** .
2. Le programme d'installation supprime, puis recrée, le dossier partagé du système de site et le composant **SMS Executive** sur l'ordinateur local et sur les ordinateurs de système de site distants.
3. Le programme d'installation redémarre le service **SMS_SITE_COMPONENT_MANAGER** , et ce service installe les services **SMS_EXECUTIVE** et **SMS_SQL_MONITOR** .

La réinitialisation d'un site restaure, également, les objets suivants :

- Les clés de Registre **SMS** ou **NAL** et toutes les sous-clés par défaut dépendant de ces clés.
- L'arborescence du répertoire de fichiers Configuration Manager et tous les fichiers par défaut ou tous les sous-répertoires de cette arborescence du répertoire de fichiers.

**Configuration requise pour exécuter une réinitialisation du site**

Le compte que vous utilisez pour effectuer une réinitialisation du site doit disposer des autorisations suivantes :

- Le compte que vous utilisez pour effectuer une réinitialisation du site doit disposer des autorisations suivantes :
  - **Site d'administration centrale**: le compte que vous utilisez pour réinitialiser un site de ce site doit être un administrateur local situé sur le serveur de site d'administration centrale et doit disposer de privilèges équivalents au rôle de sécurité de l'administration basée sur le rôle **Administrateur complet** .
  - **Site principal**: le compte que vous utilisez pour réinitialiser un site de ce site doit être un administrateur local situé sur le serveur de site principal et doit disposer de privilèges équivalents au rôle de sécurité de l'administration basée sur le rôle **Administrateur complet** . Si le site principal se trouve dans une hiérarchie disposant d'un site d'administration centrale, ce compte doit également être un administrateur local sur le serveur du site d'administration centrale.

**Limitations d'une réinitialisation de site**

- Depuis la version 1602, vous ne pouvez pas utiliser une réinitialisation de site pour modifier les modules linguistiques serveur ou client qui ont été installés sur les sites tant que la hiérarchie est configurée pour prendre en charge les tests des mises à niveau du client dans un regroupement de préproduction.

**Pour effectuer une réinitialisation de site**

1. Exécutez **Installation de Configuration Manager** à partir de **<dossier_installation_du_site_Configuration_Manager>\BIN\X64\setup.exe**.

> **TIP**
> Vous pouvez également exécuter une réinitialisation de site en démarrant le programme d'installation de Configuration Manager dans le menu **Démarrer** de l'ordinateur serveur de site ou depuis le média source Configuration Manager.

2. Sur la page **Mise en route** , sélectionnez **Effectuer une maintenance de site ou réinitialiser ce site**, puis cliquez sur **Suivant**.
3. Sur la page **Maintenance de site** , sélectionnez **Réinitialiser le site sans modification de la configuration**, puis cliquez sur **Suivant**.
4. Cliquez sur **Oui** pour démarrer la réinitialisation du site.

Une fois la réinitialisation du site terminée, cliquez sur **Fermer** pour terminer cette procédure.

## Gérer les modules linguistiques sur un site

Après l'installation d'un site, vous pouvez modifier les modules linguistiques client et serveur en cours d'utilisation :

**Modules linguistiques serveur :**

- **S'applique à :**

  Installations de la console Configuration Manager

  Nouvelles installations de rôles de système de site applicables

- **Détails :**

  Après la mise à jour des modules linguistiques serveur d'un site, vous pouvez ajouter la prise en charge des modules linguistiques dans les consoles Configuration Manager.

  Pour ajouter la prise en charge d'un module linguistique serveur dans une console Configuration Manager, vous devez installer la console Configuration Manager à partir du dossier **ConsoleSetup** d'un serveur de site dans lequel figure le module linguistique que vous souhaitez utiliser. Si la console Configuration Manager est déjà installée, vous devez commencer par la désinstaller, afin de permettre à la nouvelle installation d'identifier la liste actuelle des modules linguistiques pris en charge.

**Modules linguistiques client :**

- **S'applique à :**

  Les modifications apportées aux modules linguistiques client mettent à jour les fichiers sources d'installation du client, pour que les nouvelles installations et mises à niveau de client ajoutent la prise en charge de la liste des langues client mise à jour.

- **Détails :**

  Après la mise à jour des modules linguistique client d'un site, vous devez installer chacun des clients qui utiliseront les modules linguistiques en utilisant les fichiers sources qui incluent les modules linguistiques client.

Pour plus d'informations sur les langues client et serveur prises en charge par Configuration Manager, consultez Modules linguistiques dans System Center Configuration Manager.

#### Pour modifier les modules linguistiques pris en charge par un site

1. Sur le serveur de site, exécutez le programme d'installation de Configuration Manager à partir de

**<dossier_installation_du_site_Configuration_Manager>\BIN\X64\setup.exe**.

2. Sur la page **Mise en route** , sélectionnez **Effectuer une maintenance de site ou réinitialiser ce site**, puis cliquez sur **Suivant**.
3. Sur la page **Maintenance de site** , sélectionnez **Modifier la configuration de la langue**, puis cliquez sur **Suivant**.
4. Sur la page **Téléchargements requis** , sélectionnez **Télécharger les fichiers requis** pour acquérir des mises à jour de modules linguistiques ou **Utiliser des fichiers précédemment téléchargés** pour utiliser les fichiers précédemment téléchargés incluant les modules linguistiques que vous souhaitez ajouter au site. Cliquez sur **Suivant** pour valider les fichiers et continuer.
5. Sur la page **Sélection de la langue du serveur** , activez les cases à cocher correspondant aux langues serveur prises en charge par ce site, puis cliquez sur **Suivant**.
6. Sur la page **Sélection de la langue client** , activez les cases à cocher correspondant aux langues client prises en charge par ce site, puis cliquez sur **Suivant**.
7. Cliquez sur **Suivant**pour modifier les langues prises en charge au niveau du site.

   > **NOTE**
   > Configuration Manager lance une réinitialisation de site qui réinstalle également tous les rôles de système de site au niveau du site.

8. Cliquez sur **Fermer** pour terminer cette procédure.

## Modifier le seuil d'alerte du serveur de base de données

Par défaut, Configuration Manager génère des alertes lorsque l'espace disque libre sur un serveur de base de données de site est faible. Les valeurs par défaut sont définies pour générer un avertissement lorsque l'espace disque libre est de 10 Go ou moins et une alerte critique lorsque l'espace disque libre est de 5 Go ou moins. Vous pouvez modifier ces valeurs ou désactiver les alertes pour chaque site.

Pour modifier ces paramètres :

1. Dans l'espace de travail **Administration** , développez **Configuration du site**, puis cliquez sur **Sites**.
2. Sélectionnez le site que vous souhaitez configurer et ouvrez les **Propriétés** de ce site.
3. Dans la boîte de dialogue **Propriétés** du site, sélectionnez l'onglet **Alerte**, puis modifiez les paramètres.
4. Cliquez sur **OK** pour fermer la boîte de dialogue des propriétés de site.

# Dossier CD.Latest pour System Center Configuration Manager

22/06/2018 • 7 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

System Center Configuration Manager inaugure un nouveau processus de mise à jour qui permet de remettre les mises à jour du produit à partir de la console Configuration Manager. Pour prendre en charge cette nouvelle méthode de mise à jour de Configuration Manager, un nouveau dossier est créé sous le nom **CD.Latest** : il contient une copie des fichiers d'installation de Configuration Manager pour la version mise à jour de votre site.

Le dossier CD.Latest contient un dossier nommé **Redist** dans lequel se trouvent les fichiers redistribuables téléchargés et utilisés par le programme d'installation. Ces fichiers sont mis en correspondance avec la version des fichiers de Configuration Manager dans ce dossier CD.Latest. Quand vous exécutez le programme d'installation à partir d'un dossier CD.Latest, vous devez utiliser les fichiers qui correspondent à cette version du programme d'installation. Pour ce faire, vous pouvez faire en sorte que le programme d'installation télécharge les fichiers nouveaux et existants à partir de Microsoft, ou faire en sorte qu'il utilise les fichiers présents dans le dossier Redist du dossier CD.Latest.

Toutefois, le support de base de référence, comme la version de base de référence 1802 publiée en mars 2018, ne comprend pas de dossier Redist. Le dossier Redist n'est créé qu'au terme de l'installation d'une mise à jour dans la console. En attendant, utilisez le dossier Redist auquel vous avez eu recours lors de l'installation de sites à partir du média de base de référence.

> **TIP**
> Veillez à utiliser la dernière version des fichiers redistribuables. Si vous n'avez pas téléchargé les fichiers redistribuables les plus récents, autorisez le programme d'installation à le faire à partir du site web de Microsoft.

Vous trouverez ci-dessous des scénarios permettant de créer ou de mettre à jour le dossier CD.Latest sur un serveur de site d'administration centrale ou de site principal :

- Vous installez une mise à jour ou un correctif logiciel à partir de la console Configuration Manager : le dossier est créé ou mis à jour dans le dossier d'installation de Configuration Manager.
- Vous exécutez la tâche de sauvegarde intégrée de Configuration Manager : le dossier est créé ou mis à jour à l'emplacement du dossier de sauvegarde désigné.
- Le dossier CD.Latest est créé quand vous installez un nouveau site en utilisant un support de base de référence (version 1802, par exemple).

Les fichiers sources du dossier CD.Latest sont pris en charge pour les opérations suivantes :

1. **Sauvegarde et récupération :** pour récupérer un site, vous devez utiliser les fichiers source d'un dossier CD.Latest correspondant à votre site. Lorsque vous exécutez une sauvegarde de site à l'aide de la tâche de sauvegarde de site intégrée, le dossier CD.Latest est inclus dans le cadre de la sauvegarde.
   - **Quand vous réinstallez le site dans le cadre d'une récupération de site** , vous installez le site à partir du dossier CD.Latest inclus dans votre sauvegarde. Cette opération installe le site à l'aide des versions de fichier correspondant à la sauvegarde et à la base de données de votre site. Si vous n'avez pas accès à la version appropriée du dossier CD.Latest, vous pouvez obtenir un dossier

CD.Latest avec les versions de fichiers appropriées en installant un site dans un environnement de laboratoire, puis en mettant à jour ce site afin qu'il corresponde à la version que vous souhaitez récupérer.

> **IMPORTANT**
> Si le dossier CD.Latest approprié et son contenu ne sont pas disponibles, vous ne pouvez pas récupérer un site et devez le réinstaller.

- Lorsque vous n'avez pas de dossier CD.Latest mais disposez d'un site principal enfant ou d'un site d'administration centrale opérationnels, vous pouvez utiliser ce site en tant que site de référence pour la récupération d'un site.

2. **Pour installer un site principal enfant :** quand vous souhaitez installer un nouveau site principal enfant sous un site d'administration centrale qui a installé une ou plusieurs mises à jour dans la console, vous devez utiliser le programme d'installation et les fichiers sources figurant dans le dossier CD.Latest du site d'administration centrale. Lorsque le programme d'installation s'exécute à partir d'une copie du dossier CD.Latest figurant sur le site d'administration centrale, il utilise les fichiers sources d'installation correspondant à la version du site d'administration centrale. Pour plus d'informations, consultez Utiliser l'Assistant Installation pour installer des sites.

3. **Pour étendre un site principal autonome :** quand vous étendez un site principal autonome en installant un nouveau site d'administration centrale, vous devez utiliser le programme d'installation et les fichiers sources figurant dans le dossier CD.Latest du site principal pour installer le nouveau site d'administration centrale. Lorsque vous exécutez à partir d'une copie du dossier CD.Latest du site principal, les fichiers sources d'installation utilisés correspondent à la version du site principal. Pour plus d'informations, consultez Étendre un site principal autonome) dans Utiliser l'Assistant Installation pour installer des sites.

> **IMPORTANT**
> Les fichiers sources mis à jour du dossier CD.Latest ne sont pas pris en charge pour les opérations suivantes :
>
> - installation d'un nouveau site pour une nouvelle hiérarchie ;
> - Mise à niveau d'un site Microsoft System Center 2012 Configuration Manager vers System Center Configuration Manager
> - Installation du client Configuration Manager
> - Installation de la console d'administration Configuration Manager

# Mettre à niveau l'infrastructure locale qui prend en charge System Center Configuration Manager

26/06/2018 • 19 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez les informations de cet article pour mettre à niveau l'infrastructure de serveur qui exécute Configuration Manager.

- Si vous voulez effectuer la *mise à niveau* à partir d'une version antérieure de Configuration Manager vers System Center Configuration Manager, Current Branch, consultez Mettre à niveau vers System Center Configuration Manager.
- Si vous voulez *mettre à jour* votre infrastructure System Center Configuration Manager, Current Branch, vers une nouvelle version, consultez Mises à jour pour System Center Configuration Manager.

## Mettre à niveau le système d'exploitation des systèmes de site

Configuration Manager prend en charge la mise à niveau sur place du système d'exploitation de serveurs qui hébergent un serveur de site et des serveurs distants hébergeant un rôle de système de site, dans les situations suivantes :

- Mise à niveau sur place vers un Service Pack Windows Server ultérieur si le niveau du Service Pack de Windows résultant est pris en charge par Configuration Manager.
- Mise à niveau sur place à partir de :
  - Windows Server 2012 R2 vers Windows Server 2016 (afficher des informations supplémentaires).
  - Windows Server 2012 vers Windows Server 2016 (afficher des informations supplémentaires).
  - Windows Server 2012 vers Windows Server 2012 R2 (afficher des informations supplémentaires).
  - Windows Server 2008 R2 vers Windows Server 2012 R2 (afficher des informations supplémentaires).

> **WARNING**
> Avant d'effectuer une mise à niveau vers un autre système d'exploitation, *vous devez désinstaller WSUS* du serveur. Vous pouvez conserver la base de données SUSDB et l'attacher de nouveau après la réinstallation de WSUS. Pour plus d'informations sur cette étape critique, consultez la section Fonctionnalités nouvelles et modifiées de la rubrique Vue d'ensemble des services WSUS (Windows Server Update Services) dans la documentation de Windows Server.

Pour mettre à niveau un serveur, utilisez les procédures de mise à niveau fournies par le système d'exploitation vers lequel vous effectuez la mise à niveau. Consultez les articles suivants :

- Options de mise à niveau pour Windows Server 2012 R2 dans la documentation de Windows Server.
- Options de mise à niveau et de conversion pour Windows Server 2016 dans la documentation de Windows Server.

#### Mise à niveau de Windows Server 2012 ou Windows Server 2012 R2 vers la version 2016

Lorsque vous mettez à niveau Windows Server 2012 ou Windows Server 2012 R2 vers Windows Server 2016, ce qui suit s'applique :

##### Avant la mise à niveau

- Supprimez le client SCEP (System Center Endpoint Protection). Windows Defender, qui remplace le client SCEP,

est intégré à Windows Server 2016. La présence du client SCEP peut empêcher une mise à niveau vers Windows Server 2016.

- Supprimez le rôle WSUS du serveur, s'il est installé. Vous pouvez conserver la base de données SUSDB et l'attacher de nouveau après la réinstallation de WSUS.

#### Après la mise à niveau

- Vérifiez que Windows Defender est activé, configuré pour démarrer automatiquement et en cours d'exécution.
- Vérifiez que les services Configuration Manager suivants sont en cours d'exécution :
  - SMS_EXECUTIVE
  - SMS_SITE_COMPONENT_MANAGER
- Vérifiez que le **service d'activation des processus Windows** et le **service WWW/W3SVC** sont activés, configurés pour démarrer automatiquement et en cours d'exécution pour les rôles de système de site suivants (ces services sont désactivés pendant la mise à niveau) :
  - Serveur de site
  - Point de gestion
  - Point de service web du catalogue des applications
  - Point du site web du catalogue des applications
- Vérifiez que chaque serveur qui héberge un rôle de système de site respecte l'ensemble des prérequis pour les rôles de système de site qui s'exécutent sur ce serveur. Par exemple, il se peut que vous deviez réinstaller le service BITS ou le service WSUS, ou de configurer des paramètres spécifiques pour IIS.
- Après avoir restauré les prérequis manquants, redémarrez le serveur une fois de plus pour être sûr que les services sont démarrés et en cours d'exécution.
- Si vous mettez à niveau le serveur de site principal, exécutez une réinitialisation du site.

#### Problème connu lié aux consoles Configuration Manager distantes

Une fois la mise à niveau du serveur de site ou d'un serveur qui héberge une instance de SMS_Provider vers Windows Server 2016 effectuée, il se peut que les utilisateurs administratifs ne puissent pas connecter une console Configuration Manager au site. Pour contourner ce problème, vous devez restaurer manuellement les autorisations pour le groupe Administrateurs SMS dans WMI. Les autorisations doivent être définies sur le serveur de site, ainsi que sur chaque serveur distant qui héberge une instance de SMS_Provider :

1. Sur les serveurs applicables, ouvrez la console MMC (Microsoft Management Console) et ajoutez le composant logiciel enfichable pour le **Contrôle WMI**, puis sélectionnez **Ordinateur local**.
2. Dans la console MMC, ouvrez les **Propriétés** du **Contrôle WMI (local)**, puis sélectionnez l'onglet **Sécurité**.
3. Développez l'arborescence sous la racine, sélectionnez le nœud **SMS**, puis choisissez **Sécurité**. Vérifiez que le groupe **Administrateurs SMS** dispose des autorisations suivantes :
   - Activer le compte
   - Appel à distance autorisé
4. Dans **l'onglet Sécurité** sous le nœud **SMS**, sélectionnez le nœud **site_<sitecode>**, puis choisissez **Sécurité**. Vérifiez que le groupe **Administrateurs SMS** dispose des autorisations suivantes :
   - Méthodes d'exécution
   - Écriture fournisseur
   - Activer le compte
   - Appel à distance autorisé
5. Enregistrez les autorisations pour restaurer l'accès à la console Configuration Manager.

### Windows Server 2012 vers Windows Server 2012 R2

#### Avant la mise à niveau

- Supprimez le rôle WSUS du serveur, s'il est installé. Vous pouvez conserver la base de données SUSDB et

l'attacher de nouveau après la réinstallation de WSUS.

#### Après la mise à niveau

- Vérifiez que le service de déploiement Windows est démarré et en cours d'exécution pour les rôles de système de site suivants (ce service est arrêté pendant la mise à niveau) :
  - Serveur de site
  - Point de gestion
  - Point de service web du catalogue des applications
  - Point du site web du catalogue des applications
- Vérifiez que le **service d'activation des processus Windows** et le **service WWW/W3SVC** sont activés, configurés pour démarrer automatiquement et en cours d'exécution pour les rôles de système de site suivants (ces services sont désactivés pendant la mise à niveau) :
  - Serveur de site
  - Point de gestion
  - Point de service web du catalogue des applications
  - Point du site web du catalogue des applications
- Vérifiez que chaque serveur qui héberge un rôle de système de site respecte l'ensemble des prérequis pour les rôles de système de site qui s'exécutent sur ce serveur. Par exemple, il se peut que vous deviez réinstaller le service BITS ou le service WSUS, ou de configurer des paramètres spécifiques pour IIS.

  Après avoir restauré les prérequis manquants, redémarrez le serveur une fois de plus pour être sûr que les services sont démarrés et en cours d'exécution.

### Mise à niveau de Windows Server 2008 R2 vers Windows Server 2012 R2

Ce scénario de mise à niveau du système d'exploitation a les conditions suivantes :

#### Avant la mise à niveau

- Désinstallez WSUS 3.2.
  Avant de mettre à niveau le système d'exploitation d'un serveur vers Windows Server 2012 R2, vous devez désinstaller WSUS 3.2 du serveur. Pour plus d'informations sur cette étape critique, consultez la section Fonctionnalités nouvelles et modifiées de la rubrique Vue d'ensemble des services WSUS (Windows Server Update Services) dans la documentation de Windows Server.

#### Après la mise à niveau

- Vérifiez que le service de déploiement Windows est démarré et en cours d'exécution pour les rôles de système de site suivants (ce service est arrêté pendant la mise à niveau) :
  - Serveur de site
  - Point de gestion
  - Point de service web du catalogue des applications
  - Point du site web du catalogue des applications
- Vérifiez que le **service d'activation des processus Windows** et le **service WWW/W3SVC** sont activés, configurés pour démarrer automatiquement et en cours d'exécution pour les rôles de système de site suivants (ces services sont désactivés pendant la mise à niveau) :
  - Serveur de site
  - Point de gestion
  - Point de service web du catalogue des applications
  - Point du site web du catalogue des applications
- Vérifiez que chaque serveur qui héberge un rôle de système de site respecte l'ensemble de la configuration requise pour les rôles de système de site qui s'exécutent sur ce serveur. Par exemple, il se peut que vous deviez réinstaller le service BITS ou le service WSUS, ou de configurer des paramètres spécifiques pour IIS.

Après avoir restauré les prérequis manquants, redémarrez le serveur une fois de plus pour être sûr que les services sont démarrés et en cours d'exécution.

**Scénarios de mise à niveau non pris en charge**

Les scénarios de mise à niveau de Windows Server suivants font souvent l'objet de questions, mais ils ne sont pas pris en charge par Configuration Manager :

- Windows Server 2008 vers Windows Server 2012 ou version ultérieure
- Windows Server 2008 R2 vers Windows Server 2012

## Mettre à niveau le système d'exploitation de clients Configuration Manager

Configuration Manager prend en charge une mise à niveau sur place du système d'exploitation pour les clients Configuration Manager dans les situations suivantes :

- La mise à niveau sur place vers un Service Pack Windows ultérieur si le niveau du Service Pack résultant est pris en charge par Configuration Manager.
- Mise à niveau sur place de Windows à partir d'une version prise en charge vers Windows 10. Pour plus d'informations, consultez Effectuer une mise à niveau de Windows vers la dernière version.
- Mises à niveau de la maintenance de build à build de Windows 10. Pour plus d'informations, consultez Gérer Windows as a service.

## Mettre à niveau SQL Server sur le serveur de base de données de site

Configuration Manager prend en charge une mise à niveau sur place de SQL Server à partir d'une version prise en charge de SQL sur le serveur de base de données de site. Les scénarios de mise à niveau de SQL Server décrits dans cette section sont pris en charge par Configuration Manager et incluent la configuration requise pour chaque scénario.

Pour plus d'informations sur les versions de SQL Server prises en charge par Configuration Manager, consultez Prise en charge des versions de SQL Server.

**Mise à niveau de la version du Service Pack de SQL Server**

Configuration Manager prend en charge la mise à niveau sur place de SQL Server vers un Service Pack ultérieur si le niveau du Service Pack SQL Server résultant est pris en charge par Configuration Manager.

Si vous utilisez plusieurs sites Configuration Manager dans une hiérarchie, chaque site peut exécuter une version différente du Service Pack de SQL Server. Il n'existe pas de limitation quant à l'ordre dans lequel les sites effectuent une à niveau de la version du Service Pack de SQL Server utilisé pour la base de données de site.

**Mise à niveau vers une nouvelle version de SQL Server**

Configuration Manager prend en charge la mise à niveau sur place de SQL Server vers les versions suivantes :

- SQL Server 2017
- SQL Server 2016
- SQL Server 2014

Quand vous mettez à niveau la version de SQL Server qui héberge la base de données du site, vous devez mettre à niveau la version de SQL Server qui est utilisée sur les sites dans l'ordre suivant :

1. Mettez d'abord à niveau SQL Server sur le site administration centrale.
2. Mettez à niveau les sites secondaires avant de mettre à niveau le site principal parent d'un site secondaire.
3. Mettez à niveau les sites principaux parents en dernier. Ces sites incluent les sites principaux enfants qui

dépendent d'un site d'administration centrale et les sites principaux autonomes qui constituent les sites de plus haut niveau d'une hiérarchie.

**Niveau Estimation de cardinalité SQL Server et base de données de site**

Quand une base de données de site est mise à niveau à partir d'une version antérieure de SQL Server, la base de données conserve son niveau Estimation de cardinalité SQL Server (SQL Server CE) existant s'il est au minimum autorisé pour cette instance de SQL Server. En mettant à niveau SQL Server avec une base de données à un niveau de compatibilité inférieur que celui autorisé automatiquement, vous définissez la base de données sur le niveau de compatibilité le plus bas autorisé par SQL Server.

Le tableau suivant identifie les niveaux de compatibilité recommandés pour les bases de données de site Configuration Manager :

| VERSION SQL SERVER | NIVEAUX DE COMPATIBILITÉ PRIS EN CHARGE | NIVEAU CONSEILLÉ |
|---|---|---|
| SQL Server 2017 | 140, 130, 120, 110 | 140 |
| SQL Server 2016 | 130, 120, 110 | 130 |
| SQL Server 2014 | 120, 110 | 110 |

Pour identifier le niveau de compatibilité SQL Server CE en cours d'utilisation pour votre base de données de site, exécutez la requête SQL suivante sur le serveur de base de données de site :

```
SELECT name, compatibility_level FROM sys.databases
```

Pour plus d'informations sur les niveaux de compatibilité SQL CE et comment les définir, consultez Niveau de compatibilité ALTER DATABASE (Transact-SQL).

Pour plus d'informations sur la mise à niveau de SQL Server, consultez la documentation de SQL Server suivante :

- Mise à niveau vers SQL Server 2017
- Mise à niveau vers SQL Server 2016
- Mise à niveau vers SQL Server 2014

**Pour mettre à niveau SQL Server sur le serveur de base de données de site**

1. Arrêtez tous les services de Configuration Manager sur le site.
2. Mettez à niveau SQL Server vers une version prise en charge.
3. Redémarrez les services de Configuration Manager.

> **NOTE**
> Quand vous changez l'édition de SQL Server utilisée sur le site d'administration centrale d'une édition Standard en une édition Enterprise ou Datacenter, la partition de base de données qui limite le nombre de clients que la hiérarchie prend en charge ne change pas.

# Mises à jour pour System Center Configuration Manager

22/06/2018 • 16 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Configuration Manager utilise une méthode de service dans la console appelée **Mises à jour et maintenance**. Cette méthode dans la console facilite la localisation et l'installation des mises à jour recommandées pour votre infrastructure Configuration Manager. La maintenance dans la console est complétée par des mises à jour hors bande, telles que des correctifs logiciels, qui s'adressent aux clients qui ont besoin de résoudre des problèmes qui peuvent être propres à leur environnement.

> **TIP**
> Les termes *mise à niveau*, *mise à jour* et *installation* sont utilisés pour décrire trois concepts distincts dans Configuration Manager. Pour plus d'informations sur l'utilisation de chaque terme, consultez À propos de la mise à niveau, de la mise à jour et de l'installation.

**Les rubriques suivantes peuvent vous aider à comprendre comment rechercher et installer les différents types de mise à jour pour Configuration Manager :**

- Installer des mises à jour dans la console
- Utiliser l'outil de connexion de service
- Importer des correctifs logiciels avec l'outil Inscription de la mise à jour
- Utiliser le programme d'installation de correctif logiciel pour installer des mises à jour

Pour plus d'informations sur la branche Technical Preview, consultez Technical Preview pour System Center Configuration Manager.

## Versions de base et de mise à jour

La dernière version de base est à utiliser quand il s'agit d'installer un nouveau site dans une nouvelle hiérarchie.

- Utilisez également une version de base de référence pour effectuer la mise à niveau à partir de System Center 2012 Configuration Manager.
- Après la mise à niveau vers la version Current Branch de Configuration Manager, n'utilisez pas les versions de base de référence pour rester à jour. À la place, utilisez uniquement les mises à jour dans la console pour effectuer une mise à jour vers la version la plus récente.
- D'autres versions de base sont publiées régulièrement. Quand vous utilisez la dernière version de base de référence pour installer une nouvelle hiérarchie, cela vous évite d'installer une version obsolète ou non prise en charge de Configuration Manager, suivie d'une mise à niveau supplémentaire de votre infrastructure pour la mettre à jour.

Après avoir installé une version de base, d'autres versions de Configuration Manager sont disponibles sous forme de mises à jour dans la console. Les mises à jour dans la console mettent à jour votre infrastructure vers la dernière version de Configuration Manager.

- L'installation des mises à jour dans la console visent à mettre à jour la version de votre site de niveau supérieur.
- Les mises à jour que vous installez sur le site d'administration centrale s'installent automatiquement sur les sites principaux enfants. Contrôlez cette synchronisation à l'aide d'une fenêtre de maintenance sur le site principal.
- Mettez à jour manuellement les sites secondaires vers une nouvelle version de mise à jour à partir de la console.

Quand vous installez une mise à jour, elle stocke les fichiers d'installation de cette version sur le serveur de site dans un dossier nommé **CD.Latest**. Pour plus d'informations sur ces fichiers, consultez Dossier CD.Latest.

- Utilisez les fichiers du dossier CD.Latest durant la récupération de site. De même, quand votre hiérarchie n'exécute plus de version de base de référence, utilisez ces fichiers pour installer des sites supplémentaires.
- Vous ne pouvez pas vous servir des fichiers d'installation du dossier CD.Latest pour installer le premier site d'une nouvelle hiérarchie, ni pour mettre à niveau un site à partir de System Center 2012 Configuration Manager.

Certaines mises à jour de Configuration Manager sont disponibles à la fois comme version de mise à jour dans la console pour l'infrastructure existante et comme nouvelle version de base.

Les versions suivantes de Configuration Manager sont disponibles sous forme de version de base, de mise à jour ou les deux à la fois :

| VERSION | DATE DE DISPONIBILITÉ | DATE DE FIN DE SUPPORT | DE BASE | MISE À JOUR DANS LA CONSOLE |
|---|---|---|---|---|
| 1802<br>5.00.8634.1000 | 22 mars 2018 | 22 septembre 2019 | Oui | Oui |
| 1710<br>5.00.8577.1000 | 20 novembre 2017 | Mai 20, 2019 | Non | Oui |
| 1706<br>5.00.8540.1000 | 31 juillet 2017 | 31 juillet 2018 | Non | Oui |
| 1702<br>5.00.8498.1000 | 27 mars 2017 | 27 mars 2018 | Oui | Oui |
| 1610<br>5.00.8458.1000 | 18 novembre 2016 | 18 novembre 2017 | Non | Oui |
| 1606<br>5.00.8412.1000 | 22 juillet 2016 | 22 juillet 2017 | Non | Oui |

| VERSION | DATE DE DISPONIBILITÉ | DATE DE FIN DE SUPPORT | DE BASE | MISE À JOUR DANS LA CONSOLE |
|---|---|---|---|---|
| 1606 avec le correctif cumulatif 1606 (KB3186654) 5.00.8412.1307 *(Note 1)* | 12 octobre 2016 | 12 octobre 2017 | Oui | Non |
| 1602<br><br>5.00.8355.1000 | 11 mars 2016 | 11 mars 2017 | Non | Oui |
| 1511<br><br>5.00.8325.1000 | 8 décembre 2015 | 8 décembre 2016 | Oui | Non |

*(Remarque 1)* Le support de la base de référence 1802 est disponible dans les versions suivantes du VLSC (Centre de gestion des licences en volume) :

- System Center Config Mgr (Current Branch)
- System Center 2016 Datacenter
- System Center 2016 Standard. Par exemple, recherchez `System Center Config Mgr (current branch)` dans VLSC. Recherchez le support de la base de référence 1802 dans la liste des fichiers, puis téléchargez-le pour cette version.

Pour vérifier la version de votre site Configuration Manager, en haut à gauche de la console, accédez à **À propos de System Center Configuration Manager**. Cette boîte de dialogue affiche les versions du site et de la console.

> **NOTE**
> À compter de la version 1802, la version de la console est légèrement différente de la version du site. La version mineure de la console correspond maintenant à la version publiée de Configuration Manager. Par exemple, dans Configuration Manager version 1802, la version initiale du site est 5.0.8634.1000, et la version initiale de la console est 5.**1802**.1082.1700. Les numéros de build (1082) et de révision (1700) peuvent changer avec les correctifs logiciels futurs sur la version 1802.

## Mises à jour et maintenance dans la console

Quand vous utilisez une installation Current Branch de System Center Configuration Manager prête pour la production, la plupart des mises à jour sont disponibles via le canal **Mises à jour et maintenance**. Cette méthode identifie, télécharge et met à disposition les mises à jour qui s'appliquent à la version et à la configuration actuelles de votre infrastructure. Elle inclut uniquement les mises à jour que Microsoft recommande à tous les clients.

Ces mises à jour comportent :

- Les nouvelles versions comme la version 1702, 1706, 1710 ou 1802.
- Les mises à jour qui comprennent de nouveaux composants pour votre version actuelle
- Les correctifs logiciels pour votre version de Configuration Manager que tous les clients doivent installer

Les mises à jour dans la console offrent une stabilité accrue et résolvent les problèmes courants. Elles remplacent les types de mise à jour déjà rencontrés pour les versions de produit précédentes, par exemple les

Service Packs, les mises à jour cumulatives, les correctifs logiciels applicables à tous les clients et l'extension pour Microsoft Intune.

Les mises à jour dans la console peuvent s'appliquer à un ou plusieurs des systèmes suivants :

- Serveurs de site principal et d'administration centrale
- Rôles de système de site et serveurs de système de site
- Instances du fournisseur SMS
- Consoles Configuration Manager
- Clients Configuration Manager

Configuration Manager découvre de nouvelles mises à jour pour vous. Synchronisez votre point de connexion de service Configuration Manager avec le service cloud Microsoft, en notant les comportements suivants :

- Quand votre point de connexion de service est en mode en ligne, votre site se synchronise tous les jours avec Microsoft. Il identifie automatiquement les nouvelles mises à jour qui s'appliquent à votre infrastructure. Pour télécharger les mises à jour et les fichiers redistribuables, l'ordinateur qui héberge le rôle de système de site du point de connexion de service utilise le contexte **System** pour accéder aux emplacements Internet suivants : go.microsoft.com et download.microsoft.com. Pour plus d'informations sur les emplacements supplémentaires utilisés par le point de connexion de service, consultez Conditions requises pour l'accès Internet.
- Quand votre point de connexion de service est en mode hors connexion, utilisez l'outil de connexion de service pour effectuer une synchronisation manuelle avec le cloud Microsoft. Pour plus d'informations, consultez Utiliser l'outil de connexion de service.
- Les mises à jour dans la console vous évitent d'avoir à localiser et à installer indépendamment les mises à jour, les service packs et les nouveaux composants.
- Installez uniquement les mises à jour dans la console de votre choix. Quand vous installez certaines mises à jour, vous pouvez sélectionner des fonctionnalités individuelles à activer et à utiliser. Pour plus d'informations, consultez Activer les fonctionnalités facultatives des mises à jour.

Quand vous installez une mise à jour dans la console, le processus suivant se produit :

- Elle procède automatiquement à une vérification de la configuration requise. Vous pouvez également effectuer cette vérification manuellement avant de commencer l'installation.
- Elle s'installe sur le site de niveau supérieur de votre environnement. Ce site est le site d'administration centrale si vous en avez un. Dans une hiérarchie, la mise à jour s'installe automatiquement sur les sites principaux. Contrôlez le moment où chaque serveur de site principal est autorisé à se mettre à jour à l'aide des fenêtres de maintenance pour les serveurs de site.
- Après la mise à jour d'un serveur de site, tous les rôles de système de site affectés se mettent automatiquement à jour. Ces rôles incluent les instances du fournisseur SMS. Une fois que le site a installé la mise à jour, la console Configuration Manager invite également son utilisateur à la mettre à jour.
- Si une mise à jour inclut le client Configuration Manager, possibilité vous est offerte de tester la mise à jour en préproduction ou d'appliquer tout de suite la mise à jour à tous les clients.
- Après la mise à jour d'un site principal, les sites secondaires ne sont pas mis à jour automatiquement. Vous devez en effet lancer manuellement leur mise à jour.

> **NOTE**
> Les branches Current Branch, Long-Term Servicing Branch et Technical Preview de Configuration Manager sont des versions distinctes. Ainsi, les mises à jour qui s'appliquent à une branche ne sont pas disponibles en tant que mises à jour dans la console pour les autres branches. Pour plus d'informations sur les branches disponibles, consultez Quelle branche de Configuration Manager dois-je utiliser ?

## Correctifs logiciels hors bande

Certains correctifs logiciels sont publiés avec une disponibilité limitée pour résoudre des problèmes spécifiques. D'autres correctifs logiciels s'appliquent à tous les clients mais ne peuvent pas être installés via la méthode dans la console. Ces correctifs logiciels sont fournis hors bande et ne sont pas détectés à partir du service cloud Microsoft.

En règle générale, quand vous cherchez à corriger ou à résoudre un problème lié à votre déploiement de Configuration Manager, vous pouvez en savoir plus sur les correctifs logiciels hors bande par l'intermédiaire des services de support technique Microsoft, via un article de la Base de connaissances du Support Microsoft ou à partir du blog de l'équipe System Center Configuration Manager.

Installez ces correctifs logiciels manuellement, à l'aide de l'une des deux méthodes suivantes :

- **Outil Inscription de la mise à jour** : cet outil permet d'importer manuellement le correctif logiciel dans votre console Configuration Manager. Installez ensuite la mise à jour de la même façon que les mises à jour dans la console découvertes automatiquement.
  - Cette méthode est utilisée pour les correctifs logiciels qui emploient la structure de nom de fichier suivante :
    `<Product>-<product version>-<KB article ID>-ConfigMgr.Update.exe`
  - Pour plus d'informations, consultez Importer des correctifs logiciels avec l'outil Inscription de la mise à jour.
- **Programme d'installation de correctif logiciel :** cet outil permet d'installer manuellement un correctif logiciel qui ne peut pas être installé via la méthode dans la console.
  - Cette méthode est utilisée pour les correctifs qui emploient la structure de nom de fichier suivante :
    `<Product>-<product version>-<KB article ID>-<platform>-<language>.exe`
  - Pour plus d'informations, consultez Utiliser le programme d'installation de correctif logiciel pour installer des mises à jour.

# Installation de mises à jour dans la console pour System Center Configuration Manager

22/06/2018 • 44 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Configuration Manager se synchronise avec le service cloud Microsoft pour obtenir les mises à jour. Vous pouvez installer ces mises à jour à partir de la console Configuration Manager.

## Obtenir les mises à jour disponibles

Seules les mises à jour qui s'appliquent à votre infrastructure et à votre version sont téléchargées et mises à disposition dans votre hiérarchie. Cette synchronisation peut être automatique ou manuelle, selon la manière dont vous configurez le point de connexion de service pour votre hiérarchie :

- En **mode en ligne**, le point de connexion de service se connecte automatiquement au service cloud Microsoft et télécharge les mises à jour applicables.

  Par défaut, Configuration Manager vérifie la disponibilité de nouvelles mises à jour toutes les 24 heures. Vous pouvez également rechercher des mises à jour immédiatement en choisissant **Rechercher les mises à jour** dans le nœud **Administration** > **Mises à jour et maintenance** de la console Configuration Manager.

- En **mode hors connexion**, le point de connexion de service ne se connecte pas au service cloud Microsoft. Pour télécharger et importer les mises à jour disponibles, utilisez l'outil de connexion de service.

> **NOTE**
> Vous pouvez importer des correctifs hors bande dans votre console. Pour cela, utilisez l'outil d'inscription de la mise à jour. Ces correctifs hors bande complètent les mises à jour que vous obtenez lors de la synchronisation avec le service cloud Microsoft.

Une fois les mises à jour synchronisées, vous pouvez les afficher dans la console Configuration Manager en accédant au nœud **Administration** > **Mises à jour et maintenance** :

- Les mises à jour que vous n'avez pas installées apparaissent **Disponibles**.
- Les mises à jour que vous avez installées apparaissent **Installées**. Seule la mise à jour installée le plus récemment s'affiche. Vous pouvez choisir le bouton **Historique** sur le ruban pour afficher les mises à jour installées précédemment.

Avant de configurer le point de connexion de service, vous devez comprendre et planifier ses utilisations supplémentaires. Les utilisations suivantes peuvent affecter la façon dont vous configurez ce rôle de système de site :

- Le point de connexion de service est utilisé pour charger les informations d'utilisation relatives à votre site. Ces informations permettent au service cloud de Microsoft d'identifier les mises à jour disponibles pour la version actuelle de votre infrastructure. Pour plus d'informations, consultez Données de diagnostic et d'utilisation.
- Le point de connexion de service permet de gérer des appareils avec Microsoft Intune et à l'aide de la fonctionnalité de gestion des appareils mobiles locale de Configuration Manager. Pour plus d'informations,

consultez Gestion des appareils mobiles (MDM) hybride avec System Center Configuration Manager et Microsoft Intune.

Pour mieux comprendre ce qui se passe quand des mises à jour sont téléchargées, consultez :

- Organigramme - Téléchargement des mises à jour pour System Center Configuration Manager
- Organigramme - Réplication des mises à jour pour System Center Configuration Manager

## Attribuer les autorisations d'afficher et de gérer les mises à jour et les fonctionnalités

Pour qu'un utilisateur puisse afficher les mises à jour dans la console, un rôle de sécurité d'administration incluant la classe de sécurité **Packages de mise à jour** doit lui être attribué. Cette classe accorde l'autorisation d'afficher et de gérer les mises à jour dans la console Configuration Manager.

#### À propos de la classe Packages de mise à jour

Par défaut, la classe **Packages de mise à jour** (SMS_CM_Updatepackages) fait partie des rôles de sécurité intégrés suivants avec les autorisations répertoriées :

- **Administrateur complet** avec autorisations **Modifier** et **Lecture** :
  - Un utilisateur disposant de ce rôle de sécurité et de l'accès à l'étendue de sécurité **Tout** peut afficher et installer les mises à jour. L'utilisateur peut également activer des fonctionnalités pendant l'installation et activer des fonctionnalités individuelles une fois la mise à jour installée.
  - Un utilisateur disposant de ce rôle de sécurité et de l'accès à l'étendue de sécurité **Par défaut** peut afficher et installer les mises à jour. L'utilisateur peut également activer des fonctionnalités pendant l'installation et afficher des fonctionnalités une fois la mise à jour installée. En revanche, cet utilisateur ne peut pas activer les fonctionnalités après l'installation de la mise à jour.
- **Analyste en lecture seule** avec autorisations **Lecture** :
  - Un utilisateur disposant de ce rôle de sécurité et de l'accès à l'étendue **Par défaut** peut afficher les mises à jour mais pas les installer. Il peut également afficher les fonctionnalités après l'installation d'une mise à jour mais pas les activer.

#### Autorisations requises pour les mises à jour et la maintenance

- Utilisez un compte affecté à un rôle de sécurité qui comprend la classe **Packages de mise à jour** avec les autorisations **Modifier** et **Lecture** .
- L'étendue **Par défaut** doit être affectée au compte.

#### Autorisations requises pour seulement voir les mises à jour

- Utilisez un compte assigné à un rôle de sécurité qui comprend la classe **Packages de mise à jour** avec uniquement l'autorisation **Lecture**.
- L'étendue **Par défaut** doit être affectée au compte.

#### Autorisations requises pour activer des fonctionnalités après l'installation de mises à jour

- Utilisez un compte affecté à un rôle de sécurité qui comprend la classe **Packages de mise à jour** avec les autorisations **Modifier** et **Lecture** .
- L'étendue **Tout** doit être affectée au compte.

## Avant d'installer une mise à jour dans la console

Passez en revue les étapes suivantes avant d'installer une mise à jour à partir de la console Configuration Manager.

#### Étape 1 : consulter la liste de contrôle de mise à jour

Passez en revue la liste de contrôle de mise à jour applicable pour connaître les actions à entreprendre avant de

lancer la mise à jour :

- Liste de contrôle pour l'installation de la mise à jour 1706
- Liste de contrôle pour l'installation de la mise à jour 1710
- Liste de contrôle pour l'installation de la mise à jour 1802

**Étape 2 : exécuter l'Outil de vérification des prérequis avant d'installer une mise à jour**

Avant d'installer une mise à jour, envisagez d'exécuter la vérification des prérequis pour cette mise à jour. Si vous effectuez cette vérification avant d'installer une mise à jour :

- Les fichiers de mise à jour sont répliqués vers d'autres sites avant l'installation de la mise à jour.
- La vérification des prérequis est automatiquement réexécutée lorsque vous choisissez d'installer la mise à jour.

> **NOTE**
> Si vous lancez une vérification des prérequis, puis que vous affichez l'état, la phase **Installation** semble active, mais la mise à jour n'est pas réellement en cours d'installation. Pour effectuer la vérification des prérequis, le processus de mise à jour extrait le package dans la bibliothèque de contenu et le place dans un dossier intermédiaire où sont accessibles les vérifications de prérequis en cours. Le même processus s'exécute à l'installation d'une mise à jour. C'est pourquoi l'installation s'affiche comme étant « En cours ». Seule l'étape *Extraire la mise à jour* apparaît dans la catégorie Installation.

Par la suite, lorsque vous installez la mise à jour, vous pouvez configurer la mise à jour de manière à ignorer les avertissements relatifs à la vérification des prérequis.

**Pour exécuter l'Outil de vérification des prérequis avant d'installer une mise à jour**

1. Dans la console Configuration Manager, accédez à **Administration** > **Mises à jour et maintenance**.
2. Cliquez avec le bouton droit sur le package de mise à jour pour lequel vous souhaitez exécuter la vérification des prérequis.
3. Choisissez **Exécuter la vérification de la condition préalable**.

   Lorsque vous exécutez la vérification des prérequis, le contenu de la mise à jour est répliqué sur des sites enfants. Vous pouvez consulter le fichier distmgr.log sur le serveur du site pour vérifier que le contenu est répliqué correctement.
4. Pour afficher les résultats de la vérification, dans la console Configuration Manager, accédez à **Surveillance** > **État des mises à jour et de la maintenance**, puis recherchez l'état du prérequis. Vous pouvez également consulter le fichier ConfigMgrPrereq.log sur le serveur du site pour plus de détails.

## Installation de mises à jour dans la console

Quand vous êtes prêt à installer des mises à jour à partir de la console Configuration Manager, commencez par le site de niveau supérieur de votre hiérarchie. Ce site est soit le site d'administration centrale, soit un site principal autonome.

Nous vous recommandons d'installer la mise à jour en dehors des heures de bureau normales pour chaque site afin de minimiser l'impact sur les opérations commerciales. Cette recommandation s'explique par le fait que l'installation de la mise à jour peut inclure des actions telles que la réinstallation des composants de site et des rôles de système de site.

- Les sites principaux enfants démarrent la mise à jour automatiquement après que le site d'administration centrale a installé la mise à jour. C'est le processus par défaut et recommandé. Vous pouvez cependant utiliser des fenêtres de maintenance pour les serveurs de site pour contrôler à quel moment le site

principal installe les mises à jour.

- Après la mise à jour du site principal parent, mettez à jour manuellement les sites secondaires à partir de la console Configuration Manager. La mise à jour automatique des serveurs de sites secondaires n'est pas prise en charge.
- Quand vous utilisez une console Configuration Manager, vous êtes invité à mettre à jour la console après la mise à jour du site.
- Après avoir mené à bien l'installation d'une mise à jour, le serveur de site met automatiquement à jour tous les rôles de système de site applicables. Le seul inconvénient concerne les points de distribution. Lors de l'installation d'une mise à jour, tous les points de distribution ne sont pas réinstallés et mis hors connexion pour être mis à jour simultanément. Au lieu de cela, le serveur de site utilise les paramètres de distribution de contenu du site pour distribuer la mise à jour à un sous-ensemble de points de distribution à la fois. Résultat : seuls certains points de distribution passent en mode hors connexion pour l'installation de la mise à jour. Les points de distribution dont la mise à jour n'a pas commencé ou est terminée restent en ligne et peuvent fournir du contenu aux clients.

### Vue d'ensemble de l'installation d'une mise à jour dans la console

#### 1. Au démarrage de l'installation de la mise à jour

L'Assistant Mises à jour affiche la liste des zones de produit auxquelles s'applique la mise à jour.

- Dans la page **Général** de l'Assistant, vous pouvez configurer les **Avertissements relatifs à la configuration requise**.
  - Les erreurs de configuration requise bloquent toujours l'installation de la mise à jour. Corrigez les erreurs avant de réessayer d'installer correctement la mise à jour. Pour plus d'informations, consultez Nouvelle tentative d'installation d'une mise à jour ayant échoué.
  - Des avertissements de configuration requise peuvent également bloquer l'installation de la mise à jour. Corrigez les avertissements avant de réessayer d'installer la mise à jour. Pour plus d'informations, consultez Nouvelle tentative d'installation d'une mise à jour ayant échoué.
  - **Ignorer les avertissements relatifs aux conditions requises et installer cette mise à jour sans tenir compte des manquements à la configuration requise** : définit une condition pour que l'installation de la mise à jour ignore les avertissements relatifs aux prérequis. Cette option permet de poursuivre l'installation de la mise à jour. Si vous ne sélectionnez pas cette option, l'installation de la mise à jour s'arrête en cas d'avertissement. Si vous n'avez pas exécuté la vérification des prérequis et corrigé les avertissements relatifs aux prérequis pour un site, nous vous déconseillons d'utiliser cette option.

    Dans les espaces de travail **Administration** et **Surveillance**, le nœud Mises à jour et maintenance affiche un bouton **Ignorer les avertissements de configuration requise** sur le ruban. Ce bouton devient disponible quand l'installation d'un package de mise à jour n'arrive pas à terme en raison d'avertissements de vérification des prérequis. Par exemple, vous installez une mise à jour sans utiliser l'option pour ignorer les avertissements de configuration requise (à partir de l'Assistant Mises à jour). L'installation de la mise à jour s'interrompt, avec un état d'avertissement de configuration requise, mais sans erreur. Vous pouvez plus tard choisir d'**ignorer les avertissements de configuration requise** dans le ruban pour poursuivre automatiquement l'installation de cette mise à jour en ignorant les avertissements de configuration requise. Quand vous utilisez cette option, l'installation de la mise à jour se poursuit automatiquement après quelques minutes.
- Quand une mise à jour s'applique au client Configuration Manager, une option vous est proposée pour tester la mise à jour du client avec un ensemble limité de clients. Pour plus d'informations, consultez Guide pratique pour tester les mises à niveau du client dans un regroupement de préproduction.

#### 2. Lors de l'installation de la mise à jour

Au cours de l'installation de la mise à jour, Configuration Manager :

- réinstalle tous les composants concernés, comme les rôles de système de site ou la console Configuration Manager ;
- gère les mises à jour des clients en fonction des sélections que vous avez effectuées pour le test du client et pour les mises à niveau automatiques du client ;
- ne redémarre pas les serveurs de système de site dans le cadre de la mise à jour, sauf si .NET est installé en raison d'un prérequis lié aux rôles de système de site.

> **TIP**
> Lors de l'installation des mises à jour, Configuration Manager met aussi à jour le dossier CD.Latest. Ce dossier est utilisé pendant la récupération d'un site.

#### 3. Analyse de la progression des mises à jour durant le processus d'installation

Pour surveiller l'état d'avancement, procédez comme suit :

- Dans la console Configuration Manager : nœud **Administration** > **Mises à jour et maintenance**. Ce nœud affiche l'état d'installation de tous les packages de mise à jour.
- Dans la console Configuration Manager, accédez au nœud **Administration** > **Vue d'ensemble** > **Mises à jour et maintenance**. Ce nœud affiche l'état d'installation uniquement du package de mise à jour en cours d'installation.

  L'installation du pack de mise à jour est décomposée selon les phases suivantes pour faciliter la surveillance. Pour chaque phase, des détails supplémentaires indiquent le fichier journal à consulter pour obtenir plus d'informations :

  - **Téléchargement** (cette phase s'applique uniquement au site de niveau supérieur où est installé le site du point de connexion de service.)
  - **Réplication**
  - **Vérification des prérequis**
  - **Installation**
  - **Post-installation** : pour plus d'informations, consultez Tâches post-installation.
- Vous pouvez consulter le fichier **CMUpdate.log** dans **<<Répertoire_Installation_ConfiMgr>\Logs**

#### 4. Après l'installation de la mise à jour

Une fois l'installation de la mise à jour sur le premier site terminée :

- Les sites principaux enfants installent automatiquement la mise à jour. Aucune action supplémentaire n'est requise.
- Les sites secondaires doivent être mis à jour manuellement dans la console Configuration Manager.

  > **TIP**
  > Bien que la version d'un site secondaire n'apparaisse pas dans la console, vous pouvez utiliser le Kit de développement logiciel (SDK) Configuration Manager pour vérifier la version d'un site. Voir SMS_Site Server WMI Class (Classe WMI serveur SMS_Site).

- Tant que tous les sites de votre hiérarchie n'ont pas été mis à jour vers la nouvelle version, la hiérarchie

fonctionne en mode mixte de versions. Pour plus d'informations, consultez Interopérabilité entre les différentes versions de Configuration Manager.

#### 5. Mettre à jour des consoles Configuration Manager

Dès lors qu'un site d'administration centrale ou un site principal est mis à jour, chaque console Configuration Manager qui se connecte à ce site doit aussi être mise à jour. Vous êtes invité à mettre à jour une console dans les cas suivants :

- lorsque vous ouvrez la console ;
- Quand vous accédez à un nouveau nœud dans une console ouverte

Nous vous recommandons d'installer la mise à jour immédiatement.

Une fois la mise à niveau de la console terminée, vous pouvez vérifier que les versions de la console et du site sont correctes. Accédez à **À propos de System Center Configuration Manager** en haut à gauche de la console.

> **NOTE**
> À compter de la version 1802, la version de la console est légèrement différente de la version du site. La version mineure de la console correspond maintenant à la version publiée de Configuration Manager. Par exemple, dans Configuration Manager version 1802, la version initiale du site est 5.0.8634.1000, et la version initiale de la console est 5.**1802**.1082.1700. Les numéros de build (1082) et de révision (1700) peuvent changer avec les correctifs logiciels futurs sur la version 1802.

**Pour démarrer l'installation de la mise à jour sur le site de niveau supérieur**

Sur le site de niveau supérieur de votre hiérarchie, dans la console Configuration Manager, accédez à **Administration** > **Mises à jour et maintenance**, sélectionnez une mise à jour **Disponible**, puis cliquez sur **Installer le package de mise à jour**.

**Pour démarrer l'installation de la mise à jour sur un site secondaire**

Après la mise à jour du site principal parent d'un site secondaire, vous pouvez mettre à jour ce dernier à partir de la console Configuration Manager. Pour ce faire, vous utilisez l' **Assistant Mise à niveau d'un site secondaire**.

1. Dans la console Configuration Manager, accédez à **Administration** > **Configuration du site** > **Sites**, sélectionnez le site à mettre à jour, puis, sous l'onglet Accueil, dans le groupe **Site**, choisissez **Mettre à niveau**.
2. Cliquez sur **Oui** pour démarrer la mise à jour du site secondaire.

Pour surveiller l'installation de la mise à jour sur un site secondaire, sélectionnez le serveur de site secondaire. Ensuite, sous l'onglet **Accueil**, dans le groupe **Site**, choisissez **Afficher l'état d'installation**. Vous pouvez également ajouter la colonne **Version** à l'affichage de la console pour voir la version de chaque site secondaire.

À l'issue de la mise à jour d'un site secondaire, si l'état dans la console ne s'actualise pas ou laisse supposer que la mise à jour a échoué, utilisez l'option **Réessayer l'installation**. Cette option ne réinstalle pas la mise à jour sur un site secondaire qui a correctement installé la mise à jour ; elle force la console à mettre à jour l'état.

**Tâches post-installation**

Lorsqu'un site installe une mise à jour, plusieurs tâches ne peuvent pas démarrer tant que la mise à jour n'est pas installée sur le serveur de site. Voici une liste des tâches post-installation essentielles aux opérations de site et de hiérarchie. Ces tâches étant critiques, elles sont activement surveillées. D'autres tâches ne sont pas directement surveillées, par exemple la réinstallation de rôles de système de site. Pour afficher l'état des tâches post-installation critiques, sélectionnez une tâche **post-installation** lorsque vous surveillez l'installation de la mise à jour d'un site.

Toutes les tâches ne se terminent pas immédiatement. Certaines tâches ne démarrent pas tant que chaque site n'a pas terminé l'installation de la mise à jour. Les nouvelles fonctionnalités que vous souhaitez utiliser peuvent être

retardées en attendant la fin de ces tâches. Ces nouvelles fonctionnalités peuvent ne pas être visibles temporairement, car leur activation démarre seulement quand tous les sites ont terminé l'installation de la mise à jour.

Les tâches post-installation incluent :

- **Installation du service SMS_EXECUTIVE**
  - Service critique qui s'exécute sur le serveur de site.
  - La réinstallation de ce service devrait s'exécuter rapidement.
- **Installation du composant SMS_DATABASE_NOTIFICATION_MONITOR**
  - Thread de composant de site critique du service SMS_EXECUTIVE.
  - La réinstallation de ce service devrait s'exécuter rapidement.
- **Installation du composant SMS_HIERARCHY_MANAGER**
  - Composant de site critique qui s'exécute sur le serveur de site.
  - Responsable de la réinstallation des rôles de système de site sur les serveurs de système de site. L'état de la réinstallation d'un rôle de système de site individuel n'apparaît pas.
  - La réinstallation de ce service devrait s'exécuter rapidement.
- **Installation du composant SMS_REPLICATION_CONFIGURATION_MONITOR**
  - Composant de site critique qui s'exécute sur le serveur de site.
  - La réinstallation de ce service devrait s'exécuter rapidement.
- **Installation du composant SMS_POLICY_PROVIDER**
  - Composant de site critique qui s'exécute uniquement sur les sites principaux.
  - La réinstallation de ce service devrait s'exécuter rapidement.
- **Surveillance de l'initialisation de la réplication**
  - Cette tâche s'affiche uniquement sur le site d'administration centrale et sur les sites principaux enfants.
  - Dépend de SMS_REPLICATION_CONFIGURATION_MONITOR.
  - Devrait s'exécuter rapidement.
- **Mise à jour du package de préproduction du client Configuration Manager**
  - Cette tâche s'affiche même si le client en préproduction (également appelé pilotage du client) n'est pas activé pour être utilisé.
  - Ne commence pas tant que tous les sites dans la hiérarchie n'ont pas terminé l'installation de la mise à jour.
- **Mise à jour du dossier du client sur le serveur de site**
  - Cette tâche ne s'affiche pas si vous utilisez le client en préproduction.
  - Devrait s'exécuter rapidement.
- **Mise à jour du package du client Configuration Manager**
  - Cette tâche ne s'affiche pas si vous utilisez le client en préproduction.
  - Se termine uniquement une fois que tous les sites ont installé la mise à jour.
- **Activation des fonctionnalités**
  - Cette tâche s'affiche uniquement sur le site de niveau supérieur de la hiérarchie.
  - Ne commence pas tant que tous les sites dans la hiérarchie n'ont pas terminé l'installation de la mise à jour.
  - Les fonctionnalités individuelles ne sont pas affichées.

# Nouvelle tentative d'installation d'une mise à jour ayant échoué

Quand l'installation d'une mise à jour échoue, passez en revue les commentaires dans la console pour identifier les résolutions des avertissements et erreurs. Vous pouvez également consulter le fichier ConfigMgrPrereq.log sur le serveur du site pour plus de détails. Avant de réessayer l'installation d'une mise à jour, vous devez corriger les erreurs et il est recommandé de corriger aussi les avertissements.

> **TIP**
> Si une mise à jour a des problèmes lors du téléchargement ou de réplication, vous pouvez utiliser la outil de réinitialisation de mise à jour.

Quand vous êtes prêt à réessayer l'installation d'une mise à jour, sélectionnez la mise à jour ayant échoué, puis choisissez une option applicable. Le comportement de nouvelle tentative d'installation de mise à jour dépend du nœud où vous lancez la nouvelle tentative et de l'option de nouvelle tentative que vous utilisez.

#### Réessayer l'installation pour la hiérarchie

Vous pouvez réessayer l'installation d'une mise à jour pour l'ensemble de la hiérarchie lorsque cette mise à jour est dans l'un des états suivants :

- Les vérifications des prérequis ont généré un ou plusieurs avertissements, et l'option permettant d'ignorer les avertissements de vérification des prérequis n'a pas été activée dans l'Assistant Mise à jour. (La valeur de mise à jour pour **Ignorer l'avertissement de condition préalable** dans le nœud **Mises à jour et maintenance** est **Non**.)
- La vérification des prérequis a échoué.
- L'installation a échoué.
- La réplication du contenu sur le site a échoué.

Accédez à **Administration** > **Mises à jour et maintenance**, sélectionnez la mise à jour, puis choisissez l'une des options suivantes :

- **Nouvelle tentative** : quand vous exécutez **Nouvelle tentative** à partir de ce nœud, l'installation de la mise à jour redémarre et ignore automatiquement les avertissements relatifs aux prérequis. Le contenu pour la mise à jour est uniquement répliqué si la réplication a échoué précédemment.
- **Ignorer les avertissements de configuration requise** : si l'installation de la mise à jour s'arrête en raison d'un avertissement, vous pouvez cliquer sur **Ignorer les avertissements de configuration requise**. Cette action permet à l'installation de la mise à jour de continuer (après quelques minutes) et utilise l'option pour ignorer les avertissements de prérequis.

#### Réessayer l'installation pour le site

Vous pouvez réessayer l'installation d'une mise à jour sur un site spécifique lorsque cette mise à jour est dans l'un des états suivants :

- Les vérifications des prérequis ont généré un ou plusieurs avertissements, et l'option permettant d'ignorer les avertissements de vérification des prérequis n'a pas été activée dans l'Assistant Mise à jour. (La valeur de mise à jour pour **Ignorer l'avertissement de condition préalable** dans le nœud Mises à jour et maintenance est **Non**.)
- La vérification des prérequis a échoué.
- L'installation a échoué.

Accédez à **Surveillance** > **Vue d'ensemble** > **État de la maintenance de site**, sélectionnez la mise à jour, puis cliquez sur l'une des options suivantes :

- **Nouvelle tentative** : quand vous exécutez **Nouvelle tentative** à partir de ce nœud, vous redémarrez l'installation de la mise à jour uniquement sur ce site. Contrairement à l'exécution de **Nouvelle tentative** à

partir du nœud **Mises à jour et maintenance**, cette nouvelle tentative n'ignore pas les avertissements relatifs aux prérequis.

- **Ignorer les avertissements de configuration requise** : si l'installation de la mise à jour s'arrête en raison d'un avertissement, vous pouvez cliquer sur **Ignorer les avertissements de configuration requise**. Cette action permet à l'installation de la mise à jour de continuer (après quelques minutes) et utilise l'option pour ignorer les avertissements de prérequis.

## Après l'installation d'une mise à jour sur un site

Utilisez la liste de vérification suivante pour effectuer les tâches courantes et les configurations nécessaires après la mise à jour d'un site.

**Vérifier que la réplication de site à site est active :** dans la console Configuration Manager, accédez aux emplacements suivants pour consulter l'état et vérifier que la réplication est active :

- **Surveillance** > **Vue d'ensemble** > **Hiérarchie de site**
- **Surveillance** > **Vue d'ensemble** > **Réplication de base de données**

Pour plus d'informations, consultez Surveiller l'infrastructure de la hiérarchie et de la réplication et À propos de l'analyseur de lien de réplication.

**Vérifier que les serveurs de site et les serveurs de système de site distants ont redémarré (si nécessaire) :** examinez l'infrastructure de votre site et vérifiez que les serveurs de site et serveurs de système de site appropriés ont redémarré correctement. En règle générale, les serveurs de site redémarrent uniquement quand Configuration Manager installe .NET en tant que prérequis pour un rôle de système de site.

**Mettre à jour les consoles Configuration Manager autonomes :** vérifiez que toutes les consoles Configuration Manager distantes ont été mises à jour vers la même version. Vous êtes invité à mettre à jour la console dans les cas suivants :

- lorsque vous accédez à un nouveau nœud dans la console ;
- lorsque vous ouvrez la console.

**Reconfigurer les réplicas de base de données pour les points de gestion sur les sites principaux :** si vous utilisez des réplicas de base de données pour les points de gestion sur les sites principaux, vous devez désinstaller les réplicas de base de données avant de mettre à jour le site. Après avoir mis à niveau un site principal, reconfigurez le réplica de base de données pour les points de gestion. Pour plus d'informations, consultez Réplicas de base de données pour les points de gestion.

**Reconfigurer les tâches de maintenance de base de données désactivées avant la mise à jour :** si vous avez désactivé les tâches de maintenance sur un site avant d'installer la mise à jour, reconfigurez ces tâches sur le site. Utilisez les mêmes paramètres qui étaient en vigueur avant la mise à jour.

**Mettre à niveau les clients** : pour plus d'informations, consultez Guide pratique pour mettre à niveau les clients pour les ordinateurs Windows.

**Configurations supplémentaires :** examinez les modifications que vous avez apportées avant de commencer la mise à jour, puis restaurez ces configurations sur vos sites et votre hiérarchie.

## Activation de fonctionnalités facultatives de mises à jour

Lorsqu'une mise à jour inclut une ou plusieurs fonctionnalités facultatives, vous avez la possibilité d'activer celles-ci dans votre hiérarchie. Vous pouvez activer les fonctionnalités au moment de l'installation de la mise à jour ou revenir à la console ultérieurement pour activer les fonctionnalités facultatives.

Pour afficher les fonctionnalités disponibles et leur état, dans la console, accédez à **Administration** > **Mises à**

**jour et maintenance** > **Fonctionnalités**.

Quand une fonctionnalité n'est pas facultative, elle est installée automatiquement. Elle n'apparaît pas dans le nœud **Fonctionnalités**.

> **IMPORTANT**
> Dans une hiérarchie multisite, vous pouvez uniquement activer les fonctionnalités facultatives ou en préversion sur le site d'administration centrale. Ceci vise à éviter les conflits au sein de la hiérarchie.

Quand vous activez une nouvelle fonctionnalité ou une fonctionnalité en préversion, le Gestionnaire de hiérarchie de Configuration Manager (HMAN) doit traiter le changement avant que cette fonctionnalité ne soit disponible. Le traitement du changement est souvent immédiat, mais il peut prendre jusqu'à 30 minutes en fonction du cycle de traitement HMAN. Une fois le changement traité, vous devez redémarrer la console pour voir les nouveaux nœuds associés à cette fonctionnalité.

#### Liste des fonctionnalités facultatives

Les fonctionnalités suivantes sont facultatives dans la dernière version de Configuration Manager :

- Accès conditionnel pour les PC gérés
- Passport for Work (également appelé *Windows Hello Entreprise*)
- VPN pour Windows 10
- Stratégie Windows Defender Exploit Guard
- Connecteur OMS (Microsoft Operations Management Suite)
- Créer un certificat PFX
- Cache d'homologue client
- Point de service de l'entrepôt de données
- Passerelle de gestion cloud
- Mises à jour du pilote Surface
- Mise en cache préalable du contenu de la séquence de tâches
- Exécuter l'étape de la séquence de tâches
- Créer et exécuter des scripts
- Évaluation de l'attestation de l'intégrité des appareils pour les stratégies de conformité pour l'accès conditionnel
- Approuver les demandes d'application pour les utilisateurs par appareil

> **TIP**
> Pour plus d'informations sur les fonctionnalités qui nécessitent un consentement pour être activées, consultez Fonctionnalités en préversion.
> Pour plus d'informations sur les fonctionnalités qui sont disponibles uniquement dans la branche Technical Preview, consultez Technical Preview.

## Utiliser des fonctionnalités de préversions de mises à jour

Les fonctionnalités en préversion sont incluses dans la branche Current Branch à des fins de test préalable dans un environnement de production. Vous pouvez utiliser ces fonctionnalités dans un environnement de production, mais elles ne doivent pas être considérées comme prêtes pour la production. Pour en savoir plus sur les fonctionnalités de préversion, y compris sur la façon de les activer dans votre environnement, consultez Fonctionnalités de préversion.

# Forum aux questions

**Pourquoi certaines mises à jour ne s'affichent pas dans ma console ?**

Si vous ne trouvez pas une mise à jour spécifique dans votre console après une synchronisation réussie avec le service cloud Microsoft, les causes possibles de ce comportement sont les suivantes :

- La mise à jour requiert une configuration que votre infrastructure n'utilise pas, ou votre version actuelle du produit ne remplit pas une condition préalable pour la réception de la mise à jour.

  Si vous pensez que vous disposez des configurations requises et prérequis pour une mise à jour manquante, vérifiez que votre point de connexion de service est en mode en ligne. Ensuite, utilisez l'option **Rechercher les mises à jour** dans le nœud **Mises à jour et maintenance** pour forcer la vérification. Si vous êtes en mode hors connexion, vous devez recourir à l'outil de connexion au service pour synchroniser manuellement le service cloud.

- Votre compte ne dispose pas des autorisations d'administration basée sur des rôles appropriées pour afficher les mises à jour dans la console Configuration Manager.

  Pour plus d'informations sur les autorisations requises pour afficher les mises à jour et activer les fonctionnalités à partir de la console, consultez Autorisations de gérer les mises à jour dans cette rubrique.

# Outil de réinitialisation des mises à jour

22/06/2018 • 7 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

À compter de la version 1706, les sites d'administration centrale et les sites principaux Configuration Manager incluent l'outil de réinitialisation des mises à jour Configuration Manager (**CMUpdateReset.exe**). Utilisez l'outil pour résoudre les problèmes de téléchargement ou de réplication des mises à jour dans la console. L'outil se trouve dans le dossier ***\cd.latest\SMSSETUP\TOOLS*** du serveur de site.

Vous pouvez utiliser cet outil avec n'importe quelle version de Current Branch prise en charge.

Utilisez cet outil quand une mise à jour dans la console n'a pas encore été installée et qu'elle se trouve dans un état d'échec. Un état d'échec signifie que le téléchargement de la mise à jour est en cours, mais qu'il est bloqué ou qu'il prend beaucoup trop de temps. Un téléchargement est considéré comme trop long s'il dépasse de plusieurs heures le téléchargement de packages de mise à jour de taille similaire. Il peut également s'agir d'un échec de réplication de la mise à jour sur les sites principaux enfants.

Lorsque vous exécutez l'outil, il s'exécute sur la mise à jour que vous spécifiez. Par défaut, l'outil ne supprime pas les mises à jour installées ou téléchargées avec succès.

**Prérequis**

Le compte que vous utilisez pour exécuter l'outil nécessite les autorisations suivantes :

- Autorisations en **Lecture** et **Écriture** pour la base de données de site du site d'administration centrale et pour chaque site principal de votre hiérarchie. Pour définir ces autorisations, vous pouvez ajouter le compte d'utilisateur en tant que membre des rôles de base de données fixes **db_datawriter** et **db_datareader** sur la base de données Configuration Manager de chaque site. L'outil n'interagit pas avec les sites secondaires.
- **Administrateur local** sur le site de niveau supérieur de votre hiérarchie.
- **L'administrateur local** sur l'ordinateur hébergeant le point de connexion de service.

Vous devez disposer du GUID du package de mise à jour à réinitialiser. Pour obtenir le GUID :

1. Dans la console, accédez à **Administration** > **Mises à jour et maintenance**.
2. Dans le volet qui s'affiche, cliquez avec le bouton droit sur l'en-tête d'une des colonnes (comme **État**), puis sélectionnez **GUID du package** pour ajouter cette colonne à l'affichage.
3. La colonne affiche maintenant le GUID du package de mise à jour.

> **TIP**
> Pour copier le GUID, sélectionnez la ligne pour le package de mise à jour que vous souhaitez réinitialiser, puis utilisez CTRL + C pour copier cette ligne. Si vous collez votre sélection copiée dans un éditeur de texte, vous pouvez ensuite copier uniquement le GUID pour une utilisation en tant que paramètre de ligne de commande quand vous exécutez l'outil.

**Exécution de l'outil**

L'outil doit être exécuté sur le site de niveau supérieur de la hiérarchie.

Quand vous exécutez l'outil, utilisez les paramètres de ligne de commande pour spécifier les éléments suivants :

- Serveur SQL Server sur le site de niveau supérieur de la hiérarchie.
- Nom de la base de données de site sur le site de niveau supérieur.
- GUID du package de mise à jour à réinitialiser.

En fonction de l'état de la mise à jour, l'outil identifie les serveurs supplémentaires auxquels il doit accéder.

Si le package de mise à jour est dans un état *post-téléchargement*, l'outil ne nettoie pas le package. Vous pouvez éventuellement forcer la suppression d'une mise à jour téléchargée avec succès à l'aide du paramètre de suppression de force (consultez les paramètres de ligne de commande plus loin dans cette rubrique).

Une fois que l'outil s'exécute :

- Si un package a été supprimé, redémarrez le service SMS_Executive sur le site de niveau supérieur. Ensuite, recherchez les mises à jour pour pouvoir retélécharger le package.
- Si un package n'a pas été supprimé, aucune action n'est nécessaire. La mise à jour se réinitialise, puis redémarre la réplication ou l'installation.

**Paramètres de ligne de commande :**

| PARAMÈTRE | DESCRIPTION |
|---|---|
| **-S <Nom de domaine complet de l'instance SQL Server de votre site de niveau supérieur >** | *Obligatoire*<br>Permet de spécifier le nom de domaine complet de l'instance SQL Server qui héberge la base de données de site pour le site de niveau supérieur de votre hiérarchie. |
| **D - <Nom de la base de données>** | *Obligatoire*<br>Permet de spécifier le nom de la base de données pour le site de niveau supérieur. |
| **-P <GUID du package>** | *Obligatoire*<br>Permet de spécifier le GUID du package de mise à jour à réinitialiser. |
| **-I <Nom de l'instance SQL Server>** | *Facultatif*<br>Permet d'identifier l'instance de SQL Server qui héberge la base de données du site. |
| **-FDELETE** | *Facultatif*<br>Permet de forcer la suppression d'un package de mise à jour téléchargé avec succès. |

**Exemples :**
Dans un scénario classique, vous souhaitez réinitialiser une mise à jour qui présente des problèmes de téléchargement. Votre nom de domaine complet SQL Server est *server1.fabrikam.com*, la base de données du site est *CM_XYZ* et le GUID du package est *61F16B3C-F1F6-4F9F-8647-2A524B0C802C*. Vous exécutez : ***CMUpdateReset.exe -S server1.fabrikam.com -D CM_XYZ -P 61F16B3C-F1F6-4F9F-8647-2A524B0C802C***

Dans un scénario plus extrême, vous souhaitez forcer la suppression du package de mise à jour problématique. Votre nom de domaine complet SQL Server est *server1.fabrikam.com*, la base de données du site est *CM_XYZ* et le GUID du package est *61F16B3C-F1F6-4F9F-8647-2A524B0C802C*. Vous exécutez : ***CMUpdateReset.exe -FDELETE -S server1.fabrikam.com -D CM_XYZ -P 61F16B3C-F1F6-4F9F-8647-2A524B0C802C***

# Tester la mise à niveau d'une base de données avant d'installer une mise à jour

22/06/2018 • 9 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les informations de cette rubrique peuvent vous aider à tester la mise à niveau d'une base de données avant d'installer une mise à jour dans la console pour la branche active de Configuration Manager. Toutefois, le test de la mise à niveau ne constitue plus une étape requise ou recommandée si votre base de données est suspecte ou a été modifiée par des personnalisations qui ne sont pas explicitement prises en charge par Configuration Manager.

## Ai-je besoin de tester une mise à niveau ?

Le test d'une mise à niveau n'est plus requis depuis les modifications apportées à System Center Configuration Manager. Ces modifications simplifient le processus et la vitesse à laquelle un environnement de production peut être mis à jour avec des versions plus récentes. Cette refonte a été effectuée pour permettre aux clients de rester à jour avec moins de risques et moins de surcharge opérationnelle lors de l'installation de chaque nouvelle mise à jour.

Les modifications concernent la façon dont les mises à jour s'installent, notamment la logique qui annule automatiquement une mise à jour ayant échoué sans avoir à exécuter une récupération de site. Ces modifications permettent d'utiliser la console pour gérer les installations de mises à jour et incluent une option pour relancer l'installation d'une mise à jour ayant échoué.

> **TIP**
> Lorsque vous effectuez une mise à niveau avec System Center Configuration Manager à partir d'un produit plus ancien, par exemple System Center 2012 Configuration Manager, le test des mises à niveau de la base de données reste une étape recommandée.

Si vous souhaitez néanmoins tester la mise à niveau d'une base de données de site lorsque vous installez une mise à jour dans la console, les informations suivantes vous fournissent des conseils sur l'installation d'une mise à jour dans la console.

## Préparer le test d'une mise à niveau de base de données

Avant d'installer une nouvelle mise à jour dans votre hiérarchie, telle que la mise à jour 1702, vous pouvez tester la mise à niveau de votre base de données de site.

Pour test une mise à niveau, utilisez le programme d'installation de Configuration Manager à partir des fichiers source figurant dans le dossier CD.Latest d'un site qui exécute la version de Configuration Manager vers laquelle vous effectuez la mise à jour. Cela signifie que pour tester la mise à jour de la base de données pour une mise à jour vers 1702 :

- Vous devez disposer d'au moins un site qui exécute la version 1702 à partir duquel vous pouvez accéder à ce dossier CD.Latest.
- Si vous n'avez pas de site qui exécute la version requise, vous pouvez installer un site dans un environnement de laboratoire, puis mettre à jour ce site avec la nouvelle version. Cette opération crée le dossier CD.Latest avec la version correcte des fichiers sources.

Le test de la mise à niveau est exécuté sur une sauvegarde de votre base de données de site que vous avez restaurée sur une instance distincte de SQL Server. Vous exécutez le programme d'installation à partir du dossier **CD.Latest** à l'aide du commutateur de ligne de commande **testdbupgrade** pour tester la mise à niveau qui a restauré la copie de la base de données. Une fois le test de la mise à niveau terminé, la base de données mise à niveau est supprimée. Elle ne peut pas être utilisée par un site Configuration Manager.

Si l'installation d'une mise à jour échoue, vous n'avez pas besoin de récupérer le site. Au lieu de cela, vous pouvez essayer de réinstaller de la mise à jour depuis la console.

## Tester une mise à niveau

1. Utilisez le programme d'installation de Configuration Manager et les fichiers sources figurant dans le dossier **CD.Latest** d'un site qui exécute la version vers laquelle vous prévoyez d'effectuer la mise à jour.

2. Copiez le dossier **CD.Latest** vers un emplacement sur l'instance SQL Server que vous utiliserez pour tester la mise à niveau de la base de données.

3. Créez une sauvegarde de la base de données du site pour laquelle vous souhaitez tester une mise à niveau. Restaurez ensuite une copie de cette base de données sur une instance de SQL Server qui n'héberge pas de site Configuration Manager. L'instance SQL Server doit utiliser la même édition de SQL Server que votre base de données de site.

4. Après avoir restauré la copie de la base de données, exécutez le fichier **Setup** dans le dossier CD.Latest contenant les fichiers sources de la version vers laquelle vous effectuez la mise à jour. Quand vous exécutez le programme d'installation, utilisez l'option de ligne de commande **/TESTDBUPGRADE** . Si l'instance SQL Server qui héberge la copie de la base de données n'est pas l'instance par défaut, fournissez les arguments de ligne de commande pour identifier l'instance qui héberge la copie de la base de données du site.

   Par exemple, vous utilisez une base de données de site dont le nom de base de données est *SMS_ABC*. Vous restaurez une copie de cette base de données de site sur une instance prise en charge de SQL Server ayant pour nom d'instance *DBTest*. Pour tester une mise à niveau de cette copie de la base de données du site, utilisez la ligne de commande suivante : **Setup.exe /TESTDBUPGRADE DBtest\CM_ABC**.

   Vous trouverez Setup.exe à l'emplacement suivant sur le média source de System Center Configuration Manager : **SMSSETUP\BIN\X64**.

5. Sur l'instance de SQL Server où vous avez exécuté le test de mise à niveau, examinez *ConfigMgrSetup.log* à la racine du lecteur système pour connaître la progression et l'issue du test.

   Si le test de la mise à niveau échoue, corrigez les problèmes ayant entraîné l'échec de la mise à niveau de la base de données du site. Puis créez une nouvelle sauvegarde de la base de données du site et testez la mise à niveau de la nouvelle copie de la base de données.

## Étapes suivantes

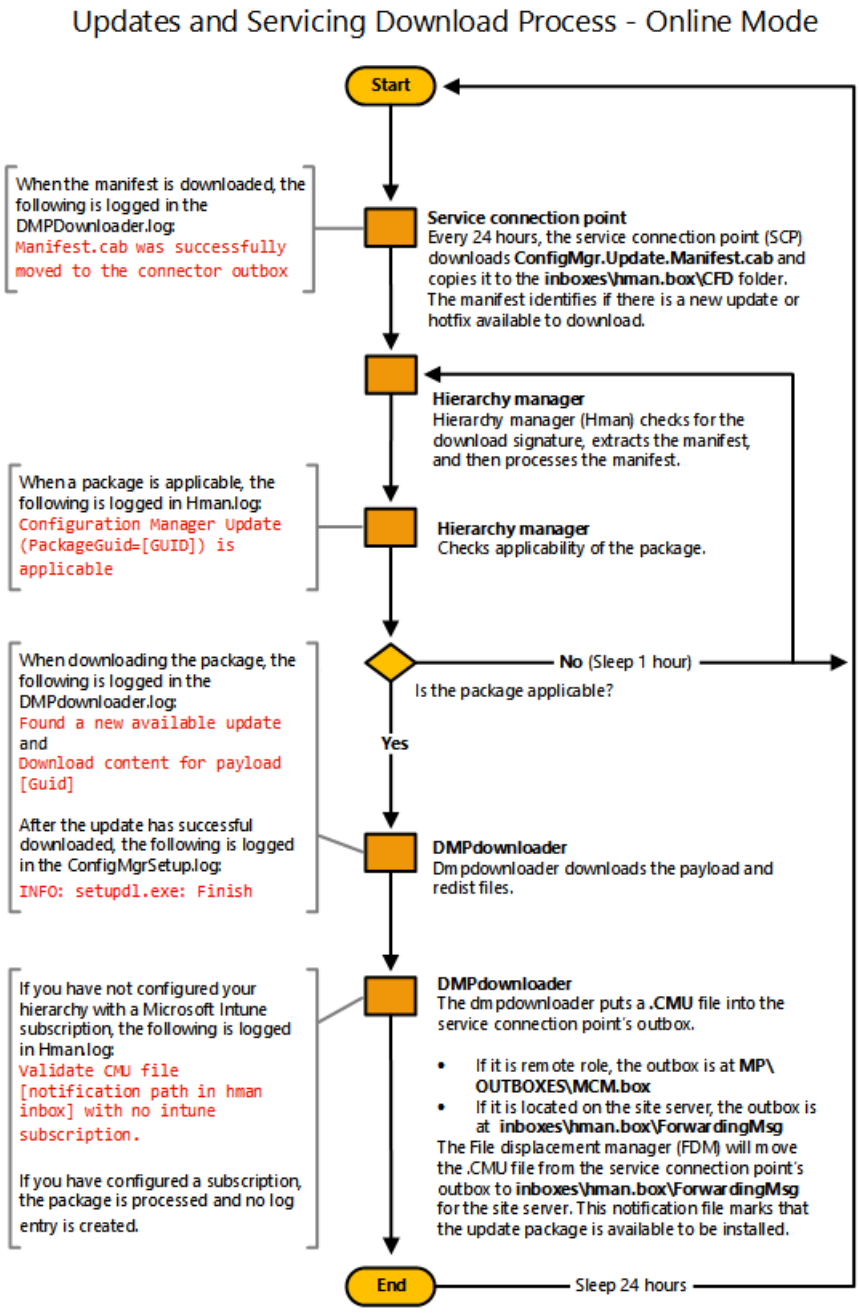
Une fois le test de la mise à jour de la base de données terminé, supprimez la base de données mise à jour. Elle ne peut pas être utilisée par un site Configuration Manager. Vous pouvez ensuite revenir à votre site actif et commencer l'installation de la mise à jour.

# Organigramme - Téléchargement des mises à jour pour System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Ce flux de données affiche le processus par lequel un site avec un point de connexion de service en ligne télécharge les mises à jour dans la console.

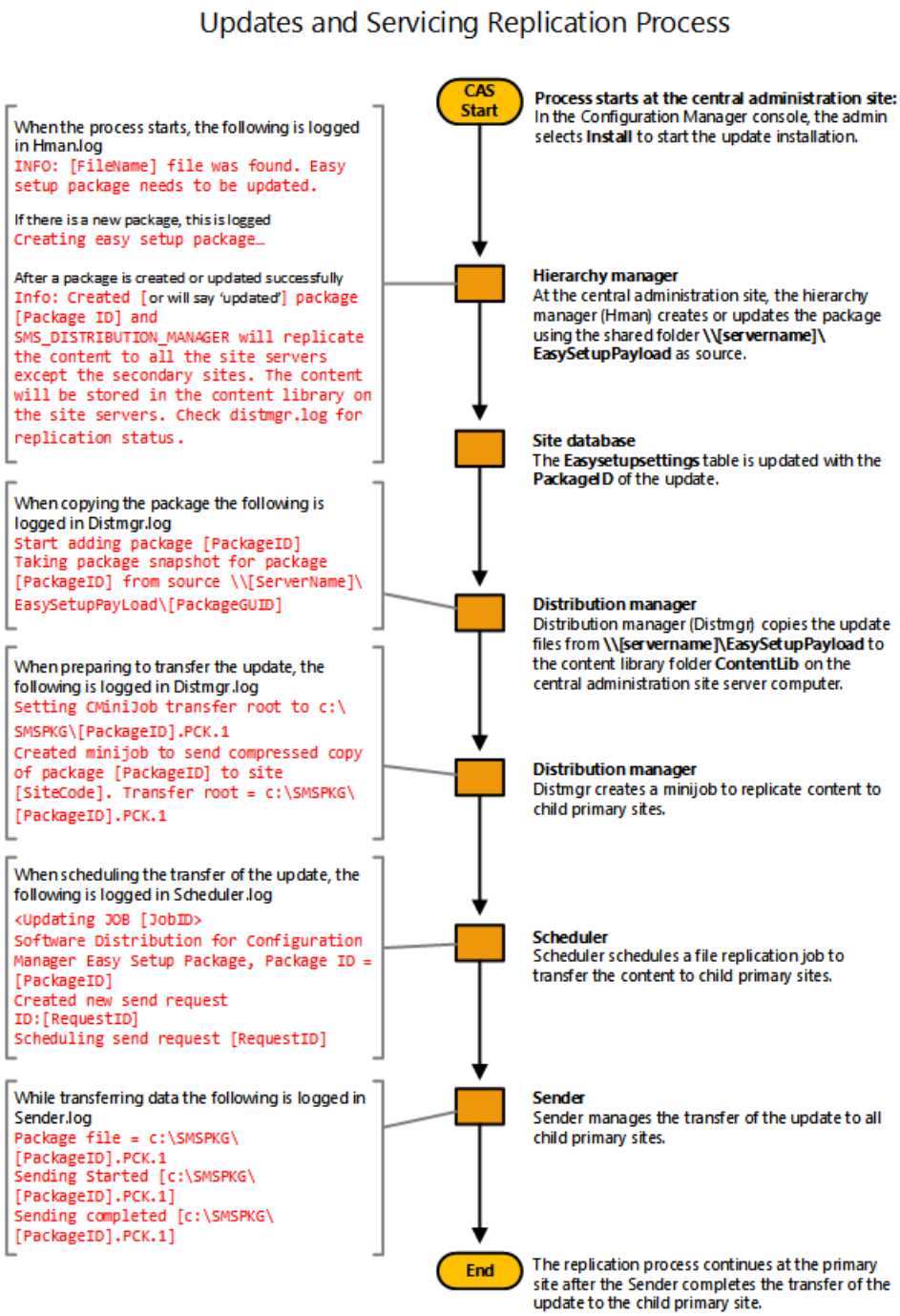


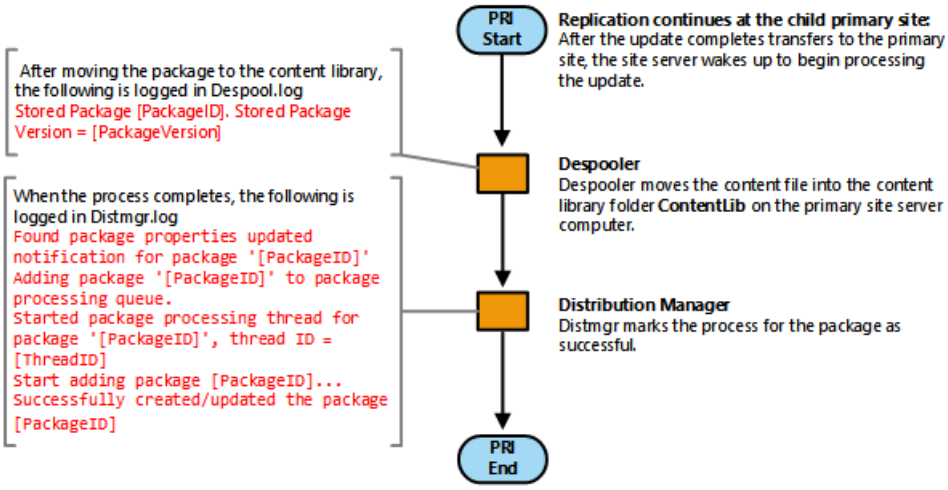
# Organigramme - Réplication des mises à jour pour System Center Configuration Manager

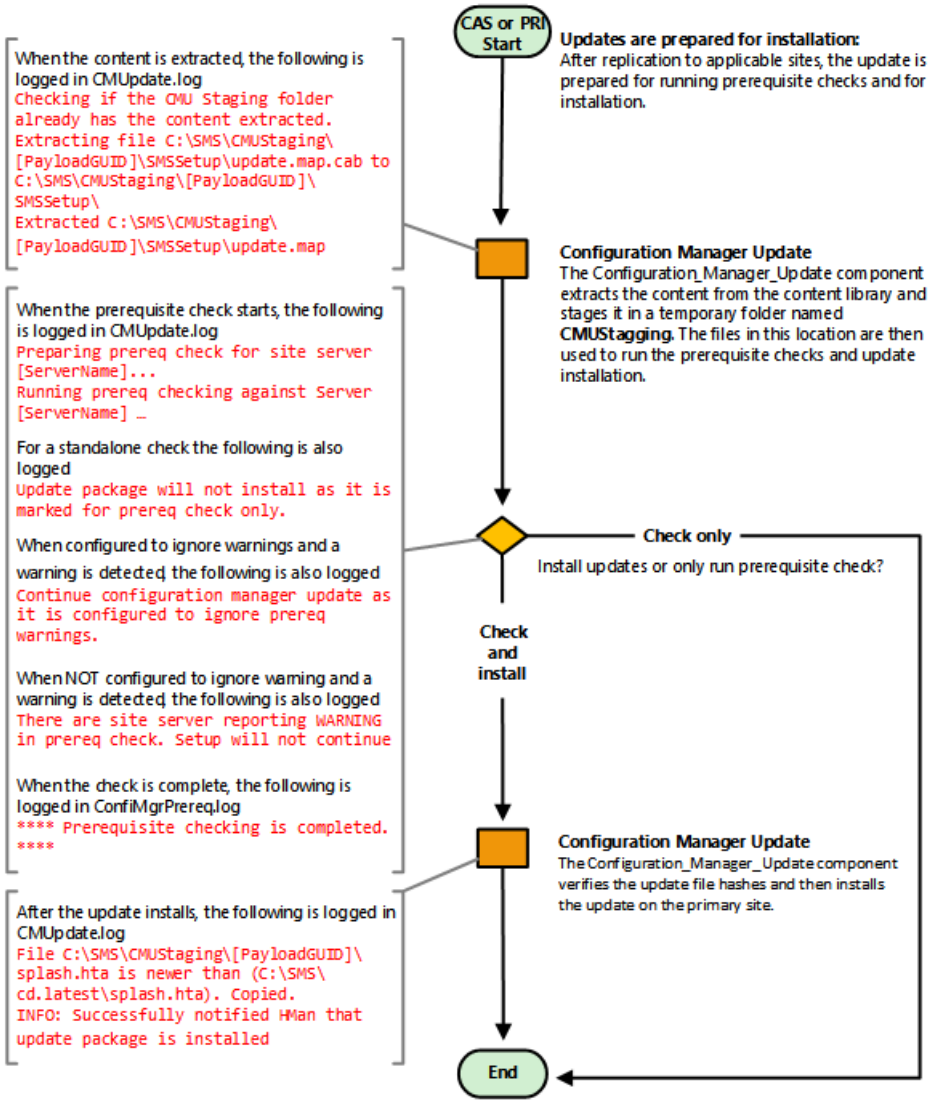
22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Ces flux de données présentent le processus par lequel une mise à jour dans la console que vous choisissez d'installer se réplique sur d'autres sites. Ces flux présentent également le processus d'extraction de la mise à jour pour exécuter les vérifications préalablement requises et installer les mises à jour sur le site d'administration centrale et sur les sites principaux.




PRI Start
Replication continues at the child primary site:
After the update completes transfers to the primary site, the site server wakes up to begin processing the update.
After moving the package to the content library, the following is logged in Despool.log
Stored Package [PackageID]. Stored Package Version = [PackageVersion]
Despooler
Despooler moves the content file into the content library folder ContentLib on the primary site server computer.
When the process completes, the following is logged in Distmgr.log
Found package properties updated notification for package '[PackageID]'
Adding package '[PackageID]' to package processing queue.
Started package processing thread for package '[PackageID]', thread ID = [ThreadID]
Start adding package [PackageID]...
Successfully created/updated the package [PackageID]
Distribution Manager
Distmgr marks the process for the package as successful.
PRI End


CAS or PRI Start
Updates are prepared for installation:
After replication to applicable sites, the update is prepared for running prerequisite checks and for installation.
When the content is extracted, the following is logged in CMUpdate.log
Checking if the CMU Staging folder already has the content extracted.
Extracting file C:\SMS\CMUStaging\[PayloadGUID]\SMSSetup\update.map.cab to C:\SMS\CMUStaging\[PayloadGUID]\SMSSetup\
Extracted C:\SMS\CMUStaging\[PayloadGUID]\SMSSetup\update.map
Configuration Manager Update
The Configuration_Manager_Update component extracts the content from the content library and stages it in a temporary folder named CMUStagging. The files in this location are then used to run the prerequisite checks and update installation.
When the prerequisite check starts, the following is logged in CMUpdate.log
Preparing prereq check for site server [ServerName]...
Running prereq checking against Server [ServerName] _
For a standalone check the following is also logged
Update package will not install as it is marked for prereq check only.
When configured to ignore warnings and a warning is detected, the following is also logged
Continue configuration manager update as it is configured to ignore prereq warnings.
When NOT configured to ignore warning and a warning is detected, the following is also logged
There are site server reporting WARNING in prereq check. Setup will not continue
When the check is complete, the following is logged in ConfiMgrPrereq.log
**** Prerequisite checking is completed. ****
Check only
Install updates or only run prerequisite check?
Check and install
Configuration Manager Update
The Configuration_Manager_Update component verifies the update file hashes and then installs the update on the primary site.
After the update installs, the following is logged in CMUpdate.log
File C:\SMS\CMUStaging\[PayloadGUID]\splash.hta is newer than (C:\SMS\cd.latest\splash.hta). Copied.
INFO: Successfully notified HMan that update package is installed
End

# Fonctionnalités en préversion dans System Center Configuration Manager

15/05/2018 • 7 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les fonctionnalités de préversion sont des fonctions incluses dans la branche Current Branch à des fins de test préalable dans un environnement de production. Ces fonctionnalités sont entièrement prises en charge mais sont toujours en cours de développement. Elles peuvent donc être modifiées jusqu'à ce qu'elles passent en préversion.

Pour pouvoir sélectionner et utiliser ces fonctions, vous devez d'abord donner votre consentement via la console Configuration Manager.

Le consentement est une action à effectuer une seule fois par hiérarchie ; elle ne peut pas être annulée. Tant que vous n'avez pas accepté de les utiliser, vous ne pouvez pas activer les fonctions en préversion incluses avec les mises à jour. Après avoir activé une fonctionnalité en préversion, vous ne pouvez pas la désactiver.

Pour donner votre consentement, accédez à la console, sélectionnez **Administration** > **Configuration du site** > **Sites**, puis choisissez **Paramètres de hiérarchie**. Sous l'onglet **Général**, choisissez **Accepter d'utiliser les fonctionnalités en préversion**.

Lorsque vous installez une mise à jour qui comprend des fonctionnalités de préversion, ces dernières sont affichées dans l'Assistant Maintenance et mises à jour, avec les fonctionnalités standard incluses dans la mise à jour :

- **Si vous avez donné votre consentement :** vous pouvez activer les fonctionnalités à partir de l'Assistant Maintenance et mises à jour quand vous installez la mise à jour. Pour ce faire, sélectionnez les fonctionnalités de préversion, comme vous le feriez pour toute autre fonctionnalité.

  Si vous le souhaitez, vous pouvez attendre pour activer une fonctionnalité en préversion par la suite à partir du nœud **Administration** > **Mises à jour et maintenance** > **Fonctionnalités** de la console. Dans le nœud **Fonctionnalités**, sélectionnez la fonctionnalité, puis choisissez **Activer**. Cette option est grisée jusqu'à ce que vous donniez votre consentement. (Avant la version 1702, les mises à jour et la maintenance s'effectuaient via le menu **Administration** > **Services cloud**.)

- **Si vous n'avez pas donné votre consentement :** lorsque vous installez une mise à jour, les fonctionnalités en préversion sont visibles dans l'Assistant Mises à jour et maintenance, mais elles sont grisées et ne peuvent pas être activées. Une fois la mise à jour installée, vous pouvez afficher ces fonctionnalités dans le nœud **Fonctionnalités**. Mais vous ne pouvez pas les activer tant que vous n'avez pas donné votre consentement dans **Paramètres de hiérarchie**.

> **IMPORTANT**
> Dans une hiérarchie multisite, vous pouvez uniquement activer les fonctionnalités facultatives ou en préversion sur le site d'administration centrale. Ceci vise à éviter les conflits au sein de la hiérarchie.
> Si vous avez donné votre consentement sur un site principal autonome, et si vous développez ensuite la hiérarchie en installant un nouveau site d'administration centrale, vous devez redonner votre consentement sur ce dernier.

Quand vous activez une fonctionnalité en préversion, le Gestionnaire de hiérarchie de Configuration Manager (HMAN) doit traiter le changement avant que cette fonctionnalité ne soit disponible. Le traitement du changement est souvent immédiat, mais il peut prendre jusqu'à 30 minutes en fonction du cycle de traitement HMAN. Une fois le changement traité, vous devez redémarrer la console pour voir la nouvelle interface utilisateur associée à cette

fonctionnalité.

**Les fonctionnalités en préversion disponibles sont les suivantes** :

| FONCTIONNALITÉ | AJOUTÉE EN PRÉVERSION | AJOUTÉE EN VERSION COMPLÈTE |
|---|---|---|
| Prise en charge de Cisco AnyConnect 4.0.07x et ultérieur pour iOS | Version 1802 | |
| Déploiements par phases | Version 1802 | |
| Exécuter l'étape de la séquence de tâches | Version 1710 | Version 1802 |
| Windows Defender Exploit Guard | Version 1710 | Version 1802 |
| Évaluation de l'attestation de l'intégrité des appareils pour les stratégies de conformité pour l'accès conditionnel | Version 1710 | Version 1802 |
| Créer et exécuter des scripts PowerShell à partir de la console Configuration Manager | Version 1706 | Version 1802 |
| Gérer les mises à jour du pilote Microsoft Surface | Version 1706 | Version 1710 |
| Gestion Device Guard avec Configuration Manager | Version 1702 | |
| Mise en cache préalable du contenu de la séquence de tâches | Version 1702 | Version 1710 |
| Vérifier si des fichiers exécutables sont en cours d'exécution avant d'installer une application | Version 1702 | Version 1706 |
| Point de service de l'entrepôt de données | Version 1702 | Version 1706 |
| Cache d'homologue pour la distribution de contenu aux clients | Version 1610 | Version 1710 |
| Passerelle de gestion cloud | Version 1610 | Version 1802 |
| Connecteur Microsoft Operations Management Suite | Version 1606 | Version 1802 |
| Maintenance d'un regroupement prenant en charge les clusters (maintenance d'un groupe de serveurs) | Version 1602 | |
| Accès conditionnel pour les PC gérés par System Center Configuration Manager | Version 1602 | Version 1702 |

**TIP**

Pour plus d'informations sur les fonctionnalités facultatives qui doivent être activées en premier, consultez Activation de fonctionnalités facultatives de mises à jour.
Pour plus d'informations sur les fonctionnalités qui sont disponibles uniquement dans la branche Technical Preview, consultez Technical Preview.

# Fenêtres de maintenance pour les serveurs de site

22/06/2018 • 3 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez configurer les fenêtres de maintenance sur les sites d'administration centrale et les sites principaux pour contrôler l'installation des mises à jour dans la console. Vous pouvez configurer plusieurs fenêtres, avec la fenêtre autorisée pour l'installation des mises à jour déterminée par une combinaison de toutes les fenêtres de maintenance pour ce serveur de site.

Quand aucune fenêtre de maintenance n'est configurée :

- **Sur votre site de niveau supérieur** (site d'administration centrale ou site principal autonome) vous choisissez quand démarrer l'installation de la mise à jour.
- **Sur un site principal enfant**, la mise à jour s'installe automatiquement après que le site d'administration centrale a installé la mise à jour.
- **Sur un site secondaire**, les mises à jour ne démarrent jamais automatiquement. Vous devez démarrer manuellement l'installation de la mise à jour à partir de la console, après que le site principal parent a installé la mise à jour.

Quand une fenêtre de maintenance est configurée :

- **Sur votre site de niveau supérieur**, vous ne serez pas en mesure de démarrer l'installation d'une nouvelle mise à jour dans la console Configuration Manager. Même avec une fenêtre de maintenance configurée, le site télécharge automatiquement les mises à jour afin qu'elles soient prêtes à être installées.
- **Sur un site principal enfant**, les mises à jour installées sur un site d'administration centrale sont téléchargées sur le site principal, mais ne démarrent pas automatiquement. Vous ne pouvez pas démarrer manuellement l'installation d'une mise à jour pendant une période bloquée par l'utilisation d'une fenêtre de maintenance. Lorsque les fenêtres de maintenance ne bloquent plus l'installation de la mise à jour, celle-ci démarre automatiquement.
- Les **sites secondaires** ne prennent pas en charge les fenêtres de maintenance et n'installent pas automatiquement les mises à jour. Une fois que le site parent principal d'un site secondaire installe une mise à jour, vous pouvez démarrer la mise à jour du site secondaire à partir de la console.

## Pour configurer une fenêtre de maintenance

1. Dans la console Configuration Manager, ouvrez **Administration** > **Configuration du site** > **Sites**, puis sélectionnez le serveur de site sur lequel vous voulez configurer une fenêtre de maintenance.

2. Ensuite, modifiez les **Propriétés** des serveurs de site et sélectionnez l'onglet **Fenêtre de service** , où vous pouvez ensuite définir une ou plusieurs fenêtres de service pour ce serveur de site.

# Utiliser l'outil de connexion de service pour System Center Configuration Manager

26/06/2018 • 20 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez l'**Outil de connexion de service** quand votre point de connexion de service est en mode hors connexion ou quand vos serveurs de système de site Configuration Manager ne sont pas connectés à Internet. Cet outil peut vous aider à tenir votre site à jour avec les dernières mises à jour pour Configuration Manager.

Quand vous l'exécutez, il se connecte manuellement au service cloud Configuration Manager pour charger les informations d'utilisation relatives à votre hiérarchie et pour télécharger des mises à jour. Le chargement de données d'utilisation est nécessaire pour que le service cloud vous propose les mises à jour adaptées à votre déploiement.

## Prérequis pour utiliser l'outil de connexion de service

Voici la liste des prérequis et des problèmes connus.

**Conditions préalables :**

- Vous avez installé un point de connexion de service et sélectionné l'option **Hors connexion, connexion à la demande**.
- L'outil doit être exécuté à partir d'une invite de commandes.
- Chaque ordinateur sur lequel l'outil s'exécute (l'ordinateur du point de connexion de service et l'ordinateur connecté à Internet) doit avoir un système x64 bits ainsi que les composants suivants :
  - Fichiers x86 et x64 **Redistributable Visual C++** . Par défaut, Configuration Manager installe la version x64 sur l'ordinateur qui héberge le point de connexion de service.

    Pour télécharger une copie des fichiers Visual C++, consultez Packages Redistributable Visual C++ pour Visual Studio 2013 dans le Centre de téléchargement Microsoft.
  - .NET Framework 4.5.2 ou version ultérieure.
- Le compte que vous utilisez pour exécuter l'outil doit avoir :
  - Des autorisations d'**administrateur local** sur l'ordinateur hébergeant le point de connexion de service (sur lequel l'outil s'exécute)
  - Des autorisations de**Lecture** sur la base de données de site
- Pour transférer des fichiers entre l'ordinateur du point de connexion de service et celui ayant accès à Internet, vous devez disposer d'un lecteur USB avec un espace libre suffisant pour stocker les fichiers et mises à jour, ou employer une autre méthode. (Ce scénario part du principe que votre site et les ordinateurs gérés ne disposent pas d'une connexion directe à Internet.)

## Utiliser l'outil de connexion de service

L'outil de connexion de service (**serviceconnectiontool.exe**) se trouve sur le support d'installation de Configuration Manager dans le dossier **%chemin%\smssetup\tools\ServiceConnectionTool**. Utilisez toujours l'outil de connexion de service qui correspond à votre version de Configuration Manager.

Dans cette procédure, les exemples de ligne de commande utilisent les noms de fichiers et les emplacements de dossiers suivants (vous pouvez très bien utiliser d'autres chemins et noms de fichiers qui correspondent à votre environnement et à vos préférences) :

- Chemin à une clé USB où sont stockées les données pour le transfert entre les serveurs : **D:\USB**
- Nom du fichier .cab contenant les données exportées à partir de votre site : **UsageData.cab**
- Nom du dossier vide dans lequel les mises à jour téléchargées pour Configuration Manager sont stockées à des fins de transfert entre les serveurs : **UpdatePacks**

Sur l'ordinateur qui héberge le point de connexion de service :

- Ouvrez une invite de commandes avec des privilèges d'administration, puis changez de répertoire pour accéder à l'emplacement du fichier **serviceconnectiontool.exe**.

  Par défaut, cet outil se trouve sur le support d'installation de Configuration Manager dans le dossier **%chemin%\smssetup\tools\ServiceConnectionTool**. Tous les fichiers dans ce dossier doivent figurer dans le même dossier pour que l'outil de connexion de service fonctionne.

Lorsque vous exécutez la commande suivante, l'outil prépare un fichier .cab contenant des informations sur l'utilisation, et le copie vers un emplacement que vous spécifiez. Les données du fichier .cab sont basées sur le niveau des données de diagnostic et d'utilisation que votre site est configuré pour collecter. (voir Données d'utilisation et de diagnostic pour System Center Configuration Manager). Exécutez la commande suivante pour créer le fichier .cab :

- **serviceconnectiontool.exe -prepare -usagedatadest D:\USB\UsageData.cab**

Vous devez également copier le dossier ServiceConnectionTool avec tout son contenu sur le lecteur USB, ou le rendre disponible sur l'ordinateur que vous allez utiliser aux étapes 3 et 4.

### Vue d'ensemble

#### L'utilisation de l'outil de connexion de service nécessite trois étapes principales

1. **Préparation** : cette étape doit être exécutée sur l'ordinateur hébergeant le point de connexion de service. Quand vous exécutez l'outil, il place les données d'utilisation dans un fichier .cab et les stocke sur un lecteur USB (ou dans un autre emplacement de transfert spécifié).
2. **Connexion** : lors de cette étape, vous exécutez l'outil sur un ordinateur distant qui se connecte à Internet pour charger les données d'utilisation puis télécharger les mises à jour.
3. **Importation** : cette étape doit être exécutée sur l'ordinateur hébergeant le point de connexion de service. Quand vous exécutez l'outil, il importe les données que vous avez téléchargées et les ajoute à votre site pour que vous puissiez ensuite afficher et installer ces mises à jour à partir de la console Configuration Manager.

À compter de la version 1606, quand vous vous connectez à Microsoft, vous pouvez charger plusieurs fichiers .cab à la fois (chacun à partir d'une hiérarchie différente) et spécifier un serveur proxy et un utilisateur du serveur proxy.

#### Pour charger plusieurs fichiers .cab

- Placez chaque fichier .cab que vous exportez à partir de hiérarchies distinctes dans le même dossier. Le nom de chaque fichier doit être unique, et vous pouvez les renommer manuellement si nécessaire.
- Ensuite, quand vous exécutez la commande pour charger des données vers Microsoft, vous spécifiez le dossier qui contient les fichiers .cab. (Avant la mise à jour 1606, vous pouviez uniquement charger des données à partir d'une seule hiérarchie à la fois, et l'outil vous obligeait à spécifier le nom du fichier .cab dans le dossier.)
- Plus tard, quand vous exécutez la tâche d'importation sur le point de connexion de service d'une hiérarchie, l'outil importe automatiquement uniquement les données de cette hiérarchie.

#### Pour spécifier un serveur proxy

Vous pouvez utiliser les paramètres facultatifs suivants pour spécifier un serveur proxy (vous trouverez des informations supplémentaires sur l'utilisation de ces paramètres dans la section Paramètres de ligne de commande de cette rubrique) :

- **-proxyserveruri [nom_domaine_complet_serveur_proxy]** Utilisez ce paramètre pour spécifier le serveur proxy à utiliser pour cette connexion.
- **-proxyusername [nom_utilisateur]** Utilisez ce paramètre quand vous devez spécifier un utilisateur du serveur proxy.

#### Spécifier le type de mises à jour à télécharger

À compter de la version 1706, le comportement par défaut du téléchargement des outils a changé, et l'outil prend en charge des options pour contrôler quels fichiers vous téléchargez.

- Par défaut, l'outil télécharge seulement la dernière mise à jour disponible qui s'applique à la version de votre site. Il ne télécharge pas les correctifs.

Pour changer ce comportement, utilisez un des paramètres suivants pour spécifier quels fichiers sont téléchargés.

> **NOTE**
>
> La version de votre site est déterminée à partir des données du fichier .cab qui est chargé quand l'outil s'exécute.
>
> Vous pouvez vérifier la version en recherchant le fichier *SiteVersion*.txt dans le fichier .cab.

- **-downloadall** : cette option télécharge tout, notamment les mises à jour et les correctifs, quelle que soit la version de votre site.
- **-downloadhotfix** : cette option télécharge tous les correctifs, quelle que soit la version de votre site.
- **-downloadsiteversion** : cette option télécharge les mises à jour et les correctifs dont la version est supérieure à celle de votre site.

Exemple de ligne de commande utilisant - *downloadsiteversion* :

- **serviceconnectiontool.exe -connect -*downloadsiteversion* -usagedatasrc D:\USB -updatepackdest D:\USB\UpdatePacks**

#### Pour utiliser l'outil de connexion de service

1. Sur l'ordinateur qui héberge le point de connexion de service :
   - Ouvrez une invite de commandes avec des privilèges d'administration, puis changez de répertoire pour accéder à l'emplacement du fichier **serviceconnectiontool.exe**.
2. Exécutez la commande suivante pour que l'outil prépare un fichier .cab contenant des informations sur l'utilisation et le copie vers un emplacement que vous spécifiez :
   - **serviceconnectiontool.exe -prepare -usagedatadest D:\USB\UsageData.cab**

   Si vous allez charger des fichiers .cab à partir de plusieurs hiérarchies en même temps, chaque fichier .cab dans le dossier doit avoir un nom unique. Vous pouvez renommer manuellement les fichiers que vous ajoutez au dossier.

   Si vous souhaitez afficher les informations d'utilisation collectées pour le chargement sur le service cloud Configuration Manager, exécutez la commande suivante pour exporter les mêmes données dans un fichier .csv que vous pouvez ensuite afficher à l'aide d'une application comme Excel :

   - **serviceconnectiontool.exe -export -dest D:\USB\UsageData.csv**

3. Une fois l'étape de préparation terminée, connectez le lecteur USB (ou transférez les données exportées au moyen d'une autre méthode) à un ordinateur ayant accès à Internet.

4. Sur l'ordinateur connecté à Internet, ouvrez une invite de commandes avec des privilèges d'administration, puis changez de répertoire pour accéder à l'emplacement contenant une copie de l'outil **serviceconnectiontool.exe** et les fichiers supplémentaires de ce dossier.

5. Exécutez la commande suivante pour commencer le chargement des informations d'utilisation et le téléchargement des mises à jour pour Configuration Manager :

   - **serviceconnectiontool.exe -connect -usagedatasrc D:\USB -updatepackdest D:\USB\UpdatePacks**

   Pour obtenir plus d'exemples de cette ligne de commande, consultez la section Options de ligne de commande plus loin dans cette rubrique.

   > **NOTE**
   > Quand vous exécutez la ligne de commande pour vous connecter au service cloud Configuration Manager, une erreur semblable à la suivante peut se produire :
   >
   > - Exception non gérée : System.UnauthorizedAccessException :
   >
   >   L'accès au chemin « C:\
   >   Users\br\AppData\Local\Temp\extractmanifestcab\95F8A562.sql » est refusé.
   >
   > Vous pouvez ignorer cette erreur sans risque. Fermez la fenêtre d'erreur et continuez.

6. Une fois le téléchargement des mises à jour pour Configuration Manager terminé, connectez le lecteur USB (ou transférez les données exportées au moyen d'une autre méthode) à l'ordinateur qui héberge le point de connexion de service.

7. Sur l'ordinateur qui héberge le point de connexion de service, ouvrez une invite de commandes avec des privilèges d'administration, changez de répertoire pour accéder à l'emplacement contenant **serviceconnectiontool.exe**, puis exécutez la commande suivante :

   - **serviceconnectiontool.exe -import -updatepacksrc D:\USB\UpdatePacks**

8. Une fois l'importation terminée, vous pouvez fermer l'invite de commandes. (Seules les mises à jour pour la hiérarchie applicable sont importées.)

9. Ouvrez la console Configuration Manager, puis accédez à **Administration** > **Mises à jour et maintenance**. Les mises à jour qui ont été importées peuvent désormais être installées. (Avant la version 1702, les mises à jour et la maintenance s'effectuaient via le menu **Administration** > **Services cloud**.)

   Pour plus d'informations, consultez Installer des mises à jour dans la console pour System Center Configuration Manager.

## Fichiers journaux

**ServiceConnectionTool.log**

Chaque fois que vous exécutez l'outil de connexion de service, un fichier journal nommé **ServiceConnectionTool.log** est généré dans le même emplacement que l'outil. Ce fichier journal fournira de simples détails sur l'exécution de l'outil en fonction des commandes utilisées. Un fichier journal existant est remplacé chaque fois que vous exécutez l'outil.

**ConfigMgrSetup.log**

Lorsque vous utilisez l'outil pour vous connecter et télécharger les mises à jour, un fichier journal appelé

**ConfigMgrSetup.log** est créé à la racine du lecteur système. Ce fichier journal fournira des informations plus détaillées, notamment la liste des fichiers téléchargés, extraits, et si les vérifications de hachage ont réussi.

## Options de ligne de commande

Pour afficher de l'aide sur l'outil de point de connexion de service, ouvrez une invite de commandes dans le dossier contenant l'outil, puis exécutez la commande suivante : **serviceconnectiontool.exe**.

| OPTIONS DE LIGNE DE COMMANDE | DÉTAILS |
|---|---|
| **-prepare -usagedatadest [lecteur:][chemin] [nom_fichier.cab]** | Cette commande stocke les données d'utilisation actuelles dans un fichier .cab.<br><br>Exécutez cette commande en tant qu' **administrateur local** sur le serveur qui héberge le point de connexion de service.<br><br>Exemple : **-prepare -usagedatadest D:\USB\Usagedata.cab** |
| **-connect -usagedatasrc [lecteur:][chemin] -updatepackdest [lecteur:][chemin] -proxyserveruri [nom_domaine_complet_serveur_proxy] -proxyusername [nom_utilisateur]**<br><br>Si vous utilisez une version de Configuration Manager antérieure à la version 1606, vous devez spécifier le nom du fichier .cab et vous ne pouvez pas utiliser les options d'un serveur proxy. Les paramètres de commande pris en charge sont les suivants :<br>**-connect -usagedatasrc [lecteur:][chemin][nom_fichier] -updatepackdest [lecteur:][chemin]** | Cette commande se connecte au service cloud Configuration Manager pour charger les fichiers .cab de données d'utilisation à partir de l'emplacement spécifié et pour télécharger le contenu de console et les packs de mise à jour disponibles. Les options pour les serveurs proxy sont facultatives.<br><br>Exécutez cette commande en tant qu' **administrateur local** sur un ordinateur capable de se connecter à Internet.<br><br>Exemple de connexion sans serveur proxy : **-connect -usagedatasrc D:\USB\ -updatepackdest D:\USB\UpdatePacks**<br><br>Exemple de connexion quand vous utilisez un serveur proxy : **-connect -usagedatasrc D:\USB\Usagedata.cab -updatepackdest D:\USB\UpdatePacks -proxyserveruri itgproxy.redmond.corp.microsoft.com -proxyusername Meg**<br><br>Si vous utilisez une version antérieure à la version 1606, vous devez spécifier un nom de fichier pour le fichier .cab et vous ne pouvez pas spécifier de serveur proxy. Utilisez l'exemple de ligne de commande suivant : **-connect -usagedatasrc D:\USB\Usagedata.cab -updatepackdest D:\USB\UpdatePacks** |
| **-import -updatepacksrc [lecteur:][chemin]** | Cette commande importe les packages de mise à jour et le contenu de la console que vous avec précédemment téléchargés dans la console Configuration Manager.<br><br>Exécutez cette commande en tant qu' **administrateur local** sur le serveur qui héberge le point de connexion de service.<br><br>Exemple : **-import -updatepacksrc D:\USB\UpdatePacks** |

| OPTIONS DE LIGNE DE COMMANDE | DÉTAILS |
| --- | --- |
| **-export -dest [lecteur:][chemin][nom_fichier.csv]** | Cette commande exporte les données d'utilisation dans un fichier .csv que vous pouvez ensuite afficher.<br><br>Exécutez cette commande en tant qu' **administrateur local** sur le serveur qui héberge le point de connexion de service.<br><br>Exemple : **-export -dest D:\USB\usagedata.csv** |

# Importer des correctifs pour System Center Configuration Manager avec l'outil Inscription de la mise à jour

22/06/2018 • 5 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Certaines mises à jour de Configuration Manager indisponibles sur le service cloud Microsoft ne peuvent être obtenues que hors-bande. C'est le cas, par exemple, d'un correctif logiciel en édition limitée destiné à résoudre un problème spécifique.
Quand vous devez installer une version hors-bande et que le nom de fichier du correctif ou de la mise à jour se termine par l'extension **update.exe**, vous pouvez vous servir de l'**outil Inscription de la mise à jour** pour importer manuellement la mise à jour dans la console Configuration Manager. Cet outil vous permet d'extraire et de transférer le package de mise à jour vers le serveur de site, et d'inscrire la mise à jour auprès de la console Configuration Manager.

Si le fichier de correctif a l'extension de fichier **.exe** et non **update.exe**, consultez Utiliser le programme d'installation de correctif logiciel pour installer les mises à jour de System Center Configuration Manager

> **NOTE**
> Cette rubrique fournit des indications générales sur la façon d'installer les correctifs pour la mise à jour de System Center Configuration Manager. Pour plus d'informations sur un correctif ou une mise à jour spécifiques, voir l'article correspondant dans la Base de connaissances du support Microsoft.

**Conditions préalables à l'utilisation de l'outil Inscription de la mise à jour :**

- Cet outil permet d'installer uniquement des mises à jour hors-bande dont le nom se termine par l'extension **.update.exe**
- L'outil est autonome et comprend les mises à jour individuelles que vous recevez directement de Microsoft.
- L'outil n'a aucune dépendance par rapport au mode du point de connexion de service.
- L'outil doit être exécuté sur l'ordinateur hébergeant le point de connexion de service.
- .NET Framework 4.52 doit être installé sur l'ordinateur sur lequel l'outil s'exécute (ordinateur faisant office de point de connexion de service).
- Le compte que vous utilisez pour exécuter l'outil doit disposer d'autorisations d'**administrateur local** sur l'ordinateur hébergeant le point de connexion de service sur lequel l'outil s'exécute
- Le compte que vous utilisez pour exécuter l'outil doit disposer d'autorisations en **écriture** sur le dossier suivant de l'ordinateur hébergeant le point de connexion de service : **<Répertoire d'installation de ConfigMgr>\EasySetupPayload\offline**

**Pour utiliser l'outil Inscription de la mise à jour**

1. Sur l'ordinateur qui héberge le point de connexion de service :
   - Ouvrez une invite de commandes avec des privilèges d'administration, puis remplacez les répertoires par l'emplacement contenant **<Produit>-<version du produit>-<ID d'article de la Base de**

**connaissances>-ConfigMgr.Update.exe**

2. Exécutez la commande suivante pour démarrer l'outil Inscription de la mise à jour :

   - **<Produit>-<version du produit>-<ID d'article de la Base de connaissances>-ConfigMgr.Update.exe**

   Une fois inscrit, le correctif logiciel s'affiche en tant que nouvelle mise à jour dans la console dans les 24 heures. Vous pouvez accélérer le processus :

   - Ouvrez la console Configuration Manager, accédez à **Administration** > **Mises à jour et maintenance** puis cliquez sur **Rechercher les mises à jour**. (Avant la version 1702, les mises à jour et la maintenance s'effectuaient via le menu **Administration** > **Services cloud**.)

   L'outil Inscription de la mise à jour consigne ses actions dans un fichier .log sur l'ordinateur local. Ce fichier journal porte le même nom que le fichier .exe du correctif, et est stocké dans le dossier **%SystemRoot%/Temp**.

   Une fois la mise à jour inscrite, vous pouvez fermer l'outil Inscription de la mise à jour.

3. Ouvrez la console Configuration Manager, puis accédez à **Administration** > **Mises à jour et maintenance**. Les correctifs importés peuvent désormais être installés. (Avant la version 1702, les mises à jour et la maintenance s'effectuaient via le menu **Administration** > **Services cloud**.)

   Pour plus d'informations sur l'installation des mises à jour, consultez Installer des mises à jour dans la console pour System Center Configuration Manager

# Utiliser le programme d'installation de correctif logiciel pour installer les mises à jour de System Center Configuration Manager

22/06/2018 • 34 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Certaines mises à jour de System Center Configuration Manager indisponibles sur le service cloud Microsoft ne peuvent être obtenues que hors bande. C'est le cas, par exemple, d'un correctif logiciel en édition limitée destiné à résoudre un problème spécifique.
Si vous devez installer une mise à jour (ou un correctif logiciel) reçu de Microsoft et que le fichier de cette mise à jour porte un nom se terminant par l'extension **.exe** (pas **update.exe**), vous utilisez le programme d'installation du correctif logiciel inclus dans le téléchargement de celui-ci pour installer la mise à jour directement sur le serveur de site Configuration Manager.

Si l'extension du nom de fichier du correctif est **.update.exe**, consultez Importer des correctifs pour System Center Configuration Manager avec l'outil Inscription de la mise à jour.

> **NOTE**
> Cette rubrique fournit des indications générales sur la façon d'installer les correctifs pour la mise à jour de System Center Configuration Manager. Pour plus d'informations sur une mise à jour spécifique, reportez-vous à l'article correspondant de la Base de connaissances du Support Microsoft.

## Vue d'ensemble des correctifs logiciels pour Configuration Manager

Les correctifs logiciels pour Configuration Manager sont similaires à ceux publiés pour d'autres produits Microsoft, tels que SQL Server. Ils se composent d'un correctif individuel ou d'un groupe de correctifs (correctif cumulatif), et sont décrits dans la Base de connaissances Microsoft.

Les mises à jour individuelles se composent d'une seule mise à jour ciblée qui s'applique à une version spécifique de Configuration Manager.
Les groupes de mises à jour comprennent plusieurs mises à jour destinées à une version spécifique de Configuration Manager.
Vous ne pouvez pas installer séparément les mises à jour individuelles incluses dans un groupe de mises à jour.

Si vous envisagez de créer des déploiements pour installer des mises à jour sur des ordinateurs supplémentaires, vous devez installer le groupe de mises à jour sur un serveur de site d'administration centrale ou un serveur de site principal.

Quand vous exécutez le groupe de mises à jour, voici ce qui se produit :

- Le groupe de mises à jour extrait les fichiers de mise à jour de chaque composant concerné.
- Il démarre un Assistant qui vous guide tout au long du processus de configuration des mises à jour et des options de déploiement associées.
- À la fin de l'Assistant, les mises à jour du groupe qui s'appliquent au serveur de site sont installées sur ce dernier.

L'Assistant crée également des déploiements que vous pouvez utiliser pour installer les mises à jour sur des

ordinateurs supplémentaires. Vous déployez les mises à jour sur des ordinateurs supplémentaires en appliquant une méthode de déploiement prise en charge, comme un package de déploiement de logiciel ou Microsoft System Center Updates Publisher 2011.

Quand il s'exécute, l'Assistant crée sur le serveur de site un fichier **.cab** à utiliser avec Updates Publisher 2011. Si vous le souhaitez, vous pouvez configurer l'Assistant pour créer également un ou plusieurs packages de déploiement de logiciels. Vous pouvez utiliser ces déploiements pour installer des mises à jour de composants, tels que les clients ou la console Configuration Manager. Vous pouvez aussi installer les mises à jour manuellement sur des ordinateurs qui n'exécutent pas le client Configuration Manager.

Dans Configuration Manager, une mise à jour peut porter sur les trois groupes suivants :

- Rôles de serveur Configuration Manager, comprenant :
  - Site d'administration centrale
  - Site principal
  - Site secondaire
  - Fournisseur SMS distant
- Console Configuration Manager
- Client de Configuration Manager

> **NOTE**
> Les **mises à jour des rôles système de site** (dont celles destinées à la base de données du site et aux points de distribution cloud) sont installées dans le cadre de la mise à jour des services et serveurs de site par le Gestionnaire de composants de site.
>
> En revanche, les mises à jour des points de distribution d'extraction sont effectuées par le Gestionnaire de distribution plutôt que par le Gestionnaire de composants de site.

Chaque groupe de mises à jour applicable à Configuration Manager est un fichier .exe auto-extractible (SFX) qui contient les fichiers nécessaires à l'installation de la mise à jour sur les composants concernés de Configuration Manager. En règle générale, le fichier SFX peut contenir les fichiers suivants :

| FICHIER | DÉTAILS |
|---|---|
| <Version_produit>-QFE-KB<ID_article_Base_connaissances>-<plateforme>-<langue>.exe | Correspond au fichier de mise à jour. La ligne de commande pour ce fichier est gérée par Updatesetup.exe.<br><br>Par exemple :<br>CM1511RTM-QFE-KB123456-X64-ENU.exe |
| Updatesetup.exe | Ce wrapper .msi gère l'installation du groupe de mises à jour.<br><br>Lorsque vous exécutez la mise à jour, Updatesetup.exe détecte la langue d'affichage de l'ordinateur sur lequel elle s'exécute. Par défaut, l'interface utilisateur de la mise à jour est l'anglais. Toutefois, si la langue d'affichage est prise en charge, l'interface utilisateur s'affiche dans la langue locale de l'ordinateur. |
| Licence_<langue>.rtf | Le cas échéant, chaque mise à jour contient un ou plusieurs fichiers de licence en fonction des langues prises en charge. |

| FICHIER | DÉTAILS |
| --- | --- |
| <Produit&type_MàJ>-<version_produit>-<ID_article_Base_connaissances>-<plateforme>.msp | Quand la mise à jour concerne la console ou les clients Configuration Manager, le groupe de mises à jour inclut des fichiers correctifs Windows Installer (.msp) distincts.<br><br>Par exemple :<br><br>**Mise à jour de la console Configuration Manager :** ConfigMgr1511-AdminUI-KB1234567-i386.msp<br><br>**Mise à jour du client :** ConfigMgr1511-client-KB1234567-i386.msp<br>ConfigMgr1511-client-KB1234567-x64.msp |

Par défaut, le groupe de mises à jour enregistre ses actions dans un fichier .log sur le serveur de site. Le fichier journal possède le même nom que le groupe de mises à jour et est écrit dans le dossier **%SystemRoot%/Temp** .

Lors de son exécution, le groupe de mises à jour extrait un fichier ayant le même nom que le sien dans un dossier temporaire sur l'ordinateur, puis il exécute Updatesetup.exe. Updatesetup.exe démarre l'Assistant Mise à jour logicielle pour Configuration Manager<version du produit> <Numéro d'article de la Base de connaissances>.

En fonction de l'étendue de la mise à jour, l'Assistant crée une série de dossiers situés sous le dossier d'installation de System Center Configuration Manager sur le serveur de site. La structure de dossiers se présente de la façon suivante :
**\\<Nom_serveur>\SMS_<Code_site>\Hotfix\<Numéro_article_Base_connaissances>\<Type_MàJ>\<plateforme>**.

Le tableau suivant fournit des détails sur les dossiers figurant dans la structure de dossiers :

| NOM DE DOSSIER | PLUS D'INFORMATIONS |
| --- | --- |
| <Nom_serveur> | Nom du serveur de site sur lequel vous exécutez le groupe de mises à jour. |
| SMS_<code_site> | Nom de partage du dossier d'installation de Configuration Manager. |
| <Numéro_article_Base_connaissances> | Numéro d'identification de l'article de la Base de connaissances pour ce groupe de mises à jour. |

| NOM DE DOSSIER | PLUS D'INFORMATIONS |
| --- | --- |
| <Type_MàJ> | Type de mise à jour de Configuration Manager. L'Assistant crée un dossier distinct pour chaque type de mise à jour contenu dans le groupe de mises à jour. Les noms de dossier représentent les types de mise à jour. Il s'agit des dossiers suivants :<br><br>**Serveur**: comprend les mises à jour des serveurs de site, des serveurs de base de données de site et des ordinateurs qui exécutent le fournisseur SMS.<br><br>**Client** : inclut les mises à jour du client Configuration Manager.<br><br>**AdminConsole** : comprend les mises à jour de la console Configuration Manager.<br><br>Outre les types de mise à jour précédents, l'Assistant crée un dossier nommé **SCUP**. Ce dossier ne représente pas un type de mise à jour. Par contre, il contient le fichier .cab pour Updates Publisher. |
| <Plateforme> | Dossier propre à la plate-forme. Il contient les fichiers de mise à jour propres à un type de processeur. Ces dossiers sont les suivants :<br><br>- x64<br><br>- I386 |

## Comment installer des mises à jour

Pour installer des mises à jour, vous devez d'abord installer le groupe de mises à jour sur un serveur de site. Lorsque vous installez un groupe de mises à jour, l'Assistant Installation démarre pour effectuer cette mise à jour. Cet Assistant assure les tâches suivantes :

- Extraction des fichiers de mise à jour
- Aide à la configuration des déploiements
- Installation des mises à jour applicables sur les composants serveur de l'ordinateur local

Après avoir installé le groupe de mises à jour sur un serveur de site, vous pouvez ensuite mettre à jour des composants supplémentaires pour Configuration Manager. Le tableau suivant décrit les actions de mise à jour pour ces divers composants :

| COMPOSANT | INSTRUCTIONS |
| --- | --- |
| Serveur de site | Déployez les mises à jour sur un serveur de site distant si vous choisissez de ne pas installer le groupe de mises à jour directement sur ce serveur de site distant. |
| Base de données de site | Pour les serveurs de site distants, déployez les mises à jour serveur qui incluent une mise à jour de la base de données de site si vous n'installez pas le groupe de mises à jour directement sur ce serveur de site distant. |

| COMPOSANT | INSTRUCTIONS |
| --- | --- |
| Console Configuration Manager | Après l'installation initiale de la console Configuration Manager, vous pouvez installer les mises à jour de la console Configuration Manager sur chaque ordinateur qui exécute cette dernière. Vous ne pouvez pas modifier les fichiers d'installation de la console Configuration Manager pour appliquer les mises à jour pendant l'installation initiale de la console. |
| Fournisseur SMS distant | Installez les mises à jour pour chaque instance du fournisseur SMS qui s'exécute sur un autre ordinateur que le serveur de site sur lequel vous avez installé le groupe de mises à jour. |
| Clients Configuration Manager | Après l'installation initiale du client Configuration Manager, vous pouvez installer les mises à jour du client Configuration Manager sur chaque ordinateur qui exécute ce dernier. |

> **NOTE**
> Vous ne pouvez déployer les mises à jour que sur les ordinateurs qui exécutent le client Configuration Manager.

Si vous réinstallez un client, la console Configuration Manager ou le fournisseur SMS, vous devez également réinstaller les mises à jour de ces composants.

Pour installer les mises à jour sur chacun des composants de Configuration Manager, utilisez les informations figurant dans les sections suivantes.

### Mettre à jour les serveurs

Les mises à jour destinées aux serveurs peuvent englober des mises à jour pour les **sites**, la **site database**et les ordinateurs qui exécutent une instance du **fournisseur SMS**.

#### Mettre à jour un site

Pour mettre à jour un site Configuration Manager, vous pouvez installer le groupe de mises à jour directement sur le serveur de site ou déployer les mises à jour sur un serveur de site après avoir installé le groupe de mises à jour sur un site différent.

Lorsque vous installez une mise à jour sur un serveur de site, le processus d'installation de mise à jour gère les autres actions nécessaires à l'application de la mise à jour, telles que la mise à jour des rôles de système de site. La base de données de site constitue une exception. La section suivante contient des informations sur la façon de mettre à jour la base de données de site.

#### Mettre à jour une base de données de site

Pour mettre à jour la base de données de site, le processus d'installation exécute un fichier nommé **update.sql** dans la base de données de site. Vous pouvez configurer le processus de mise à jour pour mettre à jour automatiquement la base de données de site. Vous pouvez également choisir de mettre à jour manuellement la base de données de site à un moment ultérieur.

### Mise à jour automatique de la base de données de site

Lorsque vous installez le groupe de mises à jour sur un serveur de site, vous pouvez choisir de mettre à jour la base de données de site automatiquement lors de l'installation de la mise à niveau du serveur. Cette décision concerne uniquement le serveur de site sur lequel vous installez le groupe de mises à jour et ne s'applique pas aux déploiements créés pour installer les mises à jour sur des serveurs de site distants.

> **NOTE**
> Lorsque vous choisissez de mettre à jour automatiquement la base de données de site, le processus met à jour une base de données, que celle-ci réside sur le serveur de site ou sur un ordinateur distant.

> **IMPORTANT**
> Avant de mettre à jour la base de données de site, créez-en une sauvegarde. Vous ne pouvez pas désinstaller une mise à jour appliquée à la base de données de site. Pour plus d'informations sur la création d'une sauvegarde pour Configuration Manager, voir Sauvegarde et récupération pour System Center Configuration Manager.

### Mise à jour manuelle de la base de données de site

Si vous choisissez de ne pas mettre à jour automatiquement la base de données de site lors de l'installation du groupe de mises à jour sur le serveur de site, la mise à jour du serveur ne modifie pas la base de données du serveur de site sur lequel le groupe de mises à jour s'exécute. En revanche, des déploiements utilisant le package créé à des fins de déploiement de logiciels ou qui installe, mettent systématiquement à jour la base de données du site.

> **WARNING**
> Lorsque la mise à jour comporte des mises à jour pour le serveur de site et la base de données de site, la mise à jour n'est pas opérationnelle tant qu'elle n'est pas terminée à la fois sur le serveur de site et sur la base de données de site. Tant que la mise à jour n'est pas appliquée à la base de données du site, celui-ci est dans un état non pris en charge.

**Pour mettre à jour manuellement une base de données de site :**

1. Sur le serveur de site, arrêtez le service SMS_SITE_COMPONENT_MANAGER, puis arrêtez le service SMS_EXECUTIVE.
2. Fermez la console Configuration Manager.
3. Exécutez le script de mise à jour nommé **update.sql** sur la base de données de ce site. Pour plus d'informations sur la façon d'exécuter un script de mise à jour de base de données SQL Server, consultez la documentation de la version de SQL Server utilisée pour votre serveur de bases de données de site.
4. Redémarrez les services que vous avez arrêtés lors des étapes précédentes.
5. Pendant son installation, le groupe de mises à niveau extrait **update.sql** à l'emplacement suivant sur le serveur de site : **\\<Nom_serveur>\SMS_<code_site>\Hotfix\<Numéro_article_Base_connaissances>\update.sql**

#### Mettre à jour un ordinateur exécutant le fournisseur SMS

Après avoir installé un groupe de mises à jour incluant des mises à jour pour le fournisseur SMS, vous devez déployer la mise à jour sur chaque ordinateur qui exécute le fournisseur SMS. La seule exception est l'instance du fournisseur SMS précédemment installée sur le serveur de site sur lequel vous installez le groupe de mises à jour. L'instance locale du fournisseur SMS sur le serveur de site est mise à jour lorsque vous installez le groupe de mises à jour.

Si vous supprimez puis réinstallez le fournisseur SMS sur un ordinateur, vous devez alors réinstaller la mise à jour pour le fournisseur SMS sur cet ordinateur.

### Mettre à jour des clients

Lorsque vous installez une mise à jour incluant des mises à jour pour le clients Configuration Manager, vous avez le choix entre mettre à niveau automatiquement les clients avec l'installation de la mise à jour ou les mettre à

niveau manuellement plus tard. Pour plus d'informations sur la mise à niveau automatique des clients, consultez Comment mettre à niveau les clients pour les ordinateurs Windows dans System Center Configuration Manager.

Vous pouvez déployer des mises à jour avec Updates Publisher ou avec un package de déploiement de logiciel, ou vous pouvez choisir d'installer manuellement la mise à jour sur chaque client. Pour plus d'informations sur l'utilisation des déploiements dans le cadre de l'installation des mises à jour, consultez la section Déployer des mises à jour pour Configuration Manager dans cette rubrique.

> **IMPORTANT**
> Lorsque vous installez des mises à jour pour des clients, et que le groupe de mises à jour comprend des mises à jour pour des serveurs, assurez-vous d'installer également les mises à jour serveur sur le site principal auquel les clients sont attribués.

Pour installer manuellement la mise à jour du client, sur chaque client Configuration Manager, vous devez exécuter le fichier **Msiexec.exe** et référencer le fichier .msp de mise à jour client spécifique à la plateforme.

Par exemple, vous pouvez utiliser la ligne de commande suivante pour une mise à jour client. Cette ligne de commande exécute MSIEXEC sur l'ordinateur client et fait référence au fichier .msp que le groupe de mises à jour a extrait sur le serveur de site : **msiexec.exe /p \\<Nom_serveur>\SMS_<Code_site>\Hotfix\<Numéro_article_Base_de_connaissances>\Client\<Plateforme>\<msp> /L*v <fichier_journal>REINSTALLMODE=mous REINSTALL=ALL**

**Mettre à jour des consoles Configuration Manager**

Pour mettre à jour une console Configuration Manager, après l'installation initiale de la console, vous devez installer la mise à jour sur l'ordinateur qui exécute cette dernière.

> **IMPORTANT**
> Quand vous installez des mises à jour pour la console Configuration Manager et que le groupe de mises à jour comprend des mises à jour pour les serveurs, veillez à également installer les mises à jour de serveur sur le site que vous utilisez avec la console Configuration Manager.

Si l'ordinateur que vous mettez à jour exécute le client Configuration Manager :

- Vous pouvez utiliser un déploiement pour installer la mise à jour. Pour plus d'informations sur l'utilisation des déploiements dans le cadre de l'installation des mises à jour, consultez la section Déployer des mises à jour pour Configuration Manager dans cette rubrique.
- Si vous êtes connecté directement à l'ordinateur client, vous pouvez exécuter l'installation de manière interactive.
- Vous pouvez installer manuellement la mise à jour sur chaque ordinateur. Pour installer manuellement la mise à jour de la console Configuration Manager, sur chaque ordinateur qui exécute la console Configuration Manager, vous pouvez exécuter le fichier Msiexec.exe et faire référence au fichier .msp de mise à jour de la console Configuration Manager.

Par exemple, vous pouvez utiliser la ligne de commande suivante pour mettre à jour une console Configuration Manager. Cette ligne de commande exécute MSIEXEC sur l'ordinateur et fait référence au fichier .msp que le groupe de mises à jour a extrait sur le serveur de site : **msiexec.exe /p \\<Nom_serveur>\SMS_<Code_site>\Hotfix\<Numéro_article_Base_connaissances>\AdminConsole\<Plateforme>\<msp> /L*v <fichier_journal>REINSTALLMODE=mous REINSTALL=ALL**

## Déployer des mises à jour pour Configuration Manager

Après avoir installé le groupe de mises à jour sur un serveur de site, vous pouvez utiliser l'une des trois méthodes

suivantes pour déployer des mises à jour sur des ordinateurs supplémentaires.

**Utiliser Updates Publisher 2011 pour installer des mises à jour**

Lorsque vous installez le groupe de mises à jour sur un serveur de site, l'Assistant Installation crée un fichier catalogue pour l'éditeur de mise à jour, que vous pouvez utiliser pour déployer les mises à jour sur les ordinateurs concernés. L'Assistant crée toujours ce catalogue, même quand vous sélectionnez l'option **Use package and program to deploy this update**.

Le catalogue de l'éditeur de mise à jour est nommé **SCUPCatalog.cab** et se trouve sur l'ordinateur sur lequel s'exécute le groupe de mises à jour logicielles à l'emplacement suivant : **\\<nom_serveur>\SMS_<code_site>\Hotfix\<Numéro_article_Base_connaissances>\SCUP\SCUPCatalog.cab**

> **IMPORTANT**
> Dans la mesure où le fichier SCUPCatalog.cab est créé à l'aide de chemins spécifiques du serveur de site sur lequel le groupe de mises à jour est installé, il ne peut pas être utilisé sur d'autres serveurs de site.

Une fois l'exécution de l'Assistant terminée, vous pouvez importer le catalogue dans l'éditeur de mise à jour, puis utiliser les mises à jour logicielles de Configuration Manager pour déployer les mises à jour. Pour plus d'informations sur l'éditeur de mise à jour, voir Updates Publisher 2011 dans la bibliothèque TechNet pour System Center 2012.

Utilisez la procédure suivante pour importer le fichier SCUPCatalog.cab vers Updates Publisher et publier les mises à jour.

**Pour importer les mises à jour vers Updates Publisher 2011**

1. Démarrez la console de l'éditeur de mise à jour et cliquez sur **Importer**.
2. Sur la page **Type d'importation** de l'Assistant Importation de catalogue des mises à jour logicielles, sélectionnez **Specify the path to the catalog to import**(Spécifier le chemin vers ce catalogue à importer), puis spécifiez le fichier SCUPCatalog.cab.
3. Cliquez sur **Suivant**, puis cliquez sur **Suivant** de nouveau.
4. Dans la boîte de dialogue **Avertissement de sécurité - Validation du catalogue** , cliquez sur **Accepter**. Fermez l'Assistant une fois la procédure terminée.
5. Dans la console de l'éditeur de mise à jour, sélectionnez la mise à jour à déployer, puis cliquez sur **Publier**.
6. Sur la page **Options de publication** de l'Assistant Publication des mises à jour logicielles, sélectionnez le **contenu complet**, puis cliquez sur **Suivant**.
7. Terminez l'Assistant pour publier les mises à jour.

**Utiliser le déploiement logiciel pour installer des mises à jour**

Lorsque vous installez le groupe de mises à jour sur le serveur de site d'un site principal ou d'un site d'administration centrale, vous pouvez configurer l'Assistant Installation pour créer des packages de mise à jour pour le déploiement de logiciels. Vous pouvez alors déployer chaque package sur un regroupement d'ordinateurs que vous voulez mettre à jour.

Pour créer un package de déploiement de logiciels, sur la page de **configuration de déploiement de mises à jour logicielles** de l'Assistant, activez la case à cocher de chaque type de package de mises à jour à mettre à jour. Les types disponibles peuvent inclure des serveurs, des console Configuration Manager et des clients. Un package distinct est créé pour chaque type de mise à jour que vous sélectionnez.

> **NOTE**
> Le package pour serveurs contient des mises à jour pour les composants suivants :
>
> - Serveur de site
> - Fournisseur SMS
> - Base de données de site

Ensuite, sur la page de **configuration de la méthode de déploiement de mises à jour logicielles** de l'Assistant, sélectionnez l'option **I will use software distribution**(Je vais utiliser la distribution de logiciels). Cette sélection indique à l'Assistant de créer les packages de déploiement de logiciels.

Une fois l'Assistant terminé, les packages créés apparaissent dans la console Configuration Manager, dans le nœud **Packages** de l'espace de travail **Bibliothèque de logiciels**. Vous pouvez ensuite utiliser votre processus standard pour déployer des packages logiciels sur des clients Gestionnaire de configuration. Lorsqu'un package s'exécute sur un client, il installe les mises à jour pour les composants applicables de Configuration Manager sur l'ordinateur client.

Pour plus d'informations sur le déploiement des packages vers des clients Configuration Manager, voir System Center Configuration Manager.

### Créer des regroupements pour déployer des mises à jour sur Configuration Manager

Vous pouvez déployer des mises à jour spécifiques vers les clients applicables. Les informations suivantes peuvent vous aider à créer des regroupements d'appareils pour les différents composants de Configuration Manager.

| COMPOSANT DE CONFIGURATION MANAGER | INSTRUCTIONS |
|---|---|
| Serveur de site d'administration centrale | Créez une requête d'adhésion directe et ajoutez l'ordinateur serveur du site d'administration centrale. |
| Tous les serveurs de site principal | Créez une requête d'adhésion directe et ajoutez chaque ordinateur serveur de site principal. |
| Tous les serveurs de site secondaire | Créez une requête d'adhésion directe et ajoutez chaque ordinateur serveur de site secondaire. |
| Tous les clients x86 | Créez un regroupement avec les critères de requête suivants :<br><br>**Select * from SMS_R_System inner join SMS_G_System_SYSTEM on SMS_G_System_SYSTEM.ResourceID = SMS_R_System.ResourceId where SMS_G_System_SYSTEM.SystemType = "X86-based PC"** |
| Tous les clients x64 | Créez un regroupement avec les critères de requête suivants :<br><br>**Select * from SMS_R_System inner join SMS_G_System_SYSTEM on SMS_G_System_SYSTEM.ResourceID = SMS_R_System.ResourceId where SMS_G_System_SYSTEM.SystemType = "X64-based PC"** |
| Tous les ordinateurs qui exécutent la console Configuration Manager | Créez une requête d'adhésion directe et ajoutez chaque ordinateur. |

| COMPOSANT DE CONFIGURATION MANAGER | INSTRUCTIONS |
| --- | --- |
| Ordinateurs distants exécutant une instance du fournisseur SMS | Créez une requête d'adhésion directe et ajoutez chaque ordinateur. |

> **NOTE**
> Pour mettre à jour une base de données de site, déployez la mise à jour vers le serveur de site de ce site.

Pour plus d'informations sur la création de regroupements, consultez Comment créer des regroupements dans Configuration Manager.

# Liste de contrôle pour l'installation de la mise à jour 1802 pour System Center Configuration Manager

18/06/2018 • 25 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Quand vous utilisez Current Branch de System Center Configuration Manager, vous pouvez installer la mise à jour dans la console de la version 1802 pour mettre à jour votre hiérarchie à partir d'une version antérieure. (Comme la version 1802 est également disponible en tant que support de base de référence, vous pouvez utiliser le support d'installation pour installer le premier site d'une nouvelle hiérarchie.)

Pour obtenir la mise à jour de la version 1802, vous devez utiliser un point de connexion de service sur le site de niveau supérieur de votre hiérarchie. Ce rôle de système de site peut être en mode en ligne ou hors connexion. Une fois que votre hiérarchie a téléchargé la mise à jour Microsoft, celle-ci est accessible dans la console de l'espace de travail **Administration**, sous le nœud **Mises à jour et maintenance**.

- Quand la mise à jour est répertoriée comme **disponible**, elle est prête à être installée. Avant d'installer la version 1802, passez en revue les informations suivantes sur l'installation de la mise à jour 1802 et la liste de contrôle pour connaître les configurations à effectuer avant de commencer la mise à jour.
- Si la mise à jour s'affiche en tant que **Téléchargement en cours** et ne change pas, recherchez les erreurs dans les journaux **hman.log** et **dmpdownloader.log**.
    - Si dmpdownloader.log indique que le processus dmpdownloader est en veille en attendant la vérification des mises à jour, vous pouvez redémarrer le service **SMS_Executive** sur le serveur de site pour redémarrer le téléchargement des fichiers de redistribution de la mise à jour.
    - Un autre problème courant de téléchargement se produit quand les paramètres du serveur proxy empêchent les téléchargements à partir de http://silverlight.dlservice.microsoft.com et http://download.microsoft.com.

Pour plus d'informations sur l'installation des mises à jour, consultez Mises à jour et maintenance dans la console.

Pour plus d'informations sur les versions de Current Branch, consultez Versions de base et de mise à jour dans Mises à jour pour System Center Configuration Manager.

## À propos de l'installation de la mise à jour 1802

**Sites :**
Vous pouvez installer la mise à jour 1802 sur le site de niveau supérieur de votre hiérarchie. Cela signifie que vous lancez l'installation à partir de votre site d'administration centrale si en avez un, ou à partir de votre site principal autonome. Après l'installation de la mise à jour sur le site de niveau supérieur, les sites enfants ont le comportement de mise à jour suivant :

- Les sites principaux enfants installent automatiquement la mise à jour quand le site d'administration centrale a fini de l'installer. Vous pouvez utiliser des fenêtres de service pour spécifier à quel moment un site installe la mise à jour. Pour plus d'informations, consultez Fenêtres de maintenance pour les serveurs de site.
- Après que le site parent principal a installé la mise à jour, vous devez mettre à jour manuellement chacun des sites secondaires à partir de la console Configuration Manager. La mise à jour automatique des serveurs de sites secondaires n'est pas prise en charge.

**Rôles de système de site :**
Quand un serveur de site installe la mise à jour, les rôles de système de site installés sur l'ordinateur serveur de site et sur des ordinateurs distants sont automatiquement mis à jour. Avant d'installer la mise à jour, vérifiez que chaque serveur de système de site remplit les prérequis pour les opérations avec la nouvelle version de mise à jour.

**Consoles Configuration Manager :**
La première fois que vous utilisez une console Configuration Manager à l'issue de la mise à jour, vous êtes invité à mettre à jour cette console. Pour cela, vous devez exécuter le programme d'installation de Configuration Manager sur l'ordinateur hébergeant la console, puis choisir l'option de mise à jour de la console. Nous vous recommandons de ne pas retarder l'installation de la mise à jour sur la console.

> **IMPORTANT**
> Lorsque vous installez une mise à jour sur le site d'administration centrale, tenez compte des limitations suivantes et des retards qui se produisent jusqu'à ce que tous les sites principaux enfants aient également terminé l'installation de la mise à jour :
>
> - La **mise à niveau des clients** ne démarre pas. Cela comprend la mise à jour automatique des clients et des clients en préproduction. En outre, il n'est pas possible de mettre en production les clients en préproduction tant que le dernier site n'a pas terminé l'installation de la mise à jour. Après l'installation de la mise à jour sur le dernier site, la mise à niveau des clients commence, en fonction de vos options de configuration.
> - Les **nouvelles fonctionnalités** que vous activez avec la mise à jour ne sont pas disponibles. L'objectif est d'éviter l'envoi de la réplication de données associées à cette fonctionnalité à un site qui n'a pas encore installé la prise en charge de cette fonctionnalité. Après l'installation de la mise à jour sur tous les sites principaux, la fonctionnalité sera utilisable.
> - Les **liens de réplication** entre le site d'administration centrale et les sites principaux enfants apparaissent comme non mis à niveau. Cela se présente, dans l'état d'installation du pack de mise à jour, sous la forme d'un état Terminé avec un avertissement pour l'initialisation de la surveillance de la réplication. Dans le nœud Surveillance de la console, cela se présente sous l'état *Lien en cours de configuration*.

## Liste de contrôle

**Vérifiez que tous les sites exécutent une version de System Center Configuration Manager qui prend en charge la mise à jour vers 1802 :**
Chaque serveur de site de la hiérarchie doit exécuter la même version de System Center Configuration Manager pour que vous puissiez lancer l'installation de la mise à jour 1802. Pour passer à la version 1802, vous devez utiliser la version 1702, 1706 ou 1710.

**Vérifiez l'état de votre contrat Software Assurance ou des droits d'abonnement équivalents :**
Vous devez disposer d'un contrat Software Assurance (SA) actif pour installer la mise à jour 1802. Quand vous installez cette mise à jour, l'onglet **Licences** propose l'option vous permettant de confirmer la **date d'expiration de Software Assurance**.

Il s'agit d'une valeur facultative que vous pouvez spécifier pour des raisons pratiques et qui vous servira de rappel concernant la date d'expiration de votre licence. Cette date est visible lorsque vous installez des mises à jour ultérieures. Vous avez peut-être déjà spécifié cette valeur pendant la configuration ou l'installation d'une mise à jour, ou en utilisant l'onglet **Licences** de **Paramètres de hiérarchie**, sur la console de Configuration Manager.

Pour plus d'informations, consultez Licences et branches pour System Center Configuration Manager.

**Examinez les versions installées de Microsoft .NET sur les serveurs de système de site** : quand un site installe cette mise à jour, Configuration Manager installe automatiquement le .NET Framework 4.5.2 sur chaque ordinateur hébergeant un des rôles de système de site suivants (si le .NET Framework 4.5 ou ultérieur n'est pas déjà installé) :

- Point proxy d'inscription

- Point d'inscription
- Point de gestion
- Point de connexion de service

Cette installation peut mettre le serveur de système de site en état d'attente de redémarrage, et signaler des erreurs sur l'Afficheur des messages d'état du composant Configuration Manager. En outre, des applications .NET sur le serveur peuvent présenter des défaillances aléatoires jusqu'au redémarrage du serveur.

Pour plus d'informations, consultez Prérequis des sites et systèmes de site.

**Vérifiez la version du Kit de déploiement et d'évaluation (ADK) Windows pour Windows 10** : la version de Windows 10 ADK doit être 1703 ou ultérieure. (Pour plus d'informations sur les versions de Windows ADK prises en charge, consultez Windows 10 ADK.) Si vous devez mettre à jour Windows ADK, faites-le avant de commencer la mise à jour de Configuration Manager. Les images de démarrage par défaut seront ainsi mises à jour automatiquement vers la dernière version de Windows PE. (Les images de démarrage personnalisé doivent être mises à jour manuellement.)

Si vous mettez à jour le site avant de mettre à jour Windows ADK, consultez Mettre à jour les points de distribution avec l'image de démarrage.

**Examinez l'état du site et de la hiérarchie, et vérifiez l'absence de tout problème non résolu :** avant de mettre à jour un site, résolvez tous les problèmes opérationnels pour le serveur de site, le serveur de bases de données du site et les rôles de système de site installés sur des ordinateurs distants. Une mise à niveau de site peut échouer en raison de l'existence de problèmes opérationnels.

Pour plus d'informations, voir Utiliser des alertes et le système d'état pour System Center Configuration Manager.

**Examinez la réplication des fichiers et données entre sites :**
vérifiez que la réplication des fichiers et bases de données entre les sites est opérationnelle et active. Des retards ou backlogs dans ces domaines peuvent perturber ou empêcher la mise à jour. Pour la réplication de la base de données, vous pouvez utiliser l'Analyseur de lien de réplication pour faciliter la résolution des problèmes avant de commencer la mise à jour.

Pour plus d'informations, consultez À propos de l'analyseur de lien de réplication dans la rubrique Surveiller l'infrastructure de la hiérarchie et de la réplication dans System Center Configuration Manager.

**Installez toutes les mises à jour critiques applicables pour les systèmes d'exploitation sur les ordinateurs hébergeant le site, le serveur de base de données du site et les rôles de système de site distants :** avant d'installer une mise à jour pour Configuration Manager, installez toutes les mises à jour critiques pour chaque système de site concerné. Si vous installez une mise à jour qui nécessite un redémarrage, redémarrez les ordinateurs concernés avant d'entreprendre la mise à jour.

**Désactivez les réplicas de base de données pour les points de gestion au niveau des sites principaux :**
Configuration Manager ne peut pas réussir la mise à jour d'un site principal ayant un réplica de base de données activé pour les points de gestion. Désactivez la réplication de base de données avant d'installer une mise à jour pour Configuration Manager.

Pour plus d'informations, consultez Réplicas de base de données pour les points de gestion de System Center Configuration Manager.

**Définissez un basculement manuel pour les groupes de disponibilité SQL Server AlwaysOn :**
Si vous utilisez un groupe de disponibilité, vérifiez qu'il est défini sur le basculement manuel avant de commencer l'installation de la mise à jour. Une fois le site mis à jour, vous pouvez restaurer le basculement automatique. Pour plus d'informations, consultez SQL Server AlwaysOn pour une base de données de site.

**Reconfigurez les points de mise à jour logicielle qui utilisent l'équilibrage de la charge réseau (NLB) :**

Configuration Manager ne peut pas mettre à jour un site qui utilise un cluster d'équilibrage de la charge réseau

(NLB) pour héberger des points de mise à jour logicielle.

Si vous utilisez des clusters NLB pour les points de mise à jour logicielle, utilisez Windows PowerShell pour supprimer le cluster NLB. Pour plus d'informations, consultez Planifier les mises à jour logicielles dans System Center Configuration Manager.

**Désactivez toutes les tâches de maintenance de site sur chaque site pendant la durée de l'installation de la mise à jour sur ce site :**
Avant d'installer la mise à jour, désactivez toutes les tâches de maintenance de site qui peuvent s'exécuter pendant le processus de mise à jour. Cela inclut, sans toutefois s'y limiter, les tâches suivantes :

- Serveur de site de sauvegarde
- Supprimer les anciennes opérations du client
- Supprimer les données de découverte anciennes

Si une tâche de maintenance de base de données du site s'exécute pendant l'installation de la mise à jour, celle-ci peut échouer. Avant de désactiver une tâche, enregistrez sa planification pour pouvoir restaurer sa configuration une fois la mise à jour installée.

Pour plus d'informations, consultez Tâches de maintenance pour System Center Configuration Manager et Référence des tâches de maintenance pour System Center Configuration Manager.

**Arrêtez temporairement tout logiciel antivirus sur les serveurs System Center Configuration Manager :** avant de mettre à jour un site, vérifiez que vous avez arrêté tout logiciel antivirus sur les serveurs Configuration Manager.

**Créez une sauvegarde de la base de données du site d'administration centrale et des sites principaux :** avant de mettre à jour un site, sauvegardez sa base de données pour être certain de disposer d'une sauvegarde correcte utilisable en cas de récupération d'urgence.

Pour plus d'informations, consultez Sauvegarde et récupération pour System Center Configuration Manager.

**Planifiez un test du client :**
Quand vous installez une mise à jour qui affecte le client, vous pouvez la tester en mode préproduction avant de procéder au déploiement et à la mise à niveau de votre client actif.

Pour tirer parti de cette option, vous devez configurer votre site pour qu'il prenne en charge les mises à niveau automatiques pour la préproduction avant de commencer l'installation de la mise à jour.

Pour plus d'informations, consultez Mettre à niveau les clients dans System Center Configuration Manager et Comment tester les mises à niveau du client dans un regroupement de préproduction dans System Center Configuration Manager.

**Planifiez l'utilisation des fenêtres de service pour contrôler le moment auquel les serveurs de site installent les mises à jour :**
Utilisez les fenêtres de service pour définir une période au cours de laquelle les mises à jour à un serveur de site peuvent être installées.

Cela peut vous aider à contrôler le moment où les sites au sein de votre hiérarchie installent la mise à jour. Pour plus d'informations, consultez Fenêtres de maintenance pour les serveurs de site.

**Passez en revue les extensions prises en charge :**

Si vous étendez Configuration Manager avec d'autres produits Microsoft ou partenaires, vérifiez que ces produits prennent en charge la version 1802. Demandez cette information au fournisseur du produit. Par exemple, consultez les notes de publication de Microsoft Deployment Toolkit.

**Exécutez l'outil de vérification des prérequis du programme d'installation :**
Quand la mise à jour est répertoriée dans la console comme **Disponible**, vous pouvez exécuter indépendamment

l'outil de vérification des prérequis avant d'installer la mise à jour. (Quand vous installez la mise à jour sur le site, l'outil de vérification des prérequis s'exécute à nouveau.)

Pour exécuter une vérification des prérequis à partir de la console, accédez à l'espace de travail **Administration**, puis sélectionnez **Mises à jour et maintenance**. Sélectionnez la mise à jour **Configuration Manager 1802**, puis cliquez sur **Exécuter la vérification des prérequis** dans le ruban.

Pour plus d'informations sur le démarrage et la surveillance de la vérification des prérequis, consultez **Étape 3 : exécuter l'outil de vérification des prérequis avant d'installer une mise à jour** dans la rubrique Installer des mises à jour dans la console pour System Center Configuration Manager.

> **IMPORTANT**
> Quand l'outil de vérification des prérequis s'exécute indépendamment ou dans le cadre de l'installation d'une mise à jour, le processus met à jour certains fichiers sources du produit qui sont utilisés pour les tâches de maintenance de site. Par conséquent, après l'exécution de l'outil de vérification des prérequis, mais avant l'installation de la mise à jour, si vous devez effectuer une tâche de maintenance de site, exécutez **Setupwfe.exe** (programme d'installation de Configuration Manager) à partir du dossier CD.Latest sur le serveur de site.

**Mettez à jour les sites :**
Vous êtes maintenant prêt à commencer l'installation de la mise à jour pour votre hiérarchie. Pour plus d'informations sur l'installation de la mise à jour, consultez Installer des mises à jour dans la console.

Nous vous recommandons de planifier l'installation de la mise à jour en dehors des heures de bureau normales pour chaque site, quand le processus d'installation de la mise à jour et ses actions pour réinstaller les composants du site et les rôles de système de site auront le moins d'effet sur les opérations de votre entreprise.

Pour plus d'informations, consultez Mises à jour pour System Center Configuration Manager.

## Liste de contrôle post-mise à jour

Vérifiez et effectuez les actions suivantes après la fin de l'installation de la mise à jour.

1. Assurez-vous que la réplication de site à site est active. Dans la console, affichez **Surveillance** > **Hiérarchie de site** et **Surveillance** > **Réplication de la base de données** pour accéder à des indications concernant les problèmes ou à la confirmation que les liens de réplication sont actifs.
2. Assurez-vous que chaque serveur de site et chaque rôle de système de site est passé à la version 1802. Dans la console, vous pouvez ajouter la colonne facultative **Version** à l'affichage de certains nœuds, y compris **Sites** et **Points de distribution**.

   Lorsque c'est nécessaire, un rôle de système de site se réinstalle automatiquement pour passer à la nouvelle version. Redémarrez les systèmes de site distants qui ne se mettent pas à jour correctement.
3. Reconfigurez les réplicas de base de données des points de gestion au niveau des sites principaux que vous avez désactivés avant de commencer la mise à jour.
4. Reconfigurez les tâches de maintenance de la base de données que vous avez désactivées avant de commencer la mise à jour.
5. Si vous avez configuré le pilotage des clients avant d'installer la mise à jour, mettez à niveau les clients selon le plan que vous avez créé.
6. Si vous utilisez des extensions Configuration Manager, mettez-les à jour vers la version la plus récente pour qu'elles prennent en charge cette mise à jour Configuration Manager.

# Liste de contrôle pour l'installation de la mise à jour 1710 pour System Center Configuration Manager

22/06/2018 • 24 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Quand vous utilisez Current Branch de System Center Configuration Manager, vous pouvez installer la mise à jour dans la console de la version 1710 pour mettre à jour votre hiérarchie à partir d'une version antérieure.

Pour obtenir la mise à jour de la version 1710, vous devez utiliser un rôle de système de site de point de connexion de service sur le site de niveau supérieur de votre hiérarchie. Cela peut être en mode en ligne ou hors connexion. Une fois que votre hiérarchie a téléchargé le package de mises à jour de Microsoft, celui-se trouve dans la console sous **Administration > Vue d'ensemble > Services cloud > Mises à jour et maintenance**.

- Quand la mise à jour est répertoriée comme **disponible**, elle est prête à être installée. Avant d'installer la version 1710, passez en revue les informations suivantes sur l'installation de la mise à jour 1710 et la liste de contrôle pour connaître les configurations à effectuer avant de commencer la mise à jour.
- Si la mise à jour s'affiche en tant que **Téléchargement en cours** et ne change pas, recherchez les erreurs dans les journaux **hman.log** et **dmpdownloader.log**.
    - Si dmpdownloader.log indique que le processus dmpdownloader est en veille en attendant la vérification des mises à jour, vous pouvez redémarrer le service **SMS_Executive** sur le serveur de site pour redémarrer le téléchargement des fichiers de redistribution de la mise à jour.
    - Un autre problème courant de téléchargement se produit quand les paramètres du serveur proxy empêchent les téléchargements à partir de http://silverlight.dlservice.microsoft.com et http://download.microsoft.com.

Pour plus d'informations sur l'installation des mises à jour, consultez Mises à jour et maintenance dans la console.

Pour plus d'informations sur les versions de Current Branch, consultez Versions de base et de mise à jour dans Mises à jour pour System Center Configuration Manager.

## À propos de l'installation de la mise à jour 1710

**Sites :**
Vous pouvez installer la mise à jour 1710 sur le site de niveau supérieur de votre hiérarchie. Cela signifie que vous lancez l'installation à partir de votre site d'administration centrale si en avez un, ou à partir de votre site principal autonome. Après l'installation de la mise à jour sur le site de niveau supérieur, les sites enfants ont le comportement de mise à jour suivant :

- Les sites principaux enfants installent automatiquement la mise à jour quand le site d'administration centrale a fini de l'installer. Vous pouvez utiliser des fenêtres de service pour spécifier à quel moment un site installe la mise à jour. Pour plus d'informations, consultez Fenêtres de maintenance pour les serveurs de site.
- Après que le site parent principal a installé la mise à jour, vous devez mettre à jour manuellement chacun des sites secondaires à partir de la console Configuration Manager. La mise à jour automatique des serveurs de sites secondaires n'est pas prise en charge.

**Rôles de système de site :**

Quand un serveur de site installe la mise à jour, les rôles de système de site installés sur l'ordinateur serveur de site et sur des ordinateurs distants sont automatiquement mis à jour. Avant d'installer la mise à jour, vérifiez que chaque serveur de système de site remplit les prérequis pour les opérations avec la nouvelle version de mise à jour.

**Consoles Configuration Manager :**
La première fois que vous utilisez une console Configuration Manager à l'issue de la mise à jour, vous êtes invité à mettre à jour cette console. Pour cela, vous devez exécuter le programme d'installation de Configuration Manager sur l'ordinateur hébergeant la console, puis choisir l'option de mise à jour de la console. Nous vous recommandons de ne pas retarder l'installation de la mise à jour sur la console.

> **IMPORTANT**
> Lorsque vous installez une mise à jour sur le site d'administration centrale, tenez compte des limitations suivantes et des retards qui se produisent jusqu'à ce que tous les sites principaux enfants aient également terminé l'installation de la mise à jour :
>
> - La **mise à niveau des clients** ne démarre pas. Cela comprend la mise à jour automatique des clients et des clients en préproduction. En outre, il n'est pas possible de mettre en production les clients en préproduction tant que le dernier site n'a pas terminé l'installation de la mise à jour. Après l'installation de la mise à jour sur le dernier site, la mise à niveau des clients commence, en fonction de vos options de configuration.
> - Les **nouvelles fonctionnalités** que vous activez avec la mise à jour ne sont pas disponibles. L'objectif est d'éviter l'envoi de la réplication de données associées à cette fonctionnalité à un site qui n'a pas encore installé la prise en charge de cette fonctionnalité. Après l'installation de la mise à jour sur tous les sites principaux, la fonctionnalité sera utilisable.
> - Les **liens de réplication** entre le site d'administration centrale et les sites principaux enfants apparaissent comme non mis à niveau. Cela se présente, dans l'état d'installation du pack de mise à jour, sous la forme d'un état Terminé avec un avertissement pour l'initialisation de la surveillance de la réplication. Dans le nœud Surveillance de la console, cela se présente sous l'état *Lien en cours de configuration*.

## Liste de contrôle

**Vérifiez que tous les sites exécutent une version de System Center Configuration Manager qui prend en charge la mise à jour vers 1710 :**
Chaque serveur de site de la hiérarchie doit exécuter la même version de System Center Configuration Manager pour que vous puissiez lancer l'installation de la mise à jour 1710. Pour passer à la version 1710, vous devez utiliser la version 1610, 1702 ou 1706.

**Vérifiez l'état de votre contrat Software Assurance ou des droits d'abonnement équivalents :**
Vous devez disposer d'un contrat Software Assurance (SA) actif pour installer la mise à jour 1710. Quand vous installez cette mise à jour, l'onglet **Licences** propose l'option vous permettant de confirmer la **date d'expiration de Software Assurance**.

Il s'agit d'une valeur facultative que vous pouvez spécifier pour des raisons pratiques et qui vous servira de rappel concernant la date d'expiration de votre licence. Cette date est visible lorsque vous installez des mises à jour ultérieures. Vous avez peut-être déjà spécifié cette valeur pendant la configuration ou l'installation d'une mise à jour, ou en utilisant l'onglet **Licences** de **Paramètres de hiérarchie**, sur la console de Configuration Manager.

Pour plus d'informations, consultez Licences et branches pour System Center Configuration Manager.

**Examinez les versions installées de Microsoft .NET sur les serveurs de système de site** : quand un site installe cette mise à jour, Configuration Manager installe automatiquement le .NET Framework 4.5.2 sur chaque ordinateur hébergeant un des rôles de système de site suivants (si le .NET Framework 4.5 ou ultérieur n'est pas déjà installé) :

- Point proxy d'inscription
- Point d'inscription

- Point de gestion
- Point de connexion de service

Cette installation peut mettre le serveur de système de site en état d'attente de redémarrage, et signaler des erreurs sur l'Afficheur des messages d'état du composant Configuration Manager. En outre, des applications .NET sur le serveur peuvent présenter des défaillances aléatoires jusqu'au redémarrage du serveur.

Pour plus d'informations, consultez Prérequis des sites et systèmes de site.

**Vérifiez la version du Kit de déploiement et d'évaluation (ADK) Windows pour Windows 10** : la version de Windows 10 ADK doit être 1703 ou ultérieure. (Pour plus d'informations sur les versions de Windows ADK prises en charge, consultez Windows 10 ADK.) Si vous devez mettre à jour Windows ADK, faites-le avant de commencer la mise à jour de Configuration Manager. Les images de démarrage par défaut seront ainsi mises à jour automatiquement vers la dernière version de Windows PE. (Les images de démarrage personnalisé doivent être mises à jour manuellement.)

Si vous mettez à jour le site avant de mettre à jour Windows ADK, consultez Mettre à jour les points de distribution avec l'image de démarrage pour découvrir les améliorations apportées à ce processus dans Configuration Manager version 1710.

**Examinez l'état du site et de la hiérarchie, et vérifiez l'absence de tout problème non résolu :** avant de mettre à jour un site, résolvez tous les problèmes opérationnels pour le serveur de site, le serveur de bases de données du site et les rôles de système de site installés sur des ordinateurs distants. Une mise à niveau de site peut échouer en raison de l'existence de problèmes opérationnels.

Pour plus d'informations, voir Utiliser des alertes et le système d'état pour System Center Configuration Manager.

**Examinez la réplication des fichiers et données entre sites :**
vérifiez que la réplication des fichiers et bases de données entre les sites est opérationnelle et active. Des retards ou backlogs dans ces domaines peuvent perturber ou empêcher la mise à jour. Pour la réplication de la base de données, vous pouvez utiliser l'Analyseur de lien de réplication pour faciliter la résolution des problèmes avant de commencer la mise à jour.

Pour plus d'informations, consultez À propos de l'analyseur de lien de réplication dans la rubrique Surveiller l'infrastructure de la hiérarchie et de la réplication dans System Center Configuration Manager.

**Installez toutes les mises à jour critiques applicables pour les systèmes d'exploitation sur les ordinateurs hébergeant le site, le serveur de base de données du site et les rôles de système de site distants :** avant d'installer une mise à jour pour Configuration Manager, installez toutes les mises à jour critiques pour chaque système de site concerné. Si vous installez une mise à jour qui nécessite un redémarrage, redémarrez les ordinateurs concernés avant d'entreprendre la mise à jour.

**Désactivez les réplicas de base de données pour les points de gestion au niveau des sites principaux :**
Configuration Manager ne peut pas réussir la mise à jour d'un site principal ayant un réplica de base de données activé pour les points de gestion. Désactivez la réplication de base de données avant d'installer une mise à jour pour Configuration Manager.

Pour plus d'informations, consultez Réplicas de base de données pour les points de gestion de System Center Configuration Manager.

**Définissez un basculement manuel pour les groupes de disponibilité SQL Server AlwaysOn :**
Si vous utilisez un groupe de disponibilité, vérifiez qu'il est défini sur le basculement manuel avant de commencer l'installation de la mise à jour. Une fois le site mis à jour, vous pouvez restaurer le basculement automatique. Pour plus d'informations, consultez SQL Server AlwaysOn pour une base de données de site.

**Reconfigurez les points de mise à jour logicielle qui utilisent l'équilibrage de la charge réseau (NLB) :**

Configuration Manager ne peut pas mettre à jour un site qui utilise un cluster d'équilibrage de la charge réseau

(NLB) pour héberger des points de mise à jour logicielle.

Si vous utilisez des clusters NLB pour les points de mise à jour logicielle, utilisez Windows PowerShell pour supprimer le cluster NLB. Pour plus d'informations, consultez Planifier les mises à jour logicielles dans System Center Configuration Manager.

**Désactivez toutes les tâches de maintenance de site sur chaque site pendant la durée de l'installation de la mise à jour sur ce site :**
Avant d'installer la mise à jour, désactivez toutes les tâches de maintenance de site qui peuvent s'exécuter pendant le processus de mise à jour. Cela inclut, sans toutefois s'y limiter, les tâches suivantes :

- Serveur de site de sauvegarde
- Supprimer les anciennes opérations du client
- Supprimer les données de découverte anciennes

Si une tâche de maintenance de base de données du site s'exécute pendant l'installation de la mise à jour, celle-ci peut échouer. Avant de désactiver une tâche, enregistrez sa planification pour pouvoir restaurer sa configuration une fois la mise à jour installée.

Pour plus d'informations, consultez Tâches de maintenance pour System Center Configuration Manager et Référence des tâches de maintenance pour System Center Configuration Manager.

**Arrêtez temporairement tout logiciel antivirus sur les serveurs System Center Configuration Manager :** avant de mettre à jour un site, vérifiez que vous avez arrêté tout logiciel antivirus sur les serveurs Configuration Manager.

**Créez une sauvegarde de la base de données du site d'administration centrale et des sites principaux :** avant de mettre à jour un site, sauvegardez sa base de données pour être certain de disposer d'une sauvegarde correcte utilisable en cas de récupération d'urgence.

Pour plus d'informations, consultez Sauvegarde et récupération pour System Center Configuration Manager.

**Planifiez un test du client :**
Quand vous installez une mise à jour qui affecte le client, vous pouvez la tester en mode préproduction avant de procéder au déploiement et à la mise à niveau de votre client actif.

Pour tirer parti de cette option, vous devez configurer votre site pour qu'il prenne en charge les mises à niveau automatiques pour la préproduction avant de commencer l'installation de la mise à jour.

Pour plus d'informations, consultez Mettre à niveau les clients dans System Center Configuration Manager et Comment tester les mises à niveau du client dans un regroupement de préproduction dans System Center Configuration Manager.

**Planifiez l'utilisation des fenêtres de service pour contrôler le moment auquel les serveurs de site installent les mises à jour :**
Utilisez les fenêtres de service pour définir une période au cours de laquelle les mises à jour à un serveur de site peuvent être installées.

Cela peut vous aider à contrôler le moment où les sites au sein de votre hiérarchie installent la mise à jour. Pour plus d'informations, consultez Fenêtres de maintenance pour les serveurs de site.

**Exécutez l'outil de vérification des prérequis du programme d'installation :**
Quand la mise à jour est répertoriée dans la console comme **Disponible**, vous pouvez exécuter indépendamment l'outil de vérification des prérequis avant d'installer la mise à jour. (Quand vous installez la mise à jour sur le site, l'outil de vérification des prérequis s'exécute à nouveau.)

Pour exécuter une vérification des prérequis à partir de la console, accédez à **Administration > Vue d'ensemble > Services cloud > Mises à jour et maintenance**. Ensuite, cliquez avec le bouton droit sur **Package de mise à**

**jour 1710 de Configuration Manager**, puis choisissez **Exécuter la vérification des prérequis**.

Pour plus d'informations sur le démarrage et la surveillance de la vérification des prérequis, consultez **Étape 3 : exécuter l'outil de vérification des prérequis avant d'installer une mise à jour** dans la rubrique Installer des mises à jour dans la console pour System Center Configuration Manager.

> **IMPORTANT**
> Quand l'outil de vérification des prérequis s'exécute indépendamment ou dans le cadre de l'installation d'une mise à jour, le processus met à jour certains fichiers sources du produit qui sont utilisés pour les tâches de maintenance de site. Par conséquent, après l'exécution de l'outil de vérification des prérequis, mais avant l'installation de la mise à jour, si vous devez effectuer une tâche de maintenance de site, exécutez **Setupwfe.exe** (programme d'installation de Configuration Manager) à partir du dossier CD.Latest sur le serveur de site.

**Mettez à jour les sites :**
Vous êtes maintenant prêt à commencer l'installation de la mise à jour pour votre hiérarchie. Pour plus d'informations sur l'installation de la mise à jour, consultez Installer des mises à jour dans la console.

Nous vous recommandons de planifier l'installation de la mise à jour en dehors des heures de bureau normales pour chaque site, quand le processus d'installation de la mise à jour et ses actions pour réinstaller les composants du site et les rôles de système de site auront le moins d'effet sur les opérations de votre entreprise.

Pour plus d'informations, consultez Mises à jour pour System Center Configuration Manager.

# Liste de contrôle post-mise à jour

Vérifiez et effectuez les actions suivantes après la fin de l'installation de la mise à jour.

1. Assurez-vous que la réplication de site à site est active. Dans la console, affichez **Surveillance** > **Hiérarchie de site** et **Surveillance** > **Réplication de la base de données** pour accéder à des indications concernant les problèmes ou à la confirmation que les liens de réplication sont actifs.
2. Assurez-vous que chaque serveur de site et chaque rôle de système de site est passé à la version 1710. Dans la console, vous pouvez ajouter la colonne facultative **Version** à l'affichage de certains nœuds, y compris **Sites** et **Points de distribution**.

   Lorsque c'est nécessaire, un rôle de système de site se réinstalle automatiquement pour passer à la nouvelle version. Redémarrez les systèmes de site distants qui ne se mettent pas à jour correctement.
3. Reconfigurez les réplicas de base de données des points de gestion au niveau des sites principaux que vous avez désactivés avant de commencer la mise à jour.
4. Reconfigurez les tâches de maintenance de la base de données que vous avez désactivées avant de commencer la mise à jour.
5. Si vous avez configuré le pilotage des clients avant d'installer la mise à jour, mettez à niveau les clients selon le plan que vous avez créé.

# Liste de contrôle de l'installation de la mise à jour 1706 pour System Center Configuration Manager

22/06/2018 • 25 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Quand vous utilisez Current Branch de System Center Configuration Manager, vous pouvez installer la mise à jour dans la console de la version 1706 pour mettre à jour votre hiérarchie à partir d'une version antérieure.

Pour obtenir la mise à jour de la version 1706, vous devez utiliser un rôle de système de site de point de connexion de service sur le site de niveau supérieur de votre hiérarchie. Cela peut être en mode en ligne ou hors connexion. Une fois que votre hiérarchie a téléchargé le package de mises à jour de Microsoft, celui-se trouve dans la console sous **Administration > Vue d'ensemble > Services cloud > Mises à jour et maintenance**.

- Quand la mise à jour est répertoriée comme **disponible**, elle est prête à être installée. Avant d'installer la version 1706, passez en revue les informations suivantes sur l'installation de la mise à jour 1706 et la liste de contrôle pour connaître les configurations à effectuer avant de commencer la mise à jour.
- Si la mise à jour s'affiche en tant que **Téléchargement en cours** et ne change pas, recherchez les erreurs dans les journaux **hman.log** et **dmpdownloader.log**.
    - Si dmpdownloader.log indique que le processus dmpdownloader est en veille en attendant la vérification des mises à jour, vous pouvez redémarrer le service **SMS_Executive** sur le serveur de site pour redémarrer le téléchargement des fichiers de redistribution de la mise à jour.
    - Un autre problème courant de téléchargement se produit quand les paramètres du serveur proxy empêchent les téléchargements à partir de http://silverlight.dlservice.microsoft.com et http://download.microsoft.com.

Pour plus d'informations sur l'installation des mises à jour, consultez Mises à jour et maintenance dans la console.

Pour plus d'informations sur les versions de Current Branch, consultez Versions de base et de mise à jour dans Mises à jour pour System Center Configuration Manager.

## À propos de l'installation de la mise à jour 1706

**Sites :**
Vous pouvez installer la mise à jour 1706 sur le site de niveau supérieur de votre hiérarchie. Cela signifie que vous lancez l'installation à partir de votre site d'administration centrale si en avez un, ou à partir de votre site principal autonome. Après l'installation de la mise à jour sur le site de niveau supérieur, les sites enfants ont le comportement de mise à jour suivant :

- Les sites principaux enfants installent automatiquement la mise à jour quand le site d'administration centrale a fini de l'installer. Vous pouvez utiliser des fenêtres de service pour spécifier à quel moment un site installe la mise à jour. Pour plus d'informations, consultez Fenêtres de maintenance pour les serveurs de site.
- Après que le site parent principal a installé la mise à jour, vous devez mettre à jour manuellement chacun des sites secondaires à partir de la console Configuration Manager. La mise à jour automatique des serveurs de sites secondaires n'est pas prise en charge.

**Rôles de système de site :**

Quand un serveur de site installe la mise à jour, les rôles de système de site installés sur l'ordinateur serveur de site et sur des ordinateurs distants sont automatiquement mis à jour. Avant d'installer la mise à jour, vérifiez que chaque serveur de système de site remplit les prérequis pour les opérations avec la nouvelle version de mise à jour.

**Consoles Configuration Manager :**
La première fois que vous utilisez une console Configuration Manager à l'issue de la mise à jour, vous êtes invité à mettre à jour cette console. Pour cela, vous devez exécuter le programme d'installation de Configuration Manager sur l'ordinateur hébergeant la console, puis choisir l'option de mise à jour de la console. Nous vous recommandons de ne pas retarder l'installation de la mise à jour sur la console.

> **IMPORTANT**
> Lorsque vous installez une mise à jour sur le site d'administration centrale, tenez compte des limitations suivantes et des retards qui se produisent jusqu'à ce que tous les sites principaux enfants aient également terminé l'installation de la mise à jour :
>
> - La **mise à niveau des clients** ne démarre pas. Cela comprend la mise à jour automatique des clients et des clients en préproduction. En outre, il n'est pas possible de mettre en production les clients en préproduction tant que le dernier site n'a pas terminé l'installation de la mise à jour. Après l'installation de la mise à jour sur le dernier site, la mise à niveau des clients commence, en fonction de vos options de configuration.
> - Les **nouvelles fonctionnalités** que vous activez avec la mise à jour ne sont pas disponibles. L'objectif est d'éviter l'envoi de la réplication de données associées à cette fonctionnalité à un site qui n'a pas encore installé la prise en charge de cette fonctionnalité. Après l'installation de la mise à jour sur tous les sites principaux, la fonctionnalité sera utilisable.
> - Les **liens de réplication** entre le site d'administration centrale et les sites principaux enfants apparaissent comme non mis à niveau. Cela se présente, dans l'état d'installation du pack de mise à jour, sous la forme d'un état Terminé avec un avertissement pour l'initialisation de la surveillance de la réplication. Dans le nœud Surveillance de la console, cela se présente sous l'état *Lien en cours de configuration*.

## Liste de contrôle

**Vérifiez que tous les sites exécutent une version de System Center Configuration Manager qui prend en charge la mise à jour vers 1706 :**
Chaque serveur de site de la hiérarchie doit exécuter la même version de System Center Configuration Manager pour que vous puissiez lancer l'installation de la mise à jour 1706. Pour passer à la version 1706, vous devez utiliser la version 1606, 1610 ou 1702.

**Vérifiez l'état de votre contrat Software Assurance ou des droits d'abonnement équivalents :**
Vous devez disposer d'un contrat Software Assurance (SA) actif pour installer la mise à jour 1706. Quand vous installez cette mise à jour, l'onglet **Licences** propose l'option vous permettant de confirmer la **date d'expiration de Software Assurance**.

Il s'agit d'une valeur facultative que vous pouvez spécifier pour des raisons pratiques et qui vous servira de rappel concernant la date d'expiration de votre licence. Cette date est visible lorsque vous installez des mises à jour ultérieures. Vous avez peut-être déjà spécifié cette valeur pendant la configuration ou l'installation d'une mise à jour, ou en utilisant l'onglet **Licences** de **Paramètres de hiérarchie**, sur la console de Configuration Manager.

Pour plus d'informations, consultez Licences et branches pour System Center Configuration Manager.

**Examinez les versions installées de Microsoft .NET sur les serveurs de système de site** : quand un site installe cette mise à jour, Configuration Manager installe automatiquement le .NET Framework 4.5.2 sur chaque ordinateur hébergeant un des rôles de système de site suivants (si le .NET Framework 4.5 ou ultérieur n'est pas déjà installé) :

- Point proxy d'inscription
- Point d'inscription

- Point de gestion
- Point de connexion de service

Cette installation peut mettre le serveur de système de site en état d'attente de redémarrage, et signaler des erreurs sur l'Afficheur des messages d'état du composant Configuration Manager. En outre, des applications .NET sur le serveur peuvent présenter des défaillances aléatoires jusqu'au redémarrage du serveur.

Pour plus d'informations, consultez Prérequis des sites et systèmes de site.

**Vérifiez la version du Kit de déploiement et d'évaluation (ADK) Windows pour Windows 10** : la version de Windows 10 ADK doit être 1703 ou ultérieure. (Pour plus d'informations sur les versions de Windows ADK prises en charge, consultez Windows 10 ADK.) Si vous devez mettre à jour Windows ADK, faites-le avant de commencer la mise à jour de Configuration Manager. Les images de démarrage par défaut seront ainsi mises à jour automatiquement vers la dernière version de Windows PE. (Les images de démarrage personnalisé doivent être mises à jour manuellement.)

Si vous mettez à jour le site avant de mettre à jour Windows ADK, consultez Mettre à jour les points de distribution avec l'image de démarrage pour découvrir les améliorations apportées à ce processus dans Configuration Manager version 1706.

**Examinez l'état du site et de la hiérarchie, et vérifiez l'absence de tout problème non résolu :** avant de mettre à jour un site, résolvez tous les problèmes opérationnels pour le serveur de site, le serveur de bases de données du site et les rôles de système de site installés sur des ordinateurs distants. Une mise à niveau de site peut échouer en raison de l'existence de problèmes opérationnels.

Pour plus d'informations, voir Utiliser des alertes et le système d'état pour System Center Configuration Manager.

**Examinez la réplication des fichiers et données entre sites :**
vérifiez que la réplication des fichiers et bases de données entre les sites est opérationnelle et active. Des retards ou backlogs dans ces domaines peuvent perturber ou empêcher la mise à jour. Pour la réplication de la base de données, vous pouvez utiliser l'Analyseur de lien de réplication pour faciliter la résolution des problèmes avant de commencer la mise à jour.

Pour plus d'informations, consultez À propos de l'analyseur de lien de réplication dans la rubrique Surveiller l'infrastructure de la hiérarchie et de la réplication dans System Center Configuration Manager.

**Installez toutes les mises à jour critiques applicables pour les systèmes d'exploitation sur les ordinateurs hébergeant le site, le serveur de base de données du site et les rôles de système de site distants :** avant d'installer une mise à jour pour Configuration Manager, installez toutes les mises à jour critiques pour chaque système de site concerné. Si vous installez une mise à jour qui nécessite un redémarrage, redémarrez les ordinateurs concernés avant d'entreprendre la mise à jour.

**Désactivez les réplicas de base de données pour les points de gestion au niveau des sites principaux :**
Configuration Manager ne peut pas réussir la mise à jour d'un site principal ayant un réplica de base de données activé pour les points de gestion. Désactivez la réplication de base de données avant d'installer une mise à jour pour Configuration Manager.

Pour plus d'informations, consultez Réplicas de base de données pour les points de gestion de System Center Configuration Manager.

**Définissez un basculement manuel pour les groupes de disponibilité SQL Server AlwaysOn :**
Si vous utilisez un groupe de disponibilité, vérifiez qu'il est défini sur le basculement manuel avant de commencer l'installation de la mise à jour. Une fois le site mis à jour, vous pouvez restaurer le basculement automatique. Pour plus d'informations, consultez SQL Server AlwaysOn pour une base de données de site.

**Reconfigurez les points de mise à jour logicielle qui utilisent l'équilibrage de la charge réseau (NLB) :**
Configuration Manager ne peut pas mettre à jour un site qui utilise un cluster d'équilibrage de la charge réseau

(NLB) pour héberger des points de mise à jour logicielle.

Si vous utilisez des clusters NLB pour les points de mise à jour logicielle, utilisez Windows PowerShell pour supprimer le cluster NLB. Pour plus d'informations, consultez Planifier les mises à jour logicielles dans System Center Configuration Manager.

**Désactivez toutes les tâches de maintenance de site sur chaque site pendant la durée de l'installation de la mise à jour sur ce site :**
Avant d'installer la mise à jour, désactivez toutes les tâches de maintenance de site qui peuvent s'exécuter pendant le processus de mise à jour. Cela inclut, sans toutefois s'y limiter, les tâches suivantes :

- Serveur de site de sauvegarde
- Supprimer les anciennes opérations du client
- Supprimer les données de découverte anciennes

Si une tâche de maintenance de base de données du site s'exécute pendant l'installation de la mise à jour, celle-ci peut échouer. Avant de désactiver une tâche, enregistrez sa planification pour pouvoir restaurer sa configuration une fois la mise à jour installée.

Pour plus d'informations, consultez Tâches de maintenance pour System Center Configuration Manager et Référence des tâches de maintenance pour System Center Configuration Manager.

**Arrêtez temporairement tout logiciel antivirus sur les serveurs System Center Configuration Manager :** avant de mettre à jour un site, vérifiez que vous avez arrêté tout logiciel antivirus sur les serveurs Configuration Manager.

**Créez une sauvegarde de la base de données du site d'administration centrale et des sites principaux :** avant de mettre à jour un site, sauvegardez sa base de données pour être certain de disposer d'une sauvegarde correcte utilisable en cas de récupération d'urgence.

Pour plus d'informations, consultez Sauvegarde et récupération pour System Center Configuration Manager.

**Planifiez un test du client :**
Quand vous installez une mise à jour qui affecte le client, vous pouvez la tester en mode préproduction avant de procéder au déploiement et à la mise à niveau de votre client actif.

Pour tirer parti de cette option, vous devez configurer votre site pour qu'il prenne en charge les mises à niveau automatiques pour la préproduction avant de commencer l'installation de la mise à jour.

Pour plus d'informations, consultez Mettre à niveau les clients dans System Center Configuration Manager et Comment tester les mises à niveau du client dans un regroupement de préproduction dans System Center Configuration Manager.

**Planifiez l'utilisation des fenêtres de service pour contrôler le moment auquel les serveurs de site installent les mises à jour :**
Utilisez les fenêtres de service pour définir une période au cours de laquelle les mises à jour à un serveur de site peuvent être installées.

Cela peut vous aider à contrôler le moment où les sites au sein de votre hiérarchie installent la mise à jour. Pour plus d'informations, consultez Fenêtres de maintenance pour les serveurs de site.

**Exécutez l'outil de vérification des prérequis du programme d'installation :**
Quand la mise à jour est répertoriée dans la console comme **Disponible**, vous pouvez exécuter indépendamment l'outil de vérification des prérequis avant d'installer la mise à jour. (Quand vous installez la mise à jour sur le site, l'outil de vérification des prérequis s'exécute à nouveau.)

Pour exécuter une vérification des prérequis à partir de la console, accédez à **Administration > Vue d'ensemble > Services cloud > Mises à jour et maintenance**. Ensuite, cliquez avec le bouton droit sur **Package de mise à**

**jour 1706 de Configuration Manager**, puis choisissez **Exécuter la vérification des prérequis**.

Pour plus d'informations sur le démarrage et la surveillance de la vérification des prérequis, consultez **Étape 3 : exécuter l'outil de vérification des prérequis avant d'installer une mise à jour** dans la rubrique Installer des mises à jour dans la console pour System Center Configuration Manager.

> **IMPORTANT**
> Quand l'outil de vérification des prérequis s'exécute indépendamment ou dans le cadre de l'installation d'une mise à jour, le processus met à jour certains fichiers sources du produit qui sont utilisés pour les tâches de maintenance de site. Par conséquent, après l'exécution de l'outil de vérification des prérequis, mais avant l'installation de la mise à jour, si vous devez effectuer une tâche de maintenance de site, exécutez **Setupwfe.exe** (programme d'installation de Configuration Manager) à partir du dossier CD.Latest sur le serveur de site.

**Mettez à jour les sites :**
Vous êtes maintenant prêt à commencer l'installation de la mise à jour pour votre hiérarchie. Pour plus d'informations sur l'installation de la mise à jour, consultez Installer des mises à jour dans la console.

Nous vous recommandons de planifier l'installation de la mise à jour en dehors des heures de bureau normales pour chaque site, quand le processus d'installation de la mise à jour et ses actions pour réinstaller les composants du site et les rôles de système de site auront le moins d'effet sur les opérations de votre entreprise.

Pour plus d'informations, consultez Mises à jour pour System Center Configuration Manager.

## Liste de contrôle post-mise à jour

Vérifiez et effectuez les actions suivantes après la fin de l'installation de la mise à jour.

1. Assurez-vous que la réplication de site à site est active. Dans la console, affichez **Surveillance** > **Hiérarchie de site** et **Surveillance** > **Réplication de la base de données** pour accéder à des indications concernant les problèmes ou à la confirmation que les liens de réplication sont actifs.
2. Assurez-vous que chaque serveur de site et chaque rôle de système de site est passé à la version 1706. Dans la console, vous pouvez ajouter la colonne facultative **Version** à l'affichage de certains nœuds, y compris **Sites** et **Points de distribution**.

   Lorsque c'est nécessaire, un rôle de système de site se réinstalle automatiquement pour passer à la nouvelle version. Redémarrez les systèmes de site distants qui ne se mettent pas à jour correctement.
3. Reconfigurez les réplicas de base de données des points de gestion au niveau des sites principaux que vous avez désactivés avant de commencer la mise à jour.
4. Reconfigurez les tâches de maintenance de la base de données que vous avez désactivées avant de commencer la mise à jour.
5. Si vous avez configuré le pilotage des clients avant d'installer la mise à jour, mettez à niveau les clients selon le plan que vous avez créé.

## Problèmes connus

Une fois effectuée la mise à jour vers la version 1706, chaque fois que SMS_Executive démarre, le message d'état avertissement suivant est créé par SMS_CERTIFICATE_MANAGER :

- Microsoft SQL Server a signalé le message SQL 515, gravité 16 : [23000][515][Microsoft][SQL Server Native Client 11.0][SQL Server] Impossible d'insérer la valeur NULL dans la colonne 'RowVersion', table 'CM_GF1.dbo.AAD_SecretChange_Notify'. Cette colonne n'accepte pas les valeurs NULL. Échec de INSERT.

Ce message peut être ignoré. Il se produit quand aucun service cloud n'a été configuré pour être utilisé avant la mise à jour vers la version 1706. Ce problème sera résolu dans une version à venir.

# Prise en charge des versions Current Branch de System Center Configuration Manager

22/06/2018 • 4 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Microsoft prévoit de publier des mises à jour de System Center Configuration Manager Current Branch plusieurs fois par an. Pour les versions de Configuration Manager publiées avant la version 1710, la prise en charge dure 12 mois. À compter de la version 1710, chaque version de mise à jour reste prise en charge pendant 18 mois suivant sa date de disponibilité générale (GA). Un support technique est assuré pendant toute la période de prise en charge. Toutefois, notre structure de prise en charge est dynamique et évolue en deux phases de maintenance distinctes qui dépendent de la disponibilité de la dernière version Current Branch.

- Phase de maintenance Mises à jour de sécurité et mises à jour critiques : quand vous exécutez la dernière version Current Branch de Configuration Manager, vous recevez des mises à jour de sécurité et des mises à jour critiques.
- Phase de maintenance Mises à jour de sécurité (uniquement) : après la publication d'une nouvelle version Current Branch, la prise en charge des branches antérieures est réduite aux mises à jour de sécurité uniquement pendant le reste du cycle de vie de prise en charge de cette version (illustré à la figure 1).

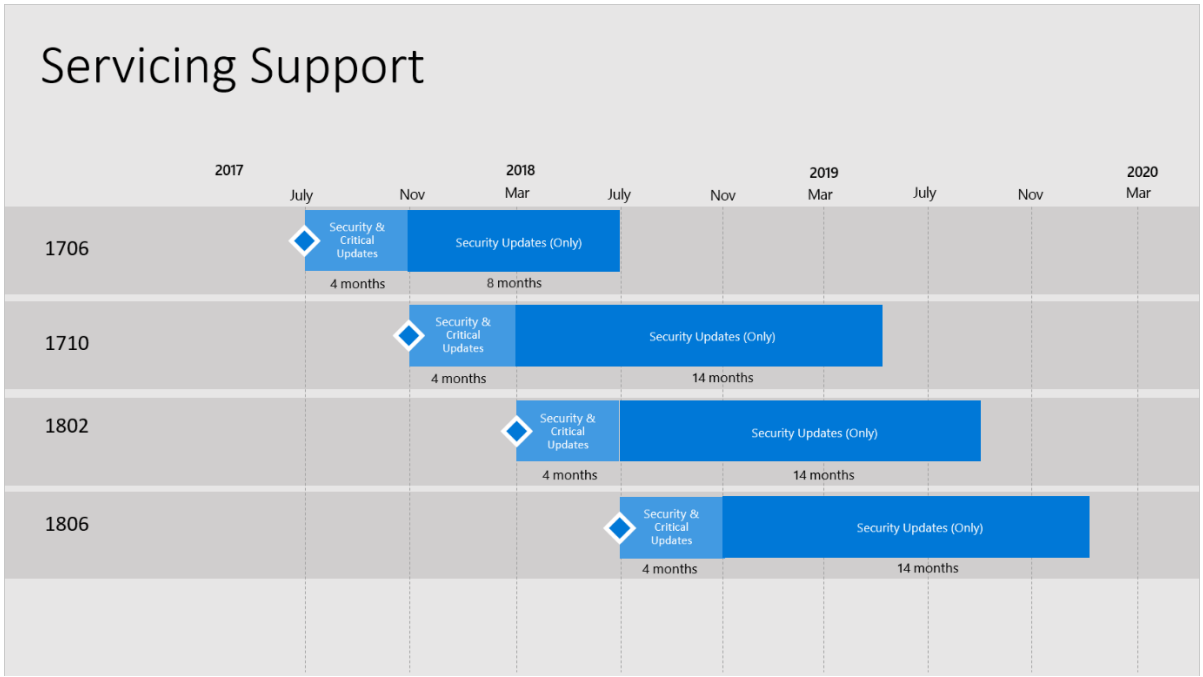



Figure 1. Exemple de la superposition du cycle de publication pour la prise en charge de maintenance de Current Branch. Cet exemple sert à illustrer le cycle et ne représente pas les dates de publication réelles ou attendues.

**NOTE**

La dernière version Current Branch est toujours en phase de maintenance Mises à jour de sécurité et mises à jour critiques. Cette déclaration de support signifie que si vous rencontrez une erreur de code qui nécessite une mise à jour critique, vous devez avoir la dernière version Current Branch afin de recevoir un correctif. Toutes les autres versions Current Branch prises en charge sont autorisées à recevoir uniquement les mises à jour de sécurité.

- Pour les versions 1710 et ultérieures, toute prise en charge se termine après l'expiration du cycle de vie de 18 mois des versions Current Branch.
- Pour les versions antérieures à la version 1710, toute prise en charge se termine après l'expiration du cycle de vie de 12 mois.

Nous vous recommandons de mettre à jour votre déploiement de Configuration Manager vers la dernière version avant que la prise en charge de votre version actuelle n'expire.

### Historique des versions

| VERSION | DATE DE DISPONIBILITÉ | DATE DE FIN DE PRISE EN CHARGE |
|---|---|---|
| 1802 | 22 mars 2018 | 22 septembre 2019 |
| 1710 | 20 novembre 2017 | Mai 20, 2019 |
| 1706 | 31 juillet 2017 | 31 juillet 2018 |
| 1702 | 27 Mars 2017 | 27 mars 2018 |
| 1610 | 18 novembre 2016 | 18 novembre 2017 |
| 1606 | 22 juillet 2016 | 22 juillet 2017 |
| 1602 | 11 Mars 2016 | 11 Mars 2017 |
| 1511 | 8 décembre 2015 | 8 décembre 2016 |

Pour plus d'informations sur les numéros de version et la disponibilité sous forme de mise à jour dans la console ou d'une ligne de base, consultez Versions de base et de mise à jour.

# Utiliser des alertes et le système d'état pour System Center Configuration Manager

22/06/2018 • 32 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Configurez des alertes et utilisez le système d'état intégré pour rester informé de l'état de votre déploiement de System Center Configuration Manager.

## Système d'état

Tous les composants de site principaux génèrent des messages d'état qui fournissent des commentaires sur les opérations de site et de hiérarchie. Cette information peut vous tenir informé de l'intégrité des différents processus de site. Vous pouvez régler le système d'alerte pour ignorer le bruit concernant les problèmes connus tout en permettant une visibilité anticipée d'autres problèmes susceptibles de nécessiter votre attention.

Par défaut, le système d'état de Configuration Manager fonctionne sans configuration en utilisant les paramètres qui conviennent à la plupart des environnements. Toutefois, vous pouvez configurer les éléments suivants :

- **Outils de synthèse d'état :** vous pouvez modifier les outils de synthèse d'état sur chaque site pour contrôler la fréquence des messages d'état qui génèrent un changement d'indicateur d'état pour les quatre outils de synthèse suivants :
  - Outil de synthèse du déploiement d'application
  - Outil de synthèse des statistiques d'application
  - Outil de synthèse d'état des composants
  - Outil de synthèse d'état du système de site
- **Règles de filtre d'état :** vous pouvez créer des règles de filtre d'état, modifier la priorité des règles, activer ou désactiver des règles, ainsi que supprimer des règles non utilisées sur chaque site.

  > **NOTE**
  > Les règles de filtre d'état ne prennent pas en charge l'utilisation de variables d'environnement pour exécuter des commandes externes.

- **Rapport d'état :** vous pouvez configurer le rapport des composants client et serveur pour modifier la façon dont les messages d'état sont signalées dans un rapport au système d'état de Configuration Manager et spécifier où les messages d'état sont envoyés.

  > **WARNING**
  > Étant donné que les paramètres de rapport par défaut conviennent à la plupart des environnements, ils doivent être modifiés avec précaution. Lorsque vous augmentez le niveau du rapport d'état en choisissant de rapporter tous les détails d'état, vous pouvez augmenter la quantité de messages d'état à traiter, ce qui accroît la charge de traitement sur le site Configuration Manager. À l'inverse, une diminution du niveau du rapport d'état peut limiter l'utilité des outils de synthèse d'état.

Étant donné que le système d'état tient à jour des configurations distinctes pour chaque site, vous devez modifier chaque site individuellement.

### Procédures de configuration du système d'état

#### Pour configurer des outils de synthèse d'état

1. Dans la console Configuration Manager, accédez à **Administration** > **Configuration du site** >**Sites**, puis sélectionnez le site dont vous voulez configurer le système d'état.
2. Dans l'onglet **Accueil** , dans le groupe **Paramètres** , cliquez sur **Outils de synthèse d'état**.
3. Dans la boîte de dialogue **Outils de synthèse d'état** , sélectionnez l'outil de synthèse d'état que vous souhaitez configurer, puis cliquez sur **Modifier** pour ouvrir les propriétés de cet outil de synthèse. Si vous modifiez l'outil de synthèse du déploiement d'application ou des statistiques d'application, passez à l'étape 5. Si vous modifiez l'outil de synthèse d'état des composants, passez à l'étape 6. Si vous modifiez l'outil de synthèse d'état du système de site, passez à l'étape 7.
4. Utilisez les étapes suivantes après avoir ouvert la page de propriétés de l'outil de synthèse du déploiement d'application ou l'outil de synthèse des statistiques d'application :
   a. Dans l'onglet **Général** de la page de propriétés des outils de synthèse, configurez les intervalles de synthèse, puis cliquez sur **OK** pour fermer la page de propriétés.
   b. Cliquez sur **OK** pour fermer la boîte de dialogue **Outils de synthèse d'état** et terminez cette procédure.
5. Utilisez les étapes suivantes après avoir ouvert la page de propriétés de l'outil de synthèse d'état des composants :
   a. Dans l'onglet **Général** de la page de propriétés des outils de synthèse, configurez les valeurs de réplication et de période seuil.
   b. Dans l'onglet **Seuils** , sélectionnez le **Type de Message** que vous souhaitez configurer, puis cliquez sur le nom d'un composant dans la liste **Seuils** .
   c. Dans la boîte de dialogue **Propriétés du seuil de l'état** , modifiez les valeurs de seuil d'avertissement et critique, puis cliquez sur **OK**.
   d. Répétez les étapes 6.b et 6.c au besoin et, lorsque vous avez terminé, cliquez sur **OK** pour fermer les propriétés de l'outil de synthèse.
   e. Cliquez sur **OK** pour fermer la boîte de dialogue **Outils de synthèse d'état** et terminez cette procédure.
6. Utilisez les étapes suivantes après avoir ouvert les pages des propriétés de l'outil de synthèse d'état du système de site :
   a. Dans l'onglet **Général** de la page de propriétés des outils de synthèse, configurez les valeurs de réplication et de planification.
   b. Dans l'onglet **Seuils** , spécifiez des valeurs pour les **Seuils par défaut** afin de configurer des seuils par défaut pour les affichages d'état critique et d'avertissement.
   c. Pour modifier les valeurs des **Objets de stockage**spécifiques, cliquez sur l'objet dans la liste **Seuils spécifiques** et cliquez sur le bouton **Propriétés** pour pouvoir accéder et modifier les seuils critique et d'avertissement des objets de stockage. Cliquez sur **OK** pour fermer les propriétés des objets de stockage.
   d. Pour créer un nouvel objet de stockage, cliquez sur le bouton **Créer un objet** et spécifiez les valeurs des objets de stockage. Cliquez sur **OK** pour fermer les propriétés de l'objet.

e. Pour supprimer un objet de stockage, sélectionnez l'objet, puis cliquez sur le bouton **Supprimer** .

f. Répétez les étapes 7.b à 7.e si besoin. Lorsque vous avez terminé, cliquez sur **OK** pour fermer les propriétés de l'outil de synthèse.

g. Cliquez sur **OK** pour fermer la boîte de dialogue **Outils de synthèse d'état** et terminez cette procédure.

#### Pour créer une règle de filtre d'état

1. Dans la console Configuration Manager, accédez à **Administration** > **Configuration du site** >**Sites**, puis sélectionnez le site pour lequel vous voulez configurer le système d'état.
2. Dans l'onglet **Accueil** , dans le groupe **Paramètres** , cliquez sur **Règles de filtre d'état**. La boîte de dialogue **Règles de filtre d'état** s'ouvre.
3. Cliquez sur **Créer**.
4. Sur la page **Général**de l' **Assistant Création de règle de filtre d'état** , spécifiez un nom pour la nouvelle règle de filtre d'état et un critère de correspondance des messages pour la règle, puis cliquez sur **Suivant**.
5. Sur la page **Actions** , spécifiez les actions à entreprendre lorsqu'un message d'état correspond à la règle de filtre, puis cliquez sur **Suivant**.
6. Sur la page **Résumé** , consultez les détails de la nouvelle règle, puis terminez l'Assistant.

> **NOTE**
> Configuration Manager exige uniquement que la nouvelle règle de filtre d'état ait un nom. Si la règle est créée, mais que vous ne spécifiez pas de critère pour traiter les messages d'état, la règle de filtre d'état n'aura aucun effet. Cela vous permet de créer et d'organiser des règles avant de configurer les critères de filtre d'état pour chaque règle.

#### Pour modifier ou supprimer une règle de filtre d'état

1. Dans la console Configuration Manager, accédez à **Administration** > **Configuration du site** >**Sites**, puis sélectionnez le site pour lequel vous voulez configurer le système d'état.
2. Dans l'onglet **Accueil** , dans le groupe **Paramètres** , cliquez sur **Règles de filtre d'état**.
3. Dans la boîte de dialogue **Règles de filtre d'état** , sélectionnez la règle que vous souhaitez modifier puis effectuez l'une des actions suivantes :
   - Cliquez sur **Augmenter la priorité** ou **Diminuer la priorité** pour modifier l'ordre de traitement de la règle de filtre d'état. Puis sélectionnez une autre action ou passez à l'étape 8 de cette procédure pour terminer cette tâche.
   - Cliquez sur **Désactiver** ou **Activer** pour modifier l'état de la règle. Après avoir modifié l'état de la règle, sélectionnez une autre action ou passez à l'étape 8 de cette procédure pour terminer cette tâche.
   - Cliquez sur **Supprimer** si vous souhaitez supprimer la règle de filtre d'état de ce site, puis cliquez sur **Oui** pour confirmer l'action. Après avoir supprimé une règle, sélectionnez une autre action ou passez à l'étape 8 de cette procédure pour terminer cette tâche.
   - Cliquez sur **Modifier** si vous souhaitez modifier les critères de la règle de message d'état et passez à l'étape 5 de cette procédure.
4. Sur l'onglet **Général** de la boîte de dialogue Propriétés de la règle de filtre d'état, modifiez la règle et les critères de correspondance des messages.
5. Cliquez sur l'onglet **Actions** , modifiez les actions à entreprendre lorsqu'un message d'état correspond à

la règle de filtre.

6. Cliquez sur **OK** pour enregistrer les modifications.
7. Cliquez sur **OK** pour fermer la boîte de dialogue **Règles de filtre d'état** .

#### Pour configurer un rapport d'état

1. Dans la console Configuration Manager, accédez à **Administration** > **Configuration du site** > **Sites**, puis sélectionnez le site pour lequel vous voulez configurer le système d'état.
2. Dans l'onglet **Accueil** , dans le groupe **Paramètres** , cliquez sur **Configurer les composants de site**, puis sélectionnez **Rapport d'état**.
3. Dans la boîte de dialogue **Propriétés du composant de rapport d'état** , spécifiez les messages d'état de composant serveur et client que vous souhaitez signaler ou journaliser :
   a. Configurez **Rapport** pour envoyer des messages d'état au système de messages d'état de Configuration Manager.
   b. Configurez **Journal** pour écrire le type et la gravité des messages d'état dans le journal des événements Windows.
4. Cliquez sur **OK**.

### Surveiller l'état du système de Configuration Manager

L'**état du système** dans Configuration Manager fournit une vue d'ensemble des opérations générales de sites et des opérations de serveur de site de votre hiérarchie. Il peut révéler des problèmes de fonctionnement des serveurs de système de site ou des composants, et vous pouvez utiliser l'état du système pour consulter des détails spécifiques pour différentes opérations de Configuration Manager. Vous surveillez l'état du système à partir du nœud **État du système** de l'espace de travail **Surveillance** dans la console Configuration Manager.

La plupart des composants et rôles de système de site Configuration Manager génèrent des messages d'état. Les détails des messages d'état sont consignés dans chaque journal opérationnel des composants, mais ils sont également soumis à la base de données de site lorsqu'ils sont résumés et présentés dans un cumul général de l'intégrité de chaque composant ou des systèmes de site. Ces cumuls de messages d'état fournissent des informations détaillées pour les opérations et avertissements réguliers ainsi que pour les détails de l'erreur. Vous pouvez configurer les seuils auxquels les avertissements ou les erreurs sont déclenchés et ajuster le système afin de vous assurer que les informations relatives au cumul ignorent les problèmes connus qui ne vous concernent pas tout en attirant votre attention sur les problèmes réels des serveurs ou sur les opérations liées aux composants que vous souhaitez peut-être examiner.

L'état du système est répliqué vers d'autres sites dans une hiérarchie en tant que données de site, pas en tant que données globales. Cela signifie que vous ne pouvez voir que l'état du site auquel votre console Configuration Manager se connecte, et les sites enfants de ce site. Ainsi, envisagez de connecter votre console Configuration Manager sur le site de niveau supérieur de votre hiérarchie lorsque vous affichez l'état du système.

Utilisez le tableau suivant pour identifier les différents affichages de l'état du système et les situations dans lesquelles les utiliser.

| NŒUD | PLUS D'INFORMATIONS |
| --- | --- |

| NŒUD | PLUS D'INFORMATIONS |
| --- | --- |
| État du site | Ce nœud permet d'afficher une synthèse de l'état de chaque système de site pour consulter l'intégrité de chaque serveur de système de site. L'intégrité d'un système de site est déterminée par des seuils que vous configurez pour chaque site dans l' **Outil de synthèse d'état du système de site**.<br><br>Vous pouvez afficher les messages d'état de chaque système de site, définir des seuils pour les messages d'état et gérer le fonctionnement des composants sur des systèmes de site à l'aide du **Gestionnaire de service de Configuration Manager**. |
| État du composant | Utilisez ce nœud pour afficher une synthèse de l'état de chaque composant de Configuration Manager pour vérifier son bon fonctionnement. L'intégrité d'un composant est déterminée par les seuils que vous configurez pour chaque site dans l' **Outil de synthèse d'état des composants**.<br><br>Vous pouvez afficher les messages d'état pour chaque composant, définir des seuils pour les messages d'état et gérer le fonctionnement des composants à l'aide du **Gestionnaire de service de Configuration Manager**. |
| Enregistrements en conflit | Utilisez ce nœud pour afficher les messages d'état de clients qui peuvent présenter des conflits de rapports.<br><br>Configuration Manager utilise l'ID du matériel pour tenter d'identifier les éventuels clients dupliqués et vous signale les enregistrements en conflit. Par exemple, si vous devez réinstaller un ordinateur, il est possible que l'ID du matériel soit le même, mais que le GUID utilisé par Configuration Manager soit différent. |
| Requêtes sur les messages d'état | Utilisez ce nœud pour demander des messages d'état d'événements spécifiques ou des informations liées. Vous pouvez utiliser les requêtes de messages d'état pour trouver des messages d'état liés à des événements spécifiques.<br><br>Il est possible d'utiliser fréquemment des requêtes de messages d'état pour identifier quand un composant, une opération ou un objet Configuration Manager spécifique a été modifié ainsi que le compte utilisé pour effectuer cette modification. Par exemple, vous pouvez exécuter la requête intégrée pour les **Regroupements créés, modifiés ou supprimés** afin d'identifier quand un regroupement a été créé et le compte utilisateur utilisé pour créer ce regroupement. |

#### Gérer l'état du site et l'état des composants

Utilisez les informations suivantes pour gérer l'état du site et l'état du composant :

- Pour configurer des seuils pour le système d'état, voir Procédures de configuration du système d'état.
- Pour gérer les composants individuels dans Configuration Manager, utilisez le **Gestionnaire de service de Configuration Manager**.

#### Afficher les messages d'état

Vous pouvez afficher les messages d'état des serveurs de système de site et des composants individuels.

Pour consulter des messages d'état dans la console Configuration Manager, sélectionnez un serveur de système

de site ou un composant spécifique, puis cliquez sur **Afficher les messages**. Lorsque vous consultez des messages, vous pouvez choisir d'afficher des types de message spécifiques ou des messages d'une période indiquée. Vous pouvez également filtrer les résultats en fonction des détails du message d'état.

# Alertes

Les alertes Configuration Manager sont générées par certaines opérations quand une condition spécifique se produit.

- Les alertes sont habituellement générées quand une erreur que vous devez résoudre se produit
- Les alertes peuvent être générées pour vous avertir qu'une condition a été détectée afin que vous puissiez continuer à surveiller la situation.
- Certaines alertes que vous configurez, telles que les alertes concernant l'état de Endpoint Protection et du client, tandis que les autres alertes sont configurées automatiquement
- Vous pouvez configurer des abonnements aux alertes qui peuvent ensuite envoyer des détails par courrier électronique, ce qui permet une plus grande sensibilisation aux problèmes clés

  Utilisez le tableau suivant pour rechercher des informations sur la façon de configurer des alertes et des abonnements aux alertes dans Configuration Manager :

| ACTION | INFORMATIONS COMPLÉMENTAIRES |
|---|---|
| Configurer des alertes Endpoint Protection pour un regroupement | Voir **Comment configurer des alertes pour Endpoint Protection dans Configuration Manager** dans Configuration de Endpoint Protection dans System Center Configuration Manager. |
| Configurer des alertes d'état du client pour un regroupement | Voir Guide pratique pour configurer l'état du client dans System Center Configuration Manager. |
| Gérer les alertes Configuration Manager | Consultez la section Management tasks for alerts de cette rubrique. |
| Configurer les abonnements par courrier électronique aux alertes | Consultez la section Management tasks for alerts de cette rubrique. |
| Surveiller les alertes | Consultez la section Surveiller les alertes |

### Management tasks for alerts

**Pour gérer les alertes générales**

1. Dans la console Configuration Manager, accédez à **Surveillance** > **Alertes**, puis sélectionnez une tâche de gestion.

   Utilisez le tableau suivant pour obtenir plus d'informations sur les tâches de gestion qui pourraient nécessiter certaines informations avant de les sélectionner.

| TÂCHE DE GESTION | DÉTAILS |
|---|---|
| **Configurer** | Ouvre la boîte de dialogue *Propriétés de* **<nom de l'alerte>** où vous pouvez modifier le nom, la gravité et les seuils de l'alerte sélectionnée. Si vous modifiez la gravité de l'alerte, cette configuration affecte la façon dont les alertes sont affichées dans la console Configuration Manager. |

| TÂCHE DE GESTION | DÉTAILS |
| --- | --- |
| **Modifier les commentaires** | Entrez un commentaire pour les alertes sélectionnées. Ces commentaires s'affichent avec l'alerte dans la console Configuration Manager. |
| **Reporter** | Suspend la surveillance de l'alerte jusqu'à la date spécifiée. À ce moment-là, l'état de l'alerte est mis à jour.<br><br>Vous pouvez reporter une alerte uniquement quand celle-ci est active. |
| **Créer un abonnement** | Ouvre la boîte de dialogue **Nouvel abonnement** où vous pouvez créer un abonnement par courrier électronique à l'alerte sélectionnée. |

#### Pour configurer des alertes d'état du client pour un regroupement

1. Dans la console Configuration Manager, cliquez sur **Ressources et Conformité** > **Regroupements d'appareils**.
2. Dans la liste **Regroupements de périphériques** , sélectionnez le regroupement pour lequel vous souhaitez configurer des alertes, puis cliquez sur **Propriétés** dans l'onglet **Accueil** , du groupe **Propriétés**.

   > **NOTE**
   > Vous ne pouvez pas configurer d'alertes pour les regroupements d'utilisateurs.

3. Sous l'onglet **Alertes** de la boîte de dialogue **Propriétés de** <*Nom du regroupement*>, cliquez sur **Ajouter**.

   > **NOTE**
   > L'onglet **Alertes** n'est visible que si le rôle de sécurité auquel vous êtes associé dispose d'autorisations pour les alertes.

4. Dans la boîte de dialogue **Ajouter de nouvelles alertes de regroupement** , choisissez les alertes que vous souhaitez générer lorsque les seuils d'état du client passent sous une valeur spécifique, puis cliquez sur **OK**.
5. Dans la liste **Conditions** de l'onglet **Alertes** , sélectionnez chaque alerte relative à l'état du client, puis spécifiez les informations suivantes.
   - **Nom d'alerte** – Acceptez le nom par défaut ou entrez un nouveau nom pour l'alerte.
   - **Gravité d'alerte** – Dans la liste déroulante, choisissez la gravité d'alerte qui sera affichée dans la console Configuration Manager.
   - **Déclencher l'alerte** : spécifiez le pourcentage seuil pour l'alerte.
6. Cliquez sur **OK** pour fermer la boîte de dialogue **Propriétés de** <*Nom du regroupement*>.

#### Pour configurer une notification par courrier électronique pour les alertes

1. Dans la console Configuration Manager, accédez à **Analyse** > **Alertes** > **Inscriptions**.
2. Sous l'onglet **Accueil** , du groupe **Créer** , cliquez sur **Configurer la notification par courrier électronique**.

3. Dans la boîte de dialogue **Propriétés du composant de notification de courrier électronique** , définissez ce qui suit :

   - **Activer les notifications par courrier électronique pour les alertes** : cochez cette case pour permettre à Configuration Manager d'utiliser un serveur SMTP pour envoyer des alertes par e-mail.
   - **Nom de domaine complet ou adresse IP du serveur SMTP pour envoyer des alertes par courrier électronique**: entrez le nom de domaine complet (FQDN) ou l'adresse IP et le port SMTP du serveur de messagerie à utiliser pour ces alertes.
   - **Compte de connexion au serveur SMTP** : spécifiez la méthode d'authentification que Configuration Manager doit utiliser pour se connecter au serveur de messagerie.
   - **Adresse de l'expéditeur pour les alertes de courrier électronique**: spécifiez l'adresse électronique à partir de laquelle les courriers électroniques d'alerte sont envoyés.
   - **Tester le serveur SMTP**: envoie un courrier électronique de test à l'adresse électronique spécifiée dans **Adresse de l'expéditeur pour les alertes de courrier électronique**.

4. Cliquez sur **OK** pour enregistrer les paramètres et fermer la boîte de dialogue des **Propriétés du composant de notification de courrier électronique** .

Pour vous abonner aux alertes par courrier électronique

1. Dans la console Configuration Manager, accédez à **Analyse** > **Alertes** .
2. Sélectionnez une alerte, puis sous l'onglet **Accueil** , dans le groupe **Abonnement** , cliquez sur **Créer un abonnement**.
3. Dans la boîte de dialogue **Nouvel abonnement** , spécifiez les éléments suivants :

   - **Nom**: entrez le nom permettant d'identifier l'abonnement par courrier électronique. Vous pouvez entrer jusqu'à 255 caractères.
   - **Adresse de messagerie**: entrez les adresses de messagerie de destination de l'alerte. Vous pouvez séparer plusieurs adresses de messagerie par un point-virgule.
   - **Langue de messagerie**: dans la liste, spécifiez la langue du courrier électronique.

4. Cliquez sur **OK** pour fermer la boîte de dialogue **Nouvel abonnement** et créer l'abonnement par courrier électronique.

> **NOTE**
> Vous pouvez supprimer et modifier les abonnements dans l'espace de travail **Surveillance** lorsque vous développez le nœud **Alertes** , puis cliquez sur le nœud **Abonnements** .

### Surveiller les alertes

Vous pouvez consulter les alertes dans le nœud **Alertes** de l'espace de travail **Surveillance** . Les alertes présentent l'un des états d'alerte suivants :

- **Jamais déclenché**: la condition de l'alerte n'a pas été remplie.
- **Actif**: la condition de l'alerte est remplie.
- **Annulé**: la condition d'une alerte active n'est plus remplie. Cet état indique que la condition qui a entraîné l'alerte est maintenant résolue.
- **Reporté à plus tard** : un utilisateur administratif a configuré Configuration Manager pour évaluer l'état

de l’alerte ultérieurement.

- **Désactivé**: l’alerte a été désactivée par un utilisateur administratif. Lorsqu'une alerte présente cet état, Configuration Manager ne la met pas à jour même si l'état de l'alerte change.

  Vous pouvez effectuer l'une des actions suivantes lorsque Configuration Manager génère une alerte :

- Corrigez la condition qui a généré l'alerte, par exemple, corrigez un problème réseau ou un problème de configuration qui a généré l'alerte. Une fois que Configuration Manager a détecté que le problème n'existe plus, l'état de l'alerte passe à **Annuler**.
- Si l'alerte est un problème connu, vous pouvez reporter l'alerte pendant une durée spécifique. À ce moment, Configuration Manager met à jour l'alerte à son état actuel.

  Vous pouvez reporter une alerte uniquement lorsque celle-ci est active.

- Vous pouvez modifier le **Commentaire** d'une alerte afin d'informer les autres utilisateurs administratifs que cette alerte est surveillée. Par exemple, dans le commentaire, vous pouvez identifier comment résoudre la condition, fournir des informations sur l'état actuel de la condition ou expliquer la raison du report de l'alerte.

# Attestation d'intégrité pour System Center Configuration Manager

22/06/2018 • 8 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les administrateurs peuvent consulter l'état de l'attestation d'intégrité des appareils Windows 10 dans la console Configuration Manager. L'attestation de l'intégrité des appareils permet à l'administrateur de s'assurer que les configurations dignes de confiance suivantes de BIOS, de module de plateforme sécurisée (TPM) et de logiciel de démarrage sont activées sur les ordinateurs clients :

- Logiciel anti-programme malveillant à lancement anticipé - Un logiciel anti-programme malveillant à lancement anticipé (ELAM) protège votre ordinateur au démarrage et avant l'initialisation de pilotes tiers. Comment activer le logiciel anti-programme malveillant à lancement anticipé (ELAM)
- BitLocker - Le chiffrement de lecteur BitLocker Windows est un logiciel qui vous permet de chiffrer toutes les données stockées sur le volume hébergeant le système d'exploitation Windows. Comment activer BitLocker
- Démarrage sécurisé - Le démarrage sécurisé est une norme de sécurité développée par des membres du secteur de la fabrication de PC pour s'assurer que votre ordinateur démarre en utilisant uniquement des logiciels approuvés par le fabricant de l'ordinateur. En savoir plus sur le démarrage sécurisé
- Intégrité du code - L'intégrité du code est une fonctionnalité qui améliore la sécurité du système d'exploitation en validant l'intégrité d'un fichier de pilote ou système chaque fois qu'il est chargé en mémoire. En savoir plus sur l'intégrité du code

Cette fonctionnalité est disponible pour les PC et les ressources locales gérés par Configuration Manager et les appareils mobiles gérés avec Microsoft Intune. Les administrateurs peuvent spécifier si le signalement s'effectue par le biais du cloud ou de l'infrastructure locale. La surveillance locale de l'attestation d'intégrité des appareils permet à l'administrateur de surveiller les ordinateurs clients sans accès Internet.

## Activer l'attestation d'intégrité

**Configuration requise :**

- Appareils clients exécutant Windows 10 version 1607 ou Windows Server 2016 version 1607 avec l'option Attestation d'intégrité de l'appareil activée.
- Appareils TPM 1.2 ou TPM 2 compatibles.
- Lors de l'utilisation de la gestion cloud, communication entre l'agent du client Configuration Manager et le point de gestion avec le service d'attestation d'intégrité (gestion du cloud) via *has.spserv.microsoft.com* (port 443). Localement, le client doit être en mesure de communiquer avec le point de gestion dont l'attestation d'intégrité de l'appareil est activée.

**Comment activer la communication avec le service d'attestation d'intégrité sur des ordinateurs clients Configuration Manager**

Utilisez cette procédure pour activer la surveillance de l'attestation d'intégrité des appareils qui se connectent à internet.

1. Dans la console Configuration Manager, choisissez **Administration** > **Vue d'ensemble** > **Paramètres client**. Sélectionnez l'onglet des paramètres de l' **Agent ordinateur** .
2. Dans la boîte de dialogue **Paramètres par défaut** , sélectionnez **Agent ordinateur** , puis accédez à **Activer la communication avec le service d'attestation d'intégrité**.
3. Affectez la valeur **Oui** à **Activer la communication avec le service d'attestation d'intégrité**, puis cliquez

sur **OK**.

4. Ciblez les regroupements d'appareils qui doivent signaler l'intégrité des appareils.

**Comment activer la communication avec le service d'attestation d'intégrité local sur des ordinateurs clients Configuration Manager**

Utilisez cette procédure pour activer la surveillance de l'attestation d'intégrité des appareils en local qui ne se connectent pas à internet.

À partir de Configuration Manager 1702, l'URL du service d'attestation d'intégrité des appareils en local peut être configurée sur le point de gestion pour prendre en charge les appareils clients sans accès à Internet.

1. Dans la console Configuration Manager, accédez à **Administration** > **Vue d'ensemble** > **Configuration du site** > **Sites**.
2. Cliquez avec le bouton droit sur le site principal ou secondaire avec le point de gestion qui prend en charge des clients d'attestation d'intégrité d'appareils en local, puis sélectionnez **Configurer des composants de site** > **Point de gestion**. La page **Propriétés du composant du point de gestion** s'ouvre.
3. Dans l'onglet **Options avancées**, sélectionnez **Ajouter** et spécifiez une URL de service d'attestation d'intégrité des appareils en local. Vous pouvez ajouter plusieurs URL. Si plusieurs URL locales sont spécifiées, les clients reçoivent le jeu complet et choisissent de façon aléatoire celle à utiliser.
4. Dans la console Configuration Manager, choisissez **Administration** > **Vue d'ensemble** > **Paramètres client**. Sélectionnez l'onglet des paramètres de l' **Agent ordinateur** .
5. Dans la boîte de dialogue **Paramètres par défaut**, sélectionnez **Agent ordinateur**, faites défiler jusqu'à **Utiliser le service d'attestation d'intégrité des appareils en local**, puis sélectionnez **Oui**.
6. Ciblez les regroupements d'appareils qui doivent signaler l'intégrité d'appareil avec les paramètres de l'agent client pour activer les rapports d'attestation d'intégrité des appareils.

Vous pouvez également **modifier** ou **supprimer** les URL du service d'attestation d'intégrité des appareils.

> **NOTE**
> Si vous avez utilisé l'attestation d'intégrité des appareils avant la mise à niveau vers Configuration Manager 1702, les URL locales spécifiées dans les paramètres de l'agent du client sont prérempliées dans les propriétés du point de gestion au cours de la mise à niveau. Les clients locaux continueront d'utiliser l'URL spécifiée dans les paramètres de l'agent client jusqu'à ce qu'ils soient mis à niveau. Ils basculeront ensuite vers une URL spécifiée sur le point de gestion.

## Surveiller l'attestation d'intégrité de l'appareil Windows

1. Pour afficher l'attestation d'intégrité de l'appareil, dans la console Configuration Manager, accédez à l'espace de travail **Surveillance** , cliquez sur le nœud **Sécurité** , puis sur **Attestation d'intégrité**.
2. L'attestation d'intégrité de l'appareil s'affiche.

L'attestation d'intégrité des appareils Configuration Manager affiche les informations suivantes :

- **État d'attestation d'intégrité** : indique la répartition des appareils en état conforme, non conforme, d'erreur ou inconnu.
- **Appareils signalant une attestation d'intégrité** : indique le pourcentage d'appareils signalant l'état d'attestation d'intégrité.
- **Appareils non conformes par type de client** : indique la répartition des appareils mobiles et ordinateurs non conformes.
- **Principaux paramètres manquants de l'attestation d'intégrité** : indique le nombre d'appareils auxquels un paramètre d'attestation d'intégrité manque, répertoriés par paramètre manquant.

L'état de l'attestation d'intégrité de l'appareil client permet de définir des règles d'accès conditionnel dans des

stratégies de conformité pour les appareils gérés par Configuration Manager avec Microsoft Intune. Pour plus d'informations, consultez Gérer les stratégies de conformité d'appareils dans System Center Configuration Manager.

# Surveiller l'infrastructure de la hiérarchie et de la réplication dans System Center Configuration Manager

22/06/2018 • 30 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Pour surveiller l'infrastructure et les opérations dans System Center Configuration Manager, utilisez l'espace de travail **Surveillance** dans la console Configuration Manager.

> **NOTE**
> À noter l'exception Migration de cet emplacement, qui est contrôlée directement dans le nœud **Migration** de l'espace de travail **Administration** . Pour plus d'informations, voir Opérations de migration vers System Center Configuration Manager.

En plus d'utiliser la console Configuration Manager pour la surveillance, vous pouvez utiliser les rapports Configuration Manager ou consulter les fichiers journaux Configuration Manager des composants Configuration Manager. Pour plus d'informations sur les rapports, consultez Génération de rapports dans System Center Configuration Manager. Pour plus d'informations sur les fichiers journaux, consultez Fichiers journaux dans System Center Configuration Manager.

Lorsque vous surveillez des sites, recherchez des signes indiquant des problèmes qui vous obligent à prendre des mesures. Par exemple :

- File d'attente de fichiers sur les serveurs de site et les systèmes de site.
- Messages d'état indiquant une erreur ou un problème.
- Échec de communication intrasite.
- Messages d'erreur et d'avertissement dans le journal d'événements système sur les serveurs.
- Messages d'erreur et d'avertissement dans le journal des erreurs Microsoft SQL Server.
- Sites ou clients n'ayant rien rapporté depuis longtemps.
- Réponse lente depuis la base de données SQL Server.
- Signe de défaillance matérielle.

Pour réduire les risques de défaillance d'un site, si les tâches de contrôle révèlent des signes de problèmes, recherchez la source du problème et réparez-le dès que possible.

## Surveiller les tâches de gestion courantes pour Configuration Manager

Configuration Manager assure une surveillance intégrée à partir de la console Configuration Manager. Vous pouvez surveiller de nombreuses tâches, dont celles liées aux mises à jour logicielles, à la gestion de l'alimentation et au déploiement de contenu au sein de votre hiérarchie.

Utilisez les informations suivantes pour vous aider à surveiller les tâches Configuration Manager courantes :

**Alertes**
Consultez Surveiller les alertes dans Utiliser des alertes et le système d'état pour System Center Configuration Manager.

**Paramètres de conformité**
Consultez Comment surveiller les paramètres de compatibilité dans System Center Configuration Manager.

**Déploiement de contenu**
Pour obtenir des informations générales sur la surveillance du contenu, consultez Gérer le contenu et l'infrastructure de contenu pour System Center Configuration Manager.

Pour plus d'informations sur la surveillance de types spécifiques de déploiement de contenu :

- Pour surveiller les applications, consultez Surveiller des applications avec System Center Configuration Manager.
- Pour surveiller les packages et programmes, consultez Comment gérer des packages et des programmes dans Packages et programmes dans System Center Configuration Manager.

**Endpoint Protection**
Consultez Comment surveiller Endpoint Protection dans System Center Configuration Manager.

**Surveiller la gestion de l'alimentation**
Consultez Comment surveiller et planifier la gestion de l'alimentation dans System Center Configuration Manager.

**Surveiller le contrôle de logiciels**
Consultez Surveiller l'utilisation des applications avec le contrôle de logiciel dans System Center Configuration Manager.

**Surveiller les mises à jour logicielles**
Consultez Surveiller les mises à jour logicielles dans System Center Configuration Manager.

# Surveiller l'infrastructure de la hiérarchie pour Configuration Manager

Configuration Manager fournit plusieurs méthodes pour surveiller l'état et les opérations de votre hiérarchie. Vous pouvez vérifier l'état du système des sites de la hiérarchie, surveiller la réplication intersite à partir d'une hiérarchie de site ou une vue géographique, surveiller les liens de réplication entre sites pour la réplication de base de données et utiliser l'outil Analyseur de lien de réplication pour corriger les problèmes de réplication.

**À propos du nœud Hiérarchie de site**

Le nœud **Hiérarchie de site** de l'espace de travail **Surveillance** fournit une vue d'ensemble de votre hiérarchie Configuration Manager et des liens intersites. Vous pouvez utiliser deux vues :

- **Diagramme hiérarchique**: Cette vue affiche votre hiérarchie comme une carte topologique qui a été simplifiée pour afficher uniquement les informations vitales.
- **Vue géographique**: Cette vue affiche vos sites sur une carte géographique présentant les emplacements des sites que vous configurez.

Utilisez le nœud **Hiérarchie de site** pour surveiller l'intégrité de chaque site ainsi que les liens de réplication intersites et leur relation à des facteurs externes, comme un emplacement géographique.

Étant donné que l'état d'un site et l'état des liens intersites sont répliqués en tant que données de site et non en tant que données globales, lorsque vous connectez votre console Configuration Manager à un site principal enfant, vous ne pouvez pas afficher l'état du site ou du lien d'autres sites principaux ou de leurs sites secondaires enfants. Par exemple, dans une hiérarchie comportant plusieurs sites principaux, lorsque votre console Configuration Manager se connecte à un site principal, vous pouvez afficher l'état des sites secondaires enfants,

du site principal et du site d'administration centrale, mais vous ne pouvez pas voir l'état d'autres nœuds de la hiérarchie sous le site d'administration centrale.

Utilisez la commande **Configurer les paramètres** pour contrôler la manière dont est rendu l'affichage de la hiérarchie du site. Lorsque votre console Configuration Manager est connectée à un seul site, les configurations que vous effectuez au niveau du nœud **Hiérarchie de site** sont répliquées sur tous les autres sites.

#### Diagramme hiérarchique

Le diagramme hiérarchique affiche vos sites dans une carte topologique. Dans cette vue, vous pouvez sélectionner un site et afficher un résumé des messages d'état à partir de ce site, effectuer une exploration pour afficher des messages d'état, et accéder à la boîte de dialogue **Propriétés** des sites.

En outre, vous pouvez suspendre le pointeur de souris sur un site ou un lien de réplication entre sites pour afficher l'état de niveau élevé pour cet objet. Étant donné que l'état des liens de réplication n'est pas répliqué globalement, dans une hiérarchie comportant plusieurs sites principaux, vous devez connecter votre console Configuration Manager au site d'administration centrale pour afficher les détails du lien de réplication entre tous les sites.

Les options suivantes modifient le diagramme hiérarchique :

- **Groupes**: vous pouvez configurer le nombre de sites principaux et de sites secondaires qui déclenchent un changement de l'affichage du diagramme hiérarchique, celui-ci combinant les sites dans un seul objet. Lorsque des sites sont combinés dans un seul objet, vous voyez le nombre total de sites et un cumul de niveau élevé des messages d'état et de l'état du site. Les configurations de groupe n'affectent pas la vue géographique.
- **Sites favoris**: Vous pouvez spécifier des sites individuels comme sites favoris. Une icône en forme d'étoile identifie un site favori dans le diagramme hiérarchique. Les sites favoris ne sont pas combinés à d'autres sites lorsque vous avez utilisé des groupes et ils sont toujours affichés individuellement.

#### Vue géographique

La vue géographique affiche l'emplacement de chaque site sur une carte géographique. Seuls les sites que vous configurez avec un emplacement sont affichés. Lorsque vous sélectionnez un site dans cette vue, les liens de réplication vers des sites parents ou enfants sont affichés. Contrairement à l'affichage du diagramme hiérarchique, vous ne pouvez pas afficher les détails du lien de réplication ou du message d'état de site dans cette vue.

> **NOTE**
> Pour utiliser la vue géographique, Internet Explorer doit être installé sur l'ordinateur auquel se connecte votre console Configuration Manager et cet ordinateur doit pouvoir accéder à Bing Maps à l'aide du protocole HTTP.

L'option suivante modifie la vue géographique.

- **Emplacement de site**: vous pouvez spécifier un emplacement géographique pour chaque site. L'emplacement peut être spécifié sous forme de nom de rue, de lieu, par exemple un nom de ville, ou par des coordonnées de latitude et de longitude. Par exemple, pour indiquer la latitude et la longitude de Redmond Washington, vous devez spécifier **47 40 26.3572 Nord 122 7 17.4432 Ouest** pour l'emplacement du site. Il n'est pas nécessaire de spécifier le symbole des degrés, minutes ou secondes de longitude ou de latitude. Configuration Manager utilise Bing Maps pour afficher l'emplacement de la vue géographique. Cela vous permet d'afficher votre hiérarchie par rapport à un emplacement géographique, ce qui peut fournir des informations sur des problèmes régionaux susceptibles d'affecter des sites spécifiques ou la réplication intersite.

  Lorsque vous spécifiez un emplacement, vous pouvez utiliser la zone **Emplacement** pour rechercher un site spécifique dans votre hiérarchie. Après avoir sélectionné le site, entrez l'emplacement sous forme de

nom de ville ou d'adresse postale dans la colonne **Emplacement** . Configuration Manager utilise Bing Maps pour résoudre l'emplacement.

### Comment surveiller des liens de réplication de la base de données et l'état de la réplication

En plus des détails approfondis accessibles à partir du nœud **Hiérarchie de site** de l'espace de travail **Surveillance** , vous pouvez également surveiller les détails de la réplication de la base de données quand vous utilisez le nœud **Réplication de la base de données** de l'espace de travail **Surveillance** . À partir de **Réplication de la base de données**, vous pouvez surveiller l'état des liens de réplication entre les sites, ainsi que les détails de l'initialisation et de la réplication des groupes de réplication sur le site auquel votre console Configuration Manager est connectée.

> **TIP**
> Un nœud **Réplication de la base de données** apparaît également sous le nœud **Configuration de la hiérarchie** dans l'espace de travail **Administration** , mais vous ne pouvez pas afficher l'état de réplication des liens de réplication de la base de données à partir de cet emplacement.

#### État des liens de réplication

La réplication de base de données entre sites implique la réplication de plusieurs ensembles d'informations, appelés groupes de réplication. Chaque groupe de réplication est répliqué avec différentes priorités de réplication. Par défaut, les données contenues dans un groupe de réplication et la fréquence de réplication ne peuvent pas être modifiées.

Lorsqu'un lien de réplication est actif et ne présente pas un état en échec ou détérioré, tous les groupes de réplication répliquent dans un délai raisonnable. Si un ou plusieurs groupes de réplication ne parviennent pas à répliquer dans le délai prévu, le lien s'affiche comme détérioré. Les liens détériorés continuent de fonctionner, mais envisagez de les surveiller pour vous assurer qu'ils repassent à l'état actif ou vérifiez-les pour vous assurer qu'ils ne se détériorent pas davantage et que la réplication n'échoue pas.

Pour chaque lien de réplication, vous pouvez spécifier le nombre de tentatives de réplication d'un groupe de réplication qui ne parvient pas à terminer la réplication avant que l'état du lien ne soit défini comme détérioré ou en échec. Même si un seul groupe de réplication ne parvient pas à se répliquer alors que les autres le font correctement, l'état du lien est défini comme détérioré ou en échec car un groupe de réplication ne parvient pas à se répliquer à l'issue du nombre de tentatives spécifié. Pour plus d'informations sur les seuils de réplication, consultez la section Seuils de réplication de la base de données dans Transfert de données entre sites dans System Center Configuration Manager.

Utilisez les informations dans le tableau suivant pour comprendre l'état des liens de réplication susceptibles de nécessiter davantage de recherches.

| DESCRIPTION DU LIEN | PLUS D'INFORMATIONS |
| --- | --- |
| **Le lien est actif** | Aucun problème n'a été détecté et la communication dans le lien est en cours. |

| DESCRIPTION DU LIEN | PLUS D'INFORMATIONS |
| --- | --- |
| **Le lien est dégradé** | La réplication est fonctionnelle, mais au moins un objet ou groupe de réplication a été retardé. Surveillez les liens dans cet état et consultez les informations depuis les deux sites sur le lien pour obtenir des indications sur l'éventualité d'un échec du lien.<br><br>Un lien peut également afficher un état dégradé lorsque le site qui reçoit les données répliquées ne peut pas valider rapidement les données dans la base de données. Cela peut se produire lors de la réplication de volumes importants de données. Par exemple, si vous déployez une mise à jour logicielle sur un grand nombre d'ordinateurs, le site parent sur le lien peut prendre un certain temps pour traiter le volume de données répliquées. Un délai de traitement sur le site parent peut entraîner la dégradation de l'état du lien jusqu'à ce que le site parent puisse traiter correctement les données en attente. |
| **Le lien a échoué** | La réplication ne fonctionne pas. Il est possible qu'un lien de réplication puisse être rétabli sans action supplémentaire. Vous pouvez utiliser l'Analyseur de lien de réplication pour examiner et corriger la réplication sur ce lien.<br><br>Cet état peut également indiquer un problème du réseau physique entre le site parent et enfant sur le lien de réplication. |

Pendant le processus de mise à niveau d'un site parent vers un nouveau Service Pack, l'état du lien s'affiche comme étant actif si vous l'affichez à partir du site enfant. Après la mise à niveau et jusqu'à la mise à niveau du site enfant vers le même Service Pack que le site parent, l'état du lien s'affiche comme étant actif depuis le site parent et comme étant en cours de configuration depuis le site enfant.

#### État de la réplication

Vous pouvez utiliser le nœud **Réplication de la base de données** dans l'espace de travail **Surveillance** pour afficher l'état de réplication d'un lien de réplication et afficher des détails sur la base de données de site sur chaque site se trouvant sur le lien de réplication. Vous pouvez également afficher des détails sur les groupes de réplication. Pour afficher les détails, sélectionnez un lien de réplication, puis sélectionnez l'onglet correspondant à l'état de réplication à afficher. Le tableau suivant fournit des détails sur les différents onglets relatifs à l'état de la réplication.

### Résumé

Permet d'afficher des informations de haut niveau sur la réplication des données de site et des données globales entre les deux sites sur un lien.

Vous pouvez également cliquer sur **Afficher les rapports des données de l'historique du trafic** pour afficher un rapport avec les détails sur la bande passante de réseau utilisée par la réplication sur l'intégralité du lien de réplication.

### Site parent

Pour le site parent sur un lien de réplication, affichez les détails sur la base de données, notamment :

- Ports de pare-feu pour SQL Server
- Espace disque disponible
- Emplacements de fichiers de base de données
- Certificats

**Site enfant**
Pour le site enfant sur un lien de réplication, affichez les détails sur la base de données, notamment :

- Ports de pare-feu pour SQL Server
- Espace disque disponible
- Emplacements de fichiers de base de données
- Certificats

**Détail de l'initialisation**
Permet d'afficher l'état d'initialisation des groupes de réplication qui répliquent sur l'intégralité du lien de réplication. Ces informations peuvent vous aider à identifier quand l'initialisation des données de réplication est en cours ou en échec.

De plus, vous pouvez utiliser ces informations pour identifier quand un site peut se trouver en mode d'interopérabilité. Le mode d'interopérabilité se produit lorsque le site enfant n'exécute pas la même version de Configuration Manager que le site parent.

**Détail de la réplication**
Permet d'afficher l'état de réplication de chaque groupe de réplication qui réplique sur l'intégralité du lien. Utilisez ces informations pour aider à identifier des problèmes ou des retards pour la réplication de données spécifiques et pour aider à déterminer les seuils de réplication de la base de données appropriés pour ce lien. Pour plus d'informations sur les seuils de réplication de la base de données, consultez la section Seuils de réplication de la base de données dans Transfert de données entre sites dans System Center Configuration Manager.

> **TIP**
> Les groupes de réplication de données de site sont envoyés uniquement à partir du site enfant vers le site parent. Les groupes de réplication pour les données globales sont répliqués dans les deux directions.

**À propos de l'analyseur de lien de réplication**

Configuration Manager inclut l'**analyseur de lien de réplication** que vous utilisez pour analyser et réparer les problèmes de réplication. Vous pouvez utiliser l'analyseur de lien de réplication pour corriger les échecs de lien de réplication en cas d'échec de la réplication et lorsque la réplication cesse de fonctionner mais n'a pas encore été signalée comme ayant échoué. L'analyseur de lien de réplication peut être utilisé pour corriger les problèmes de réplication entre les ordinateurs suivants dans la hiérarchie Configuration Manager (la direction de l'échec de réplication n'a aucune importance) :

- Entre un serveur de site et le serveur de base de données de site.
- Entre un serveur de base de données de site des sites et un autre ordinateur de base de données de site des sites (réplication intersite).

Vous pouvez exécuter l'analyseur de lien de réplication dans la console Configuration Manager ou à partir d'une invite de commandes :

- Pour l'exécuter dans la console Configuration Manager : dans l'espace de travail **Surveillance**, cliquez sur le nœud **Réplication de la base de données**, sélectionnez le lien de réplication à analyser, puis, dans le groupe **Réplication de la base de données**, sous l'onglet **Accueil**, sélectionnez **Analyseur de lien de réplication**.
- Pour l'exécuter à l'invite de commandes, entrez la commande suivante : **%chemin%\Microsoft Configuration Manager\AdminConsole\bin\Microsoft.ConfigurationManager.ReplicationLinkAnalyzer.Wizard**

**.exe <nom de domaine complet du serveur de site source> <nom de domaine complet du serveur de site de destination>**

Lorsque vous exécutez l'analyseur de lien de réplication, celui-ci détecte les problèmes à l'aide d'une série de règles et contrôles de diagnostic. Lorsque l'outil est exécuté, vous voyez les problèmes identifiés par celui-ci. Des instructions pour résoudre un problème, lorsqu'elles sont connues, sont affichées. Si l'analyseur de lien de réplication peut corriger automatiquement un problème, cette option vous est présentée. Une fois l'analyseur de lien de réplication terminé, celui-ci enregistre les résultats dans le rapport suivant basé sur XML et un fichier journal sur le bureau de l'utilisateur qui exécute l'outil :

- ReplicationAnalysis.xml
- ReplicationLinkAnalysis.log

Lorsque l'analyseur de lien de réplication s'exécute, il arrête les services suivants pendant la correction des problèmes, puis il redémarre ces services une fois la correction terminée :

- SMS_SITE_COMPONENT_MANAGER
- SMS_EXECUTIVE

Si l'analyseur de lien de réplication ne parvient pas à terminer la correction, vérifiez le serveur de site et redémarrez ces services s'ils sont arrêtés.

Les actions de recherche et de correction ayant réussi et celles ayant échoué sont consignées pour fournir des détails supplémentaires qui ne sont pas présentés dans l'interface de l'outil.

**Conditions requises pour utiliser l'analyseur de lien de réplication :**

- Le compte que vous utilisez pour exécuter l'analyseur de lien de réplication doit disposer de droits d'administrateur local sur chaque ordinateur qui est impliqué dans le lien de réplication. Le compte ne nécessite pas de rôle de sécurité d'administration basé sur des rôles spécifiques. Par conséquent, un utilisateur administratif disposant d'un accès au nœud **Réplication de la base de données** peut exécuter l'outil dans la console Configuration Manager, ou un administrateur système possédant des droits suffisants vers chaque ordinateur peut exécuter l'outil à une invite de commandes.
- Le compte que vous utilisez pour exécuter l'analyseur de lien de réplication doit disposer de droits d'administrateur système sur chaque base de données SQL Server qui est impliquée dans le lien de réplication.

**Problèmes connus de l'analyseur de lien de réplication :**

- Avec la version 1511 de System Center Configuration Manager, l'analyseur de lien de réplication génère des erreurs de certificat SQL Server Service Broker pour les sites principaux mis à niveau à partir de System Center 2012 Configuration Manager. Ces erreurs sont dues à des modifications des noms des certificats introduits dans la version 1511 pour lesquels l'analyseur de lien de réplication n'a pas encore été mis à jour. Vous pouvez ignorer ces erreurs sans risque.

### Procédures de surveillance de la réplication de la base de données

#### Pour surveiller l'état de réplication de base de données entre sites de niveau élevé

1. Dans la console Configuration Manager, cliquez sur **Surveillance**.
2. Dans l'espace de travail **Surveillance** , cliquez sur **Hiérarchie de site** pour ouvrir la vue **Diagramme hiérarchique** .
3. Suspendre brièvement le pointeur de souris sur la ligne entre les deux sites pour afficher l'état de réplication globale et des données de site pour ces sites.

#### Pour surveiller l'état de réplication d'un lien de réplication

1. Dans la console Configuration Manager, cliquez sur **Surveillance**.

2. Dans l'espace de travail **Surveillance** , cliquez sur **Réplication de la base de données**, puis sélectionnez le lien de réplication pour le lien que vous souhaitez surveiller. Ensuite, dans l'espace de travail, sélectionnez l'onglet approprié pour afficher différents détails sur l'état de la réplication de ce lien.

# Transfert de données entre sites dans System Center Configuration Manager

22/06/2018 • 43 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

System Center Configuration Manager utilise la **réplication basée sur les fichiers** et la **réplication de base de données** pour transférer différents types d'informations entre les sites. Découvrez comment Configuration Manager déplace les données entre les sites et comment vous pouvez gérer le transfert des données sur votre réseau.

## File-based replication

Configuration Manager utilise la réplication basée sur les fichiers pour transférer des données basées sur les fichiers entre les sites dans votre hiérarchie. Ces données incluent les applications et les packages que vous voulez déployer sur des points de distribution dans des sites enfants, ainsi que les enregistrements de données de découverte non traités qui sont transférés vers les sites parents puis traités.

La communication basée sur les fichiers entre les sites utilise le protocole SMB (**Server Message Block**) sur le port TCP/IP 445. Vous pouvez spécifier la limitation de bande passante et le mode impulsion pour contrôler la quantité de données transférées sur le réseau, et vous pouvez utiliser des planifications pour contrôler à quel moment les données sont envoyées sur le réseau.

### Itinéraires de réplication de fichiers

Les informations suivantes peuvent vous aider à configurer et à utiliser les itinéraires de réplication de fichiers.

#### Itinéraire de réplication de fichiers

Chaque itinéraire de réplication de fichiers identifie un site de destination vers lequel les données basées sur des fichiers peuvent être transférées. Chaque site prend en charge un seul itinéraire de réplication de fichiers vers un site de destination spécifique.

Vous pouvez modifier les paramètres suivants pour les itinéraires de réplication de fichiers :

- **Compte de réplication de fichiers**. Ce compte se connecte au site de destination et écrit des données dans le partage **SMS_Site** de ce site. Les données écrites dans ce partage sont traitées par le site de réception. Par défaut, quand un site est ajouté à la hiérarchie, Configuration Manager attribue le compte d'ordinateur du serveur de site du nouveau site comme Compte de réplication de fichiers de ce site. Ce compte est ensuite ajouté au groupe **SMS_SiteToSiteConnection_<code_site>** du site de destination, un groupe local sur l'ordinateur qui accorde l'accès au partage SMS_Site. Vous pouvez modifier ce compte en un compte d'utilisateur Windows. Si vous changez le compte, veillez à ajouter le nouveau compte au groupe **SMS_SiteToSiteConnection_<code_site>** du site de destination.

  > **NOTE**
  > Les sites secondaires utilisent toujours le compte d'ordinateur du serveur de site secondaire en tant que **Compte de réplication de fichiers**.

- **Planification**. Vous pouvez établir le calendrier de chaque itinéraire de réplication de fichiers pour restreindre le type de données et la période de transfert des données vers le site de destination.

- **Limites du taux de transfert**. Vous pouvez spécifier des limites de taux de transfert pour chaque

itinéraire de réplication de fichiers, afin de contrôler la bande passante réseau utilisée lorsque le site transfère les données vers le site de destination :

- Utilisez l'option **Mode impulsion** pour spécifier la taille des blocs de données envoyés vers le site de destination. Vous pouvez également spécifier un délai entre l'envoi de chaque bloc de données. Utilisez cette option lorsque vous devez envoyer des données via une connexion réseau à très faible bande passante vers le site de destination. Par exemple, vous pouvez forcer l'envoi de 1 Ko de données toutes les cinq secondes, mais empêcher l'envoi de 1 Ko toutes les trois secondes, quelle que soit la vitesse de la liaison ou son utilisation.
- Utilisez l'option **Limité aux taux de transfert maximaux indiqués par heure** pour permettre à un site d'envoyer des données vers un site de destination en utilisant uniquement le pourcentage de temps spécifié. Quand vous utilisez cette option, Configuration Manager n'identifie pas la bande passante disponible du réseau, mais divise plutôt le temps pendant lequel il peut envoyer des données en périodes plus petites. Ensuite, les données sont envoyées pendant une courte plage horaire, suivie de plages horaires pendant lesquelles aucune donnée n'est envoyée. Par exemple, si le taux maximal est fixé à **50 %**, Configuration Manager transmet les données pendant une durée, suivie d'une période d'une durée égale pendant laquelle aucune donnée n'est envoyée. La taille effective des donnés (taille des blocs de données) n'est pas gérée. En revanche, seule la durée pendant laquelle des données sont envoyées est gérée.

  Caution

  Par défaut, un site peut utiliser jusqu'à trois **envois simultanés** pour transférer des données vers un site de destination. Lorsque vous définissez des limites de taux pour un itinéraire de réplication de fichiers, les **envois simultanés** dans le cadre de l'envoi de données vers ce site sont limités à un. Cela s'applique même lorsque l'option **Limiter la bande passante disponible (%)** est définie sur **100 %**. Par exemple, si vous utilisez les paramètres par défaut pour l'expéditeur, le taux de transfert vers le site de destination est réduit à un tiers de la capacité par défaut.

- Vous pouvez configurer un itinéraire de réplication de fichiers entre deux sites secondaires pour acheminer du contenu basé sur des fichiers entre ces sites.

Pour gérer un itinéraire de réplication de fichiers, dans l'espace de travail **Administration**, développez le nœud **Configuration de la hiérarchie**, puis sélectionnez **Réplication de fichiers**.

#### Expéditeur

Chaque site a un expéditeur. L'expéditeur gère la connexion réseau entre un site et un site de destination et peut établir des connexions vers plusieurs sites à la fois. Pour se connecter à un site, l'expéditeur utilise l'itinéraire de réplication de fichiers vers le site pour identifier le compte à utiliser pour établir la connexion réseau. L'expéditeur utilise également ce compte pour écrire des données dans le partage SMS_Site du site de destination.

Par défaut, l'expéditeur écrit des données sur un site de destination en utilisant plusieurs **envois simultanés**, généralement appelés « thread ». Chaque envoi simultané (ou « thread ») peut transférer un objet basé sur un fichier différent vers le site de destination. Par défaut, lorsque l'expéditeur commence à envoyer un objet, il continue d'écrire des blocs de données pour cet objet jusqu'à la fin de l'envoi de l'objet complet. Une fois que toutes les données de l'objet ont été envoyées, l'envoi d'un nouvel objet peut commencer sur ce thread.

Vous pouvez modifier les paramètres suivants pour un expéditeur :

- **Nombre maximal d'envois simultanés**. Par défaut, chaque site utilise cinq envois simultanés, dont trois peuvent être utilisés dans le cadre de l'envoi de données vers un site de destination quelconque. En augmentant ce nombre, vous pouvez augmenter le débit des données échangées entre les sites, car Configuration Manager peut transférer davantage de fichiers à la fois. Cela a également pour effet d'augmenter la demande en bande passante entre les sites.
- **Paramètres de nouvelle tentative**. Par défaut, chaque site effectue deux nouvelles tentatives de connexion en cas de problème, avec un délai d'une minute entre deux essais. Vous pouvez modifier le

nombre de tentatives de connexion du site, ainsi que le délai d'attente entre les tentatives.

Pour gérer l'expéditeur pour un site, dans l'espace de travail **Administration**, développez le nœud **Configuration du site**, sélectionnez le nœud **Sites**, puis cliquez sur **Propriétés** pour le site à gérer. Sélectionnez l'onglet **Expéditeur** pour modifier les paramètres de l'expéditeur.

## Database replication

La réplication de base de données Configuration Manager utilise SQL Server pour transférer les données et fusionner les modifications apportées à la base de données d'un site avec les informations stockées dans la base de données sur d'autres sites de la hiérarchie. Notez les éléments suivants sur la réplication de base de données :

- Tous les sites partagent les mêmes informations.
- Quand vous installez un site dans une hiérarchie, la réplication de base de données est établie automatiquement entre le nouveau site et son site parent désigné.
- Une fois l'installation du site terminée, la réplication de base de données démarre automatiquement.

Quand vous ajoutez un nouveau site à une hiérarchie, Configuration Manager crée une base de données générique sur le nouveau site. Ensuite, le site parent crée un instantané des données appropriées dans sa base de données, puis transfère cet instantané vers le nouveau site par réplication basée sur des fichiers. Le nouveau site utilise ensuite le programme de copie en bloc de SQL Server pour charger les informations dans sa copie locale de la base de données Configuration Manager. Une fois l'instantané chargé, chaque site effectue une réplication de base de données avec l'autre site.

Pour répliquer des données entre les sites, Configuration Manager utilise son propre service de réplication de base de données. Le service de réplication de base de données utilise le suivi des modifications de SQL Server pour surveiller les modifications apportées à la base de données du site local, puis réplique ces modifications sur les autres sites à l'aide de SQL Server Service Broker (SSB). Par défaut, ce processus utilise le port TCP/IP 4022.

Configuration Manager regroupe les données répliquées par la réplication de base de données dans différents groupes de réplication. Notez les éléments suivants sur les groupes de réplication :

- À chaque groupe de réplication correspond une planification de réplication fixe et distincte qui détermine la fréquence de réplication vers d'autres sites des modifications apportées aux données.

  Par exemple, une modification apportée à une configuration d'administration basée sur des rôles est répliquée rapidement sur d'autres sites pour que ces modifications soient appliquées dès que possible. En revanche, une modification de configuration de plus basse priorité, telle qu'une demande d'installation d'un nouveau site secondaire, est répliquée avec moins d'urgence. Une nouvelle demande de site peut mettre plusieurs minutes pour atteindre le site principal de destination.

- Vous pouvez modifier les paramètres suivants de réplication de base de données :

  - **Liens de réplication de base de données**. Contrôlez quand un trafic spécifique traverse le réseau.
  - **Vues distribuées**. Changez les paramètres des liens de réplication qui permettent aux demandes formulées sur un site d'administration centrale relatives à des données de site sélectionnées d'accéder à ces données directement à partir de la base de données d'un site principal enfant.
  - **Planifications**. Spécifiez quand un lien de réplication doit être utilisé et quand différents types de données de site sont répliqués.
  - **Totalisation**. Changez les paramètres de totalisation des données concernant le trafic réseau qui traverse les liens de réplication. La totalisation a lieu toutes les 15 minutes par défaut et est utilisée pour la réplication de base de données dans les rapports.
  - **Seuils de réplication de base de données**. Définissez quand les liens sont signalés comme détériorés ou en échec. Vous pouvez également configurer à quel moment Configuration Manager doit déclencher des alertes au sujet des liens de réplication dont l'état est Détérioré ou Échec.

Configuration Manager classe les données qu'il réplique via la réplication de base de données comme **données globales** ou **données de site**. Lorsqu'une réplication de base de données se produit, les modifications apportées aux données globales et aux données de site sont transférées via le lien de réplication de base de données. Les données globales peuvent être répliquées vers un site parent ou enfant. Les données de site sont répliquées uniquement vers un site parent. Un troisième type de données, les données locales, n'est pas répliqué vers d'autres sites. Les données locales sont des informations qui ne sont pas requises par les autres sites. Notez les éléments suivants concernant les types de données :

- **Données globales**. Les données globales font référence aux objets créés par l'administrateur et qui sont répliquées sur tous les sites dans la hiérarchie, bien que les sites secondaires reçoivent uniquement un sous-ensemble des données globales, en tant que données globales proxy. Les déploiements logiciels, les mises à jour logicielles, les définitions de regroupement et les étendues de la sécurité de l'administration basée sur les rôles sont autant d'exemples de données globales. Les administrateurs peuvent créer des données globales sur des sites d'administration centrale et des sites principaux.
- **Données de site**. Les données de site font référence aux informations opérationnelles créées par les sites principaux Configuration Manager et les clients qui sont sous la hiérarchie de sites principaux. Les données de site sont répliquées vers le site d'administration centrale mais pas vers d'autres sites principaux. Les données de site incluent les données d'inventaire matériel, les messages d'état, les alertes et les résultats de regroupements basés sur des requêtes. Les données de site ne peuvent être consultées que sur le site d'administration centrale et sur le site principal d'où proviennent les données. Les données de site ne peuvent être modifiées que sur le site principal sur lequel elles ont été créées.

  Toutes les données de site sont répliquées vers le site d'administration centrale. Ce site effectue l'administration et la création de rapports pour toute la hiérarchie des sites.

Les sections suivantes détaillent les paramètres que vous pouvez modifier pour gérer la réplication de base de données.

**liens de réplication de base de données**

Quand vous installez un nouveau site dans une hiérarchie, Configuration Manager crée automatiquement un lien de réplication de base de données entre le site parent et le nouveau site. Un lien unique est créé pour connecter les deux sites.

Vous pouvez modifier les paramètres pour chaque lien de réplication de base de données afin de contrôler plus aisément le transfert de données via le lien de réplication. Chaque lien de réplication prend en charge des configurations distinctes. Les contrôles pour les liens de réplication de base de données sont les suivants :

- Arrêtez la réplication de données de site sélectionnées à partir d'un site principal vers le site d'administration centrale, afin que le site d'administration centrale puisse accéder directement à ces données à partir de la base de données du site principal.
- Planifiez les données de site sélectionnées à transférer d'un site principal enfant vers le site d'administration centrale.
- Définissez les paramètres qui déterminent quand un lien de réplication de base de données a l'état Détérioré ou Échec.
- Spécifiez à quel moment déclencher des alertes dans le cas d'un lien de réplication en échec.
- Spécifiez la fréquence à laquelle Configuration Manager résume les données sur le trafic de réplication qui utilise le lien de réplication. Ces données sont utilisées dans les rapports.

Pour configurer un lien de réplication de base de données, dans la console Configuration Manager, dans le nœud **Réplication de la base de données**, modifiez les propriétés du lien. Ce nœud apparaît dans l'espace de travail **Surveillance** et dans l'espace de travail **Administration**, sous le nœud **Configuration de la hiérarchie**. Vous pouvez modifier un lien de réplication à partir du site parent ou du site enfant du lien de réplication.

> **TIP**
> Vous pouvez modifier les liens de réplication de base de données à partir du nœud **Réplication de la base de données** dans chaque espace de travail. Toutefois, lorsque vous utilisez le nœud **Réplication de la base de données** dans l'espace de travail **Surveillance**, vous pouvez également consulter l'état de la réplication de base de données des liens de réplication et accéder à l'outil Analyseur de lien de réplication pour mieux identifier les problèmes de réplication de base de données.

Pour plus d'informations sur la configuration des liens de réplication, voir Contrôles de réplication de la base de données du site. Pour plus d'informations sur la surveillance de la réplication, consultez Comment surveiller des liens de réplication de la base de données et l'état de la réplication dans la rubrique Surveiller l'infrastructure de la hiérarchie et de la réplication dans System Center Configuration Manager.

Pour planifier des liens de réplication de base de données, aidez-vous des informations figurant dans les sections suivantes.

**vues distribuées**

Les vues distribuées permettent aux demandes formulées sur un site d'administration centrale relatives à des données de site sélectionnées d'accéder à ces données directement à partir de la base de données d'un site principal enfant. L'accès direct évite d'avoir à répliquer ces données de site du site principal vers le site d'administration centrale. Comme chaque lien de réplication est indépendant des autres liens de réplication, vous pouvez utiliser les vues distribuées uniquement sur les liens de réplication de votre choix. Vous ne pouvez pas utiliser les vues distribuées entre un site principal et un site secondaire.

Les vues distribuées peuvent offrir les avantages suivants :

- Elles diminuent la charge du processeur lors du traitement des modifications apportées à la base de données sur le site d'administration centrale et les sites principaux.
- Elles réduisent la quantité de données transférées sur le réseau à destination du site d'administration centrale.
- Elles améliorent les performances du serveur SQL Server qui héberge la base de données du site d'administration centrale.
- Elles réduisent l'espace disque utilisé par la base de données sur le site d'administration centrale.

Vous pouvez envisager d'utiliser des vues distribuées lorsqu'un site principal est situé à proximité du site d'administration centrale sur le réseau et que les deux sites sont toujours actifs et connectés. En effet, les vues distribuées remplacent la réplication des données sélectionnées entre les sites par des connexions directes entre les serveurs SQL Server de chaque site. Une connexion directe est établie chaque fois qu'une demande portant sur ces données est formulée sur le site d'administration centrale. En règle générale, les demandes de données que vous pouvez autoriser pour les vues distribuées sont formulées lorsque vous exécutez des rapports ou des requêtes, lorsque vous consultez des informations dans l'Explorateur de ressources et par l'évaluation des regroupements lorsque ceux-ci incluent des règles basées sur les données de site.

Par défaut, les vues distribuées sont désactivées pour chaque lien de réplication. Lorsque vous activez les vues distribuées pour un lien de réplication, vous sélectionnez les données de site qui ne seront pas répliquées vers le site d'administration centrale via ce lien. Le site d'administration centrale accède à ces données directement à partir de la base de données du site principal enfant qui partage le lien. Pour les vues distribuées, vous pouvez configurer les types de données de site suivants :

- Données d'inventaire matériel des clients
- Données d'inventaire et de contrôle de logiciel des clients
- Messages d'état en provenance des clients, du site principal et de tous les sites secondaires

Sur le plan opérationnel, les vues distribuées sont invisibles pour un utilisateur administratif qui consulte des données dans la console Configuration Manager ou dans des rapports. Quand une demande est effectuée pour

des données activées pour les vues distribuées, le serveur SQL Server qui héberge la base de données du site d'administration centrale accède directement au serveur SQL Server du site principal enfant afin d'extraire les informations. Par exemple, vous utilisez une console Configuration Manager au niveau du site d'administration centrale pour demander des informations sur l'inventaire matériel de deux sites alors qu'un seul des deux possède un inventaire matériel compatible avec une vue distribuée. Les informations d'inventaire pour les clients du site qui n'est pas configuré pour les vues distribuées sont extraites de la base de données au niveau du site d'administration centrale. Les informations d'inventaire des clients du site qui est configuré pour les vues distribuées sont accessibles à partir de la base de données au niveau du site principal enfant. Ces informations apparaissent dans la console Configuration Manager ou dans un rapport sans que la source soit identifiée.

Tant qu'un lien de réplication comporte un type de données activé pour les vues distribuées, le site principal enfant ne réplique pas ces données sur le site d'administration centrale. Dès que vous désactivez les vues distribuées pour un type de données, le site principal enfant reprend la réplication des données sur le site d'administration centrale dans le cadre d'une réplication normale des données. Toutefois, pour que ces données soient disponibles au niveau du site d'administration centrale, les groupes de réplication qui les contiennent doivent être réinitialisés entre le site principal et le site d'administration centrale. De même, après la désinstallation d'un site principal dont les vues distribuées sont activées, le site d'administration centrale doit effectuer la réinitialisation de ses données pour que vous puissiez accéder aux données activées pour les vues distribuées sur le site d'administration centrale.

> **IMPORTANT**
> Lorsque vous utilisez les vues distribuées sur un lien de réplication quelconque dans la hiérarchie des sites, vous devez les désactiver pour tous les liens de réplication avant de désinstaller un site principal. Pour plus d'informations, consultez Désinstaller un site principal configuré avec des vues distribuées.

**Prérequis et limitations des vues distribuées**

- Vous pouvez utiliser les vues distribuées uniquement sur des liens de réplication entre un site d'administration centrale et un site principal.
- Le site d'administration centrale doit utiliser une édition Enterprise de SQL Server. Le site principal n'a pas cette exigence.
- Le site d'administration centrale peut disposer d'une seule instance du fournisseur SMS installée, et cette instance doit être installée sur le serveur de base de données du site. Cette contrainte sert à prendre en charge l'authentification Kerberos requise pour permettre au serveur SQL Server au niveau du site d'administration centrale d'accéder au serveur SQL Server au niveau du site principal enfant. Il n'existe aucune limitation sur le fournisseur SMS au niveau du site principal enfant.
- Le site d'administration centrale peut disposer d'un seul point SQL Server Reporting Services installé, et ce dernier doit se trouver sur le serveur de base de données du site. Cette contrainte sert à prendre en charge l'authentification Kerberos requise pour permettre au serveur SQL Server au niveau du site d'administration centrale d'accéder au serveur SQL Server au niveau du site principal enfant.
- La base de données du site ne peut pas être hébergée sur un cluster SQL Server.
- La base de données du site ne peut pas être hébergée sur un groupe de disponibilité SQL Server Always On.
- Le compte d'ordinateur du serveur de base de données du site d'administration centrale requiert des autorisations de lecture pour la base de données du site principal.

> **IMPORTANT**
> Les vues distribuées et les planifications des périodes où les données peuvent être répliquées sont des paramètres qui s'excluent mutuellement pour un lien de réplication de base de données.

### Planifier les transferts de données de site sur les liens de réplication de la base de données

Pour mieux contrôler la bande passante réseau utilisée pour répliquer les données de site depuis un site principal

enfant vers son site d'administration centrale, vous pouvez planifier le moment auquel un lien de réplication est utilisé, ainsi que spécifier quand les différents types de données de site se répliquent. Vous pouvez contrôler le moment auquel le site principal réplique les messages d'état, l'inventaire et les données de contrôle. Les liens de réplication de la base de données des sites secondaires ne prennent pas en charge les planifications des données de site. Le transfert de données globales ne peut pas être planifié.

Quand vous configurez une planification de lien de réplication de la base de données, vous pouvez restreindre le transfert des données de site sélectionnées depuis le site principal vers le site d'administration centrale et vous pouvez configurer différentes heures pour répliquer des types différents de données de site.

> **IMPORTANT**
> Les vues distribuées et les planifications relatives aux dates de réplication des données sont des configurations qui s'excluent mutuellement pour un lien de réplication de la base de données.

**Synthèse du trafic de réplication de la base de données**

Chaque site réalise régulièrement une synthèse des données sur le trafic réseau qui traverse les liens de réplication de la base de données pour ce site. Les données résumées sont utilisées dans les rapports pour la réplication de la base de données. Les deux sites sur un lien de réplication résument le trafic réseau qui traverse le lien de réplication. Le résumé des données est effectué par le serveur SQL Server qui héberge la base de données du site. Une fois les données résumées, les informations sont répliquées vers d'autres sites en tant que données globales.

Par défaut, le résumé se produit toutes les 15 minutes. Pour modifier la fréquence de synthèse du trafic réseau, dans les propriétés du lien de réplication de la base de données, modifiez la valeur **Intervalle de résumé**. La fréquence de synthèse affecte les informations affichées dans les rapports sur la réplication de la base de données. Vous pouvez choisir un intervalle compris entre 5 et 60 minutes. Lorsque vous augmentez la fréquence de synthèse, vous augmentez la charge de traitement sur le serveur SQL Server au niveau de chaque site sur le lien de réplication.

**Seuils de réplication de base de données**

Les seuils de réplication de la base de données définissent le moment auquel un lien de réplication de la base de données est signalé comme étant détérioré ou en état d'échec. Par défaut, un lien est défini comme détérioré quand l'un des groupes de réplication ne parvient pas à terminer la réplication à l'issue de 12 tentatives consécutives. Le lien est défini en état d'échec quand l'un des groupes de réplication ne parvient pas à être répliqué à l'issue de 24 tentatives consécutives.

Vous pouvez spécifier des valeurs personnalisées pour ajuster le moment auquel Configuration Manager signale qu'un lien de réplication est détérioré ou en état d'échec. L'ajustement du moment auquel Configuration Manager signale chaque état de vos liens de réplication de la base de données peut vous aider à surveiller l'intégrité de la réplication de la base de données avec précision.

Comme il est possible qu'un ou plusieurs groupes de réplication ne parviennent pas à être répliqués alors que les autres groupes de réplication continuent d'être répliqués correctement, prévoyez de vérifier l'état de réplication d'un lien de réplication dès qu'un état détérioré est signalé. S'il existe des délais récurrents pour des groupes de réplication et qu'ils ne présentent pas de problème, où lorsque la liaison réseau entre les sites dispose d'une faible bande passante disponible, envisagez de modifier le nombre de nouvelles tentatives pour l'état détérioré ou en échec du lien. En augmentant le nombre de nouvelles tentatives à effectuer avant de définir le lien comme détérioré ou en état d'échec, vous pouvez éliminer les faux avertissements liés à des problèmes connus et suivre l'état du lien de manière plus précise.

Prenez en compte également l'intervalle de synchronisation de réplication pour chaque groupe de réplication afin de comprendre la fréquence de réplication de ce groupe. Pour afficher l'**intervalle de synchronisation** des groupes de réplication, dans l'espace de travail **Surveillance**, sous le nœud **Réplication de la base de**

**données**, sélectionnez l'onglet **Détail de la réplication** d'un lien de réplication.

Pour plus d'informations sur la manière de surveiller la réplication de la base de données, y compris la manière d'afficher l'état de réplication, consultez Comment surveiller des liens de réplication de la base de données et l'état de la réplication dans la rubrique Surveiller l'infrastructure de la hiérarchie et de la réplication dans System Center Configuration Manager.

Pour plus d'informations sur la configuration des seuils de réplication de base de données, voir Contrôles de réplication de la base de données du site.

## Contrôles de réplication de la base de données du site

Vous pouvez modifier les paramètres de chaque base de données de site pour mieux contrôler la bande passante réseau utilisée pour la réplication de base de données. Ces paramètres s'appliquent uniquement à la base de données de site dans laquelle vous configurez les paramètres. Ces paramètres sont toujours utilisés lorsque le site réplique des données via la réplication de base de données vers un autre site.

Les contrôles de réplication que vous pouvez modifier pour chaque base de données de site sont les suivants :

- Modifiez le port SSB.
- Configurez le délai d'attente avant que les échecs de réplication déclenchent la réinitialisation de la copie de la base de données du site.
- Configurez une base de données de site afin qu'elle compresse les données qu'elle réplique par réplication de base de données. Les données sont compressées uniquement pour le transfert entre les sites et non pour le stockage dans la base de données du site sur l'un des sites.

Pour modifier les paramètres des contrôles de réplication d'une base de données de site, dans la console Configuration Manager, dans le nœud **Réplication de la base de données**, modifiez les propriétés de la base de données de site. Ce nœud apparaît sous le nœud **Configuration de la hiérarchie** dans l'espace de travail **Administration** et également dans l' **espace de travail Surveillance**. Pour modifier les propriétés de la base de données de site, sélectionnez le lien de réplication entre les sites, puis ouvrez soit **Propriétés de la base de données parent**, soit **Propriétés de la base de données enfant**.

> **TIP**
> Vous pouvez configurer les contrôles de réplication de la base de données à partir du nœud **Réplication de la base de données** dans l'un ou l'autre espace de travail. Toutefois, lorsque vous utilisez le nœud **Réplication de la base de données** dans l'espace de travail **Surveillance**, vous pouvez également afficher l'état de réplication de base de données d'un lien de réplication, puis accéder à l'outil Analyseur de lien de réplication pour mieux identifier les problèmes de réplication.

# Informations techniques de référence sur les requêtes pour System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les requêtes dans System Center Configuration Manager retournent des informations de la base de données du site en fonction des critères que vous spécifiez. Vous pouvez utiliser des requêtes pour récupérer des informations sur les ressources de votre site ou sur les données d'inventaire et les messages d'état.

## Rubriques dédiées à l'utilisation des requêtes dans Configuration Manager

Utilisez les rubriques suivantes pour vous aider à utiliser des requêtes dans Configuration Manager :

- Présentation des requêtes dans System Center Configuration Manager
- Opérations et maintenance pour les requêtes dans System Center Configuration Manager
- Sécurité et confidentialité pour les requêtes dans System Center Configuration Manager

# Présentation des requêtes dans System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez créer et exécuter des requêtes pour rechercher les objets dans une hiérarchie System Center Configuration Manager qui correspondent à vos critères de requête. Ces objets incluent des éléments tels que des types spécifiques d'ordinateurs ou de groupes d'utilisateurs. Les requêtes peuvent renvoyer la plupart des types d'objets Configuration Manager, à savoir des sites, des regroupements, des applications et des données d'inventaire.

Quand vous créez une requête, vous devez spécifier au moins deux paramètres : où effectuer la recherche et ce que vous souhaitez rechercher. Par exemple, pour rechercher la quantité d'espace disponible sur le disque dur de tous les ordinateurs dans un site Configuration Manager, vous pouvez créer une requête pour rechercher la classe **Disque logique** et l'attribut **Espace libre (Mo)** pour déterminer l'espace disque disponible.

Après avoir créé une requête initiale, vous pouvez spécifier d'autres critères. Par exemple, vous pouvez spécifier que les résultats de la requête incluent uniquement les ordinateurs affectés à un site spécifié. Vous pouvez aussi modifier l'affichage des résultats pour visualiser les résultats dans un ordre qui est significatif pour vous. Par exemple, vous pouvez spécifier que les résultats doivent être classés par quantité d'espace disponible sur les disques durs en ordre croissant ou décroissant.

Lorsque vous créez une requête, elle est stockée par Configuration Manager et affichée dans le nœud **Requêtes** de l'espace de travail **Surveillance**. Dans cet emplacement, vous pouvez créer une requête et exécuter, mettre à jour ou gérer une requête existante.

Vous pouvez également importer une requête dans une règle de requête dans un regroupement Configuration Manager. Pour plus d'informations, consultez Guide pratique pour créer des regroupements dans System Center Configuration Manager.

## Voir aussi

Informations techniques de référence sur les requêtes pour System Center Configuration Manager

# Opérations et maintenance pour les requêtes dans System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Consultez les rubriques de cette section pour en savoir plus sur les opérations et la maintenance en matière de requêtes dans System Center Configuration Manager.

## Dans cette section

- Guide pratique pour créer des requêtes dans System Center Configuration Manager
- Guide pratique pour gérer les requêtes dans System Center Configuration Manager

## Voir aussi

Informations techniques de référence sur les requêtes pour System Center Configuration Manager

# Guide pratique pour gérer les requêtes dans System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Aidez-vous des informations contenues dans cette rubrique pour gérer les requêtes dans System Center Configuration Manager.

Pour plus d'informations sur la création de requêtes, consultez Guide pratique pour créer des requêtes dans System Center Configuration Manager.

## Comment gérer les requêtes

Dans l'espace de travail **Surveillance** , sélectionnez successivement **Requêtes**, la requête à gérer et une tâche de gestion.

Utilisez le tableau suivant pour obtenir plus d'informations sur les tâches de gestion qui pourraient nécessiter certaines informations avant de les sélectionner.

| TÂCHE DE GESTION | DÉTAILS | PLUS D'INFORMATIONS |
|---|---|---|
| **Exécuter** | Exécute la requête sélectionnée et affiche les résultats dans la console Configuration Manager. | Aucune information supplémentaire. |
| **Installer le client** | Ouvre l'**Assistant Installation du client** qui permet d'installer le client Configuration Manager sur les ordinateurs retournés par la requête sélectionnée.<br><br>Cette option n'est pas disponible pour les requêtes qui retournent des appareils mobiles, des utilisateurs ou des groupes d'utilisateurs. | Pour plus d'informations sur la façon d'installer des clients Configuration Manager à l'aide de l'installation push du client, consultez Guide pratique pour déployer des clients sur des ordinateurs Windows. |
| **Exporterer** | Ouvre l' **Assistant Exportation d'objets** qui permet d'exporter la requête vers un fichier MOF (Managed Object Format) qui peut ensuite être importé sur un autre site. | Aucune information supplémentaire. |
| **Déplacer** | Ouvre la boîte de dialogue **Déplacer les éléments sélectionnés** où vous pouvez transférer la requête sélectionnée vers un dossier que vous avez créé précédemment sous le nœud **Requêtes** . | Aucune information supplémentaire. |

## Voir aussi

Opérations et maintenance pour les requêtes dans System Center Configuration Manager

# Comment créer des requêtes dans System Center Configuration Manager

22/06/2018 • 12 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez utiliser cette rubrique pour créer ou importer des requêtes dans System Center Configuration Manager.

## Comment créer des requêtes

Procédez comme suit pour créer des requêtes dans Configuration Manager.

**Pour créer une requête**

1. Dans la console Configuration Manager, choisissez **Surveillance**.
2. Dans l'espace de travail **Surveillance**, choisissez **Requêtes**. Puis, sous l'onglet **Accueil**, dans le groupe **Créer**, choisissez **Créer une requête**.
3. Sous l'onglet **Général** de l' **Assistant Création de requête**, spécifiez un nom unique et un commentaire facultatif pour la requête.
4. Si vous souhaitez importer une requête existante à utiliser comme base de la nouvelle requête, choisissez **importer la déclaration de requête**. Dans le **parcourir la requête** boîte de dialogue, sélectionnez une requête existante que vous souhaitez importer, puis choisissez **OK**.
5. Dans la liste **Type d'objet** , sélectionnez le type d'objet que vous voulez que la requête renvoie. Le tableau suivant décrit certains exemples du type d'objet que vous pouvez rechercher :

| TYPE D'OBJET | DESCRIPTION |
|---|---|
| **Ressource système** | Utilisé pour rechercher des attributs système standard tels que le nom NetBIOS d'un périphérique, la version du client, l'adresse IP du client et les informations des services de domaine Active Directory. |
| **Ressource utilisateur** | Utilisé pour rechercher des informations utilisateur standard, telles que des noms d'utilisateur, des noms de groupes d'utilisateurs et des noms de groupes de sécurité. |
| **Déploiement** | Utilisé pour rechercher les attributs standard d'un déploiement, tels que le nom du déploiement, la planification et le regroupement vers lequel il a été déployé. |

6. Choisissez **Modifier l'instruction de la requête** pour ouvrir la boîte de dialogue *Propriétés de l'instruction de* **<Nom de la requête>**.
7. Sous l'onglet **Général** de la boîte de dialogue **Propriétés de l'instruction de** *<Nom de la requête>*, spécifiez les attributs que cette requête renvoie et comment ils doivent être affichés. Choisissez l'icône **Nouveau** pour ajouter un nouvel attribut. Vous pouvez également choisir **Afficher la requête** pour entrer ou modifier la requête directement en langage de requêtes WMI (WQL). Pour obtenir des exemples

de requêtes WMI, consultez la section Exemples de requêtes WQL dans cette rubrique.

> **TIP**
> Vous pouvez utiliser la documentation de référence MSDN suivante pour vous aider à créer vos propres requêtes WQL :
>
> - WQL (SQL pour WMI)
> - Clause WHERE
> - Opérateurs WQL

8. Sous l'onglet **Critères** de la boîte de dialogue **Propriétés de l'instruction de** <*Nom de la requête*>, spécifiez les critères utilisés pour affiner les résultats de la requête. Par exemple, vous pouvez renvoyer uniquement les ressources dont le code de site est **XYZ** dans les résultats de la requête. Vous pouvez configurer plusieurs critères pour une requête.

   > **IMPORTANT**
   > Si vous créez une requête qui ne contient aucun critère, elle retourne tous les appareils du regroupement **Tous les systèmes** .

9. Sous l'onglet **Jointures** de la boîte de dialogue **Propriétés de l'instruction de** <*Nom de la requête*>, vous pouvez combiner des données de deux attributs différents dans les résultats de votre requête. Bien que Configuration Manager crée automatiquement des jointures de requête lorsque vous choisissez différents attributs pour les résultats de votre requête, l'onglet **Jointures** fournit d'autres options avancées. Les classes d'attributs prises en charge par System Center 2012 Configuration Manager sont indiquées dans le tableau ci-dessous :

   | TYPE DE JOINTURE | DESCRIPTION |
   |---|---|
   | Interne | Affiche uniquement les résultats ayant une correspondance ; ce type est toujours utilisé par les jointures qui sont créées automatiquement. |
   | Gauche | Affiche tous les résultats pour l'attribut de base et uniquement les résultats ayant une correspondance pour l'attribut de jointure. |
   | Droit | Affiche tous les résultats pour l'attribut de jointure et seulement les résultats ayant une correspondance pour l'attribut de base. |
   | Complète | Affiche tous les résultats à la fois pour l'attribut de base et pour l'attribut de jointure. |

   Pour plus d'informations sur la manière d'utiliser des opérations de jointure, consultez votre documentation SQL Server.

10. Choisissez **OK** pour fermer la boîte de dialogue **Propriétés de l'instruction de** <*Nom de la requête*>.

11. Sous l'onglet **Général** de l'**Assistant Création de requête**, spécifiez si les résultats de cette requête ne sont pas limités aux membres d'un regroupement, s'ils sont limités aux membres d'un regroupement spécifique ou s'ils affichent une invite pour choisir un regroupement à chaque exécution de la requête.

12. Terminez l'assistant pour créer la requête. La nouvelle requête s'affiche dans le nœud **Requêtes** de l'espace

de travail **Surveillance** .

## Comment importer des requêtes

Procédez comme suit pour importer une requête dans Configuration Manager. Pour plus d'informations sur l'exportation des requêtes, voir Guide pratique pour gérer des requêtes dans System Center Configuration Manager.

**Pour importer une requête**

1. Dans la console Configuration Manager, choisissez **Surveillance**.
2. Dans l'espace de travail **Surveillance**, choisissez **Requêtes**. Sous l'onglet **Accueil**, dans le groupe **Créer**, choisissez **Importer des objets**.
3. Dans la page **Nom du fichier MOF** de l'**Assistant Importation d'objets**, choisissez **Parcourir** pour sélectionner le fichier MOF (Managed Object Format) contenant la requête à importer.
4. Passez en revue les informations relatives à la requête à importer, puis terminez l'Assistant. La nouvelle requête s'affiche dans le nœud **Requêtes** de l'espace de travail **Surveillance**.

## Example WQL queries

Cette section contient des exemples de requêtes WMI que vous pouvez utiliser dans votre hiérarchie ou modifier à d'autres fins. Pour utiliser ces requêtes, choisissez **Afficher la requête** dans la boîte de dialogue **Propriétés de l'instruction de la requête**. Puis copiez et collez la requête dans le champ **Instruction de la requête**.

> **TIP**
> Utilisez le caractère générique `%` pour signifier n'importe quelle chaîne de caractères. Par exemple, `%Visio%` renvoie Microsoft Office Visio 2010.

### Ordinateurs qui exécutent Windows 7

Utilisez la requête suivante pour renvoyer le nom NetBIOS et la version du système d'exploitation de tous les ordinateurs qui exécutent Windows 7.

> **TIP**
> Pour retourner les ordinateurs qui exécutent Windows Server 2008 R2, remplacez `%Workstation 6.1%` par `%Server 6.1%` .

```
select SMS_R_System.NetbiosName,
SMS_R_System.OperatingSystemNameandVersion from
SMS_R_System where
SMS_R_System.OperatingSystemNameandVersion like "%Workstation 6.1%"
```

### Ordinateurs avec un package logiciel spécifique installé

Utilisez la requête suivante pour retourner le nom NetBIOS et le nom du package logiciel de tous les ordinateurs dotés d'un package logiciel spécifique installé. Cet exemple affiche tous les ordinateurs sur lesquels une version de Microsoft Visio est installée. Remplacez `%Visio%` par le package logiciel à rechercher.

**TIP**

Cette requête recherche le package logiciel en utilisant les noms figurant dans la liste des programmes inclus dans le Panneau de configuration Windows.

```
select SMS_R_System.NetbiosName,
SMS_G_System_ADD_REMOVE_PROGRAMS.DisplayName from
SMS_R_System inner join SMS_G_System_ADD_REMOVE_PROGRAMS on
SMS_G_System_ADD_REMOVE_PROGRAMS.ResourceId =
SMS_R_System.ResourceId where
SMS_G_System_ADD_REMOVE_PROGRAMS.DisplayName like "%Visio%"
```

### Ordinateurs situés dans une unité d'organisation (UO) des services de domaine Active Directory spécifique

Utilisez la requête suivante pour retourner le nom NetBIOS et le nom d'unité d'organisation (UO) de tous les ordinateurs inclus dans une unité d'organisation spécifiée. Remplacez le texte `OU Name` par le nom de l'UO à rechercher.

```
select SMS_R_System.NetbiosName,
SMS_R_System.SystemOUName from
SMS_R_System where
SMS_R_System.SystemOUName = "OU Name"
```

### Ordinateurs portant un nom NetBIOS spécifique

Utilisez la requête suivante pour retourner le nom NetBIOS de tous les ordinateurs dont le nom commence par une chaîne de caractères spécifique. Dans cet exemple, la requête retourne tous les ordinateurs dont le nom NetBIOS commence par `ABC`.

```
select SMS_R_System.NetbiosName from
SMS_R_System where SMS_R_System.NetbiosName like "ABC%"
```

### Appareils d'un type spécifique

Les types d'appareils sont stockés dans la base de données Configuration Manager sous la classe de ressource **sms_r_system** et le nom d'attribut **AgentEdition**. Utilisez la requête suivante pour récupérer uniquement les appareils correspondant à l'édition agent du type d'appareil que vous spécifiez :

```
Select SMS_R_System.ClientEdition from SMS_R_System where SMS_R_System.ClientEdition = <Device ID>
```

Utilisez l'une des valeurs suivantes pour *<ID d'appareil>* :

| TYPE D'APPAREIL | VALEUR DE AGENTEDITION |
|---|---|
| Ordinateur portable ou de bureau Windows | 0 |
| Appareil ARM Windows (exécutant Windows RT) | 1 |
| Windows Mobile 6.5 | 2 |
| Nokia Symbian | 3 |
| Windows Phone | 4 |

| TYPE D'APPAREIL | VALEUR DE AGENTEDITION |
|---|---|
| Ordinateur Mac | 5 |
| Windows CE | 6 |
| Windows Embedded | 7 |
| iOS | 8 |
| iPad | 9 |
| iPod Touch | 10 |
| Android | 11 |
| Système Intel sur une puce | 12 |
| Serveurs Unix et Linux | 13 |
| Apple macOS (MDM) | 14 |
| Microsoft HoloLens (MDM) | 15 |
| Microsoft Surface Hub (MDM) | 16 |
| Android for Work | 17 |

Par exemple, si vous voulez que la requête retourne uniquement des ordinateurs Mac, utilisez la requête suivante :

```
Select SMS_R_System.ClientEdition from SMS_R_System where SMS_R_System.ClientEdition = 5
```

## Voir aussi

Opérations et maintenance pour les requêtes dans System Center Configuration Manager

# Sécurité et confidentialité pour les requêtes dans System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Dans System Center Configuration Manager, les requêtes vous permettent de récupérer des informations à partir de la base de données du site selon les critères que vous spécifiez. Configuration Manager collecte les informations de base de données de site pendant le fonctionnement standard. Par exemple, en utilisant les informations qui ont été collectées à partir de découverte ou d'inventaire, vous pouvez configurer une requête pour identifier les périphériques qui répondent aux critères spécifiés.

Pour plus d'informations sur les requêtes, consultez Présentation des requêtes dans System Center Configuration Manager. Pour plus d'informations sur les bonnes pratiques en matière de sécurité et les informations de confidentialité pour les opérations Configuration Manager qui collectent les informations que vous pouvez récupérer à l'aide de requêtes, consultez Sécurité et confidentialité pour System Center Configuration Manager.

## Meilleures pratiques relatives à la sécurité pour les requêtes

Utilisez les meilleures pratiques de sécurité suivantes pour les requêtes.

| BONNES PRATIQUES DE SÉCURITÉ | PLUS D'INFORMATIONS |
|---|---|
| Lorsque vous exportez ou importez une requête qui est enregistrée dans un emplacement réseau, sécurisez l'emplacement et le canal de réseau. | Veillez à restreindre l'accès au dossier réseau.<br><br>Utilisez la signature SMB ou IPsec entre l'emplacement réseau et le serveur de site pour empêcher un intrus de falsifier les données de la requête avant leur importation. |

## Voir aussi

Informations techniques de référence sur les requêtes pour System Center Configuration Manager

# Rapports dans System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les rapports dans System Center Configuration Manager fournissent un ensemble d'outils et de ressources vous permettant d'utiliser les fonctions de rapport avancées de Microsoft SQL Server Reporting Services dans la console Configuration Manager.

## Rubriques relatives aux rapports

Les rubriques suivantes vous aident à gérer les rapports dans Configuration Manager :

- Présentation des rapports
- Planification de la création de rapports
- Configurer les rapports
- Opérations et maintenance pour les rapports
- Sécurité et confidentialité pour les rapports

# Présentation des rapports dans System Center Configuration Manager

22/06/2018 • 18 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Dans System Center Configuration Manager, les rapports fournissent un ensemble d'outils et de ressources vous permettant d'utiliser les fonctions de rapport avancées de SQL Server Reporting Services (SSRS), ainsi que les rapports détaillés du Générateur de rapports Reporting Services. La création de rapports vous permet de recueillir, d'organiser et de présenter des informations relatives aux utilisateurs, à l'inventaire logiciel et matériel, aux mises à jour logicielles, aux applications, à l'état du site et à d'autres opérations de Configuration Manager dans votre organisation. Les rapports vous permettent de disposer de nombreux rapports prédéfinis que vous pouvez utiliser comme tel ou adapter à vos besoins, et vous pouvez créer des rapports personnalisés. Utilisez les sections suivantes pour vous aider à gérer la création de rapports dans Configuration Manager.

## SQL Server Reporting Services

SQL Server Reporting Services offre une gamme complète d'outils et de services prêts à être utilisés pour créer, déployer et gérer des rapports pour votre organisation, ainsi que des fonctionnalités de programmation vous permettant d'étendre et de personnaliser la fonctionnalité de création de rapport. Reporting Services est une plate-forme de création de rapport basée sur un serveur qui fournit des fonctionnalités complètes de création de rapports pour une variété de sources de données.

Configuration Manager utilise SQL Server Reporting Services comme solution de création de rapports. L'intégration avec Reporting Services offre les avantages suivants :

- Utilise un système de création de rapports standard pour interroger la base de données Configuration Manager.
- Affiche les rapports à l'aide de la Visionneuse de rapports Configuration Manager ou du Gestionnaire de rapports, qui est une connexion web au rapport.
- Fournit une performance, une disponibilité et une évolutivité élevées.
- Fournit des abonnements pour les rapports auxquels les utilisateurs peuvent s'abonner. Par exemple, un directeur pourrait s'abonner à un envoi automatique par courrier électronique d'un rapport quotidien détaillant l'état du déploiement d'une mise à jour logicielle.
- Exporte les rapports que les utilisateurs peuvent sélectionner dans différents formats souvent utilisés.

  Pour plus d'informations sur Reporting Services, voir SQL Server Reporting Services dans la documentation en ligne de SQL Server 2008.

## Point Reporting Services

Le point de Reporting Services est un rôle de système de site installé sur un serveur qui exécute Microsoft SQL Server Reporting Services. Le point de Reporting Services copie les définitions de rapport Configuration Manager vers Reporting Services, crée des dossiers de rapports basés sur les catégories de rapports et paramètre les stratégies de sécurité des dossiers de rapports et des rapports en fonction des autorisations basées sur les rôles pour les utilisateurs administratifs de Configuration Manager. Toutes les 10 minutes, le point de Reporting Services se connecte à Reporting Services pour réappliquer la stratégie de sécurité si elle a été modifiée, par exemple, à l'aide du Gestionnaire de rapports. Pour plus d'informations sur la planification et

l'installation d'un point de Reporting Services, consultez la documentation suivante :

- Planification de la création de rapports dans System Center Configuration Manager
- Configuration des rapports dans System Center Configuration Manager

# Rapports de Configuration Manager

Configuration Manager offre des définitions de rapports pour plus de 400 rapports dans plus de 50 dossiers de rapports qui sont copiés dans le dossier de rapports racine dans SQL Server Reporting Services lors du processus d'installation du point de Reporting Services. Les rapports sont affichés sur la console Configuration Manager et sont organisés dans des sous-dossiers en fonction de la catégorie de rapport. Les rapports ne se propagent pas en amont ou en aval dans la hiérarchie Configuration Manager, mais s'exécutent uniquement par rapport à la base de données du site dans lequel ils sont créés. Toutefois, étant donné que Configuration Manager réplique les données globales dans toute la hiérarchie, vous avez accès aux informations de toute la hiérarchie. Lorsqu'un rapport récupère des données depuis la base de donnée d'un site, il a accès aux données du site lui-même ainsi qu'à celles des sites enfants, pour chaque site de la hiérarchie. Comme les autres objets Configuration Manager, un utilisateur administratif doit disposer des autorisations appropriées pour l'exécution ou la modification de rapports. Pour exécuter un rapport, un utilisateur administratif doit avoir l'autorisation **Exécuter le rapport** pour cet objet. Pour créer ou modifier un rapport, un utilisateur administratif doit avoir l'autorisation **Modifier le rapport** pour cet objet.

### Création et modification de rapports

Configuration Manager utilise le Générateur de rapports Microsoft SQL Server comme outil exclusif pour la création et l'édition des rapports basés sur des modèles ou sur SQL. Quand vous créez ou modifiez un rapport sur la console Configuration Manager, le Générateur de rapports s'ouvre. Pour plus d'informations sur la gestion des rapports, consultez Opérations et maintenance pour les rapports dans System Center Configuration Manager.

### Exécution des rapports

Quand vous exécutez un rapport depuis la console Configuration Manager, la Visionneuse de rapports s'ouvre et se connecte à Reporting Services. Une fois que vous avez spécifié les paramètres de rapport requis, Reporting Services récupère les données et affiche les résultats dans la visionneuse. Vous pouvez également vous connecter à SQL Services Reporting Services, à la source de données pour le site et exécuter des rapports.

### Invites de rapport

Dans Configuration Manager, une invite de rapport ou un paramètre de rapport est une propriété de rapport que vous pouvez configurer quand un rapport est créé ou modifié. Les invites de rapport sont créées dans le but de limiter ou de cibler les données extraites par un rapport. Un rapport peut contenir plusieurs invites, tant que celles-ci portent un nom unique et qu'elles contiennent uniquement des caractères alphanumériques conformes aux règles SQL Server pour les identificateurs.

Lorsque vous exécutez un rapport, l'invite appelle la valeur d'un paramètre requis et, en fonction de cette valeur, récupère les données du rapport. Par exemple, le rapport **Informations concernant un ordinateur spécifique** récupère les informations concernant un ordinateur spécifique et invite l'utilisateur administratif à entrer un nom d'ordinateur. Reporting Services transmet ensuite la valeur spécifiée à une variable définie dans l'instruction SQL du rapport.

### Liens de rapports

Dans Configuration Manager, les liens de rapports sont utilisés dans un rapport source pour permettre aux utilisateurs administratifs d'accéder facilement aux données supplémentaires, notamment les informations détaillées sur chaque élément contenu dans le rapport source. Si le rapport de destination nécessite l'exécution d'une ou de plusieurs invites d'exécution, le rapport source doit contenir une colonne avec les valeurs appropriées pour chaque invite. Vous devez spécifier le numéro de colonne qui fournit la valeur de l'invite. Par exemple, vous

pouvez lier un rapport qui répertorie les ordinateurs nouvellement découverts à un rapport contenant les derniers messages reçus sur un ordinateur spécifique. Lorsque le lien est créé, vous pouvez indiquer que la colonne 2 du rapport source contient les noms d'ordinateurs ; il s'agit d'une invite requise pour le rapport de destination. Lorsque le rapport source est exécuté, les icônes de lien s'affichent à gauche de chaque ligne de données. Lorsque vous cliquez sur l'icône d'une ligne, la Visionneuse de rapports transmet la valeur dans la colonne spécifiée de cette ligne comme valeur d'invite nécessaire pour afficher le rapport de destination. Un rapport peut être configuré avec un seul lien, et ce lien peut être connecté à une seule ressource de destination.

> **WARNING**
> Si vous déplacez un rapport de destination vers un dossier de rapport différent, l'emplacement du rapport de destination change. Le lien de rapport du rapport source n'est pas automatiquement mis à jour avec le nouvel emplacement et le lien de rapport ne fonctionnera pas dans le rapport source.

## Dossiers de rapports

Dans System Center Configuration Manager, les dossiers de rapports permettent de trier et de filtrer les rapports qui sont stockés dans Reporting Services. Les dossiers de rapport sont particulièrement utiles lorsque vous devez gérer plusieurs rapports. Lorsque vous installez un point de Reporting Services, les rapports sont copiés vers Reporting Services et organisés en plus de 50 dossiers de rapports. Les dossiers de rapports sont en lecture seule. Vous pouvez les modifier dans la console Configuration Manager.

## Abonnements aux rapports

Un abonnement aux rapports dans Reporting Services est une demande récurrente de la remise d'un rapport à un moment donné ou en réponse à un événement et dans un format d'application que vous spécifiez à l'inscription. Les abonnements représentent une alternative à l'exécution d'un rapport à la demande. Les rapports à la demande nécessitent la sélection active du rapport, à chaque fois que vous souhaitez le visualiser. En revanche, les abonnements peuvent être utilisés pour planifier, puis automatiser la remise d'un rapport.

Vous pouvez gérer les abonnements aux rapports dans la console Configuration Manager. Elles sont traitées sur le serveur de rapports. Les abonnements sont distribués à l'aide des extensions de remise qui sont déployées sur le serveur. Par défaut, vous pouvez créer des abonnements qui envoient des rapports à un dossier partagé ou à une adresse électronique. Pour plus d'informations sur la gestion des abonnements au rapport, consultez Opérations et maintenance pour les rapports dans System Center Configuration Manager.

## Générateur de rapports

Configuration Manager utilise le Générateur de rapports Microsoft SQL Server Reporting Services en tant qu'unique outil de création et de modification des rapports basés sur un modèle et des rapports basés sur SQL. Quand vous lancez l'action pour créer ou modifier un rapport dans la console Configuration Manager, le Générateur de rapports s'ouvre. Lorsque vous créez ou modifiez un rapport pour la première fois, le Générateur de rapports est installé automatiquement. La version du Générateur de rapports associée à la version installée de SQL Server s'ouvre quand vous exécutez ou modifiez des rapports.

L'installation du Générateur de rapports ajoute la prise en charge de plus de 20 langues. Lorsque vous exécutez le Générateur de rapports, il affiche les données dans la langue du système d'exploitation qui s'exécute sur l'ordinateur local. Si le Générateur de rapports ne supporte pas cette langue, les données sont affichées en anglais. Le Générateur de rapports prend en charge toutes les fonctionnalités de SQL Server 2008 Reporting Services, qui inclut les fonctionnalités suivantes :

- Il offre un environnement de création de rapports intuitif dont l'apparence est similaire à celle de Microsoft Office.

- Il offre une mise en page flexible du rapport de SQL Server 2008 Report Definition Language (RDL).
- Il fournit divers types d'affichage des données, dont des graphiques et des jauges.
- Il fournit des zones de texte enrichi.
- Il permet des exportations vers Microsoft Word.

  Vous pouvez également ouvrir le Générateur de rapports depuis SQL Server Reporting Services.

## Modèles de rapports dans SQL Server Reporting Services

Dans Configuration Manager, SQL Reporting Services utilise des modèles de rapport pour aider l'utilisateur administratif à sélectionner les éléments de la base de données à inclure dans les rapports basés sur un modèle. L'utilisateur administratif chargé de générer le rapport peut choisir entre les vues et éléments spécifiques exposés dans le modèle de rapport. Au moins un modèle de rapport doit être disponible pour pouvoir générer des rapports basés sur un modèle. Les modèles de rapport sont dotés des fonctions ci-après :

- Vous pouvez donner des noms plus pratiques aux champs des bases de données et aux vues pour faciliter la création de rapports. La connaissance de la structure de la base de données n'est pas nécessaire pour produire des rapports.
- Vous pouvez regrouper des éléments de façon logique.
- Vous pouvez définir des relations entre les éléments.
- Vous pouvez sécuriser les éléments du modèle de manière à ce que les utilisateurs administratifs ne puissent visualiser que les données auxquelles ils sont autorisés à accéder.

  Même si Configuration Manager fournit des exemples de modèles de rapport, vous pouvez également définir des modèles de rapport afin de répondre aux besoins de votre entreprise. Pour plus d'informations sur la création des modèles de rapport, consultez Création de modèles de rapport personnalisés pour System Center Configuration Manager dans SQL Server Reporting Services.

## Étapes suivantes

Planification de la création de rapports

# Planification de la création de rapports dans System Center Configuration Manager

22/06/2018 • 10 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

La création de rapports dans System Center Configuration Manager propose un ensemble d'outils et de ressources vous permettant d'utiliser les fonctionnalités de création de rapports avancées de SQL Server Reporting Services. Utilisez les sections suivantes pour vous aider à planifier la création de rapports dans Configuration Manager.

## Déterminer où installer le point de Reporting Services

Lorsque vous exécutez des rapports Configuration Manager sur un site, les rapports ont accès aux informations de la base de données de site à laquelle ils se connectent. Utilisez les sections suivantes pour vous aider à déterminer où installer le point de Reporting Services et quelle source de données utiliser.

> **NOTE**
> Pour plus d'informations sur la planification de systèmes de site dans Configuration Manager, consultez Ajouter des rôles système de site.

**Serveurs de système de site pris en charge**

Vous pouvez installer le point de Reporting Services sur un site d'administration centrale et sur des sites principaux, ainsi que sur plusieurs systèmes de site d'un ou plusieurs sites de la hiérarchie. Le point de Reporting Services n'est pas pris en charge sur les sites secondaires. Le premier point de Reporting Services sur un site est configuré comme le serveur de rapports par défaut. Vous pouvez ajouter plus de points de Reporting Services sur un site, mais le serveur de rapports par défaut sur chaque site est activement utilisé pour les rapports Configuration Manager. Vous pouvez installer le point de Reporting Services sur le serveur de site ou sur un système de site distant. Il est toutefois plus judicieux d'utiliser Reporting Services sur un serveur de système de site distant pour des raisons d'efficacité.

**Considérations relatives à la réplication des données**

Configuration Manager classe les données qu'il réplique en tant que données globales ou données de site. Les données globales font référence à des objets ayant été créés par des utilisateurs administratifs et qui sont répliquées sur tous les sites de la hiérarchie, alors que les sites secondaires ne reçoivent qu'un sous-ensemble de données globales. Les déploiements de logiciels, les mises à jour logicielles, les regroupements et les étendues de sécurité de l'administration basée sur des rôles sont des exemples de données globales. Les données de site font référence aux informations opérationnelles créées par les sites principaux Configuration Manager et les clients qui sont sous la hiérarchie de sites principaux. Les données de site sont répliquées vers le site d'administration centrale mais pas vers d'autres sites principaux. Les données d'inventaire matériel, les messages d'états, les alertes et les résultats de regroupements basés sur des requêtes sont des exemples de données de site. Les données de site ne sont visibles que sur le site d'administration centrale et sur le site principal dont les données sont originaires.

Prenez les facteurs suivants en compte pour vous aider à déterminer où installer vos points de Reporting Services :

- Un point de Reporting Services dont la base de données du site d'administration centrale est la source des

données des rapports doit avoir accès à toutes les données globales et les données de site de la hiérarchie Configuration Manager. Si vous avez besoin de rapports qui contiennent les données de site de plusieurs sites d'une hiérarchie, il peut être intéressant d'installer le point de Reporting Services sur un système de site, du site d'administration centrale et d'utiliser la base de donnée de ce site comme la source des données des rapports.

- Un point de Reporting Services dont la base de données du site principal enfant est la source des données des rapport ne doit avoir accès aux données globales et aux données de site que pour le site principal local et les sites secondaires enfants. Les données de site d'autres sites principaux de la hiérarchie Configuration Manager ne sont pas répliquées sur le site principal, et ainsi, Reporting Services n'y a pas accès. Si vous avez besoin de rapports qui contiennent des données de site d'un site principal spécifique ou des données globales, mais que vous ne souhaitez pas que l'utilisateur du rapport ait accès aux données de site d'autres sites principaux, installez un point de Reporting Services sur un système de site du site principal et utilisez la base de données du site principal comme source des données des rapports.

**Considérations relatives à la bande passante réseau**

Les serveurs de système de site du même site communiquent entre eux à l'aide du protocole SMB, HTTP ou HTTPS, selon la configuration du site. Comme ces communications ne sont pas gérées et qu'elles peuvent se produire à tout moment sans contrôle de la bande passante réseau, vérifiez la bande passante réseau disponible avant d'installer le rôle du point de Reporting Services sur un système de site.

> **NOTE**
> Pour plus d'informations sur la planification de systèmes de site, consultez Ajouter des rôles système de site.

## Planification de l'administration basée sur des rôles pour les rapports

La sécurité des rapports est très similaire à celles d'autres objets de Configuration Manager pour lesquels il est possible d'attribuer des rôles de sécurité et des autorisations à des utilisateurs administratifs. Les utilisateurs administratifs ne peuvent exécuter et modifier que les rapports pour lesquels ils disposent de droits de sécurité appropriés. Pour exécuter des rapports sur la console Configuration Manager, vous devez disposer d'un droit de **Lecture** pour les autorisations du **Site** et les autorisations configurées pour des objets spécifiques.

Cependant, contrairement à d'autres objets dans Configuration Manager, les droits de sécurité que vous avez définis pour les utilisateurs administratifs dans la console Configuration Manager doivent également être configurés dans Reporting Services. Quand vous configurez des droits de sécurité dans la console Configuration Manager, le point de Reporting Services se connecte à Reporting Services et définit les autorisations appropriées pour les rapports. Par exemple, le rôle de sécurité **Gestionnaire des mises à jour logicielles** est associé aux autorisations **Exécuter le rapport** et **Modifier le rapport** . Les utilisateurs administratifs qui ne disposent que du rôle **Gestionnaire des mises à jour logicielles** ne peuvent exécuter et modifier des rapports que pour les mises à jour logicielles. Les rapports d'autres objets ne sont pas affichés dans la console Configuration Manager. L'exception à ce principe est que certains rapports ne sont pas associés à des objets sécurisables Configuration Manager spécifiques. Pour ces rapports, l'utilisateur administratif doit disposer du droit **Lecture** pour que le **Site** puisse exécuter les rapports et du droit **Modifier** pour que le **Site** puisse modifier les rapports.

Les rapports sont entièrement activés pour l'administration basée sur les rôles. Les données de tous les rapports inclus dans Configuration Manager sont filtrées en fonction des autorisations de l'utilisateur administratif qui exécute le rapport. Les utilisateurs administratifs dotés de rôles spécifiques ne peuvent afficher que les informations définies pour leurs rôles.

Pour plus d'informations sur les droits de sécurité pour les rapports, consultez Configurer la création de rapports.

Pour plus d'informations sur l'administration basée sur des rôles dans Configuration Manager, consultez Configurer l'administration basée sur des rôles.

# Étapes suivantes

Utilisez les rubriques supplémentaires suivantes pour vous aider à planifier les rapports dans Configuration Manager :

- Prérequis de la création de rapports dans System Center Configuration Manager
- Bonnes pratiques pour la création de rapports dans System Center Configuration Manager

# Configuration requise pour la création de rapports dans System Center Configuration Manager

22/06/2018 • 3 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

La création de rapports dans System Center Configuration Manager comporte des dépendances externes et des dépendances au sein du produit.

## Dépendances externes à Configuration Manager

Le tableau suivant répertorie les dépendances externes pour la création de rapports.

| CONDITION PRÉALABLE | PLUS D'INFORMATIONS |
|---|---|
| SQL Server Reporting Services | Pour pouvoir utiliser des rapports dans Configuration Manager, vous devez installer et configurer SQL Server Reporting Services.<br><br>Pour plus d'informations sur la planification et le déploiement de Reporting Services dans votre environnement, reportez-vous à la section Reporting Services de la documentation en ligne de SQL Server 2008. |
| Dépendances de rôle de système de site pour les ordinateurs qui exécutent le point de Reporting Services. | Configurations prises en charge pour System Center Configuration Manager |

## Dépendances internes à Configuration Manager

Le tableau suivant répertorie les dépendances pour la création de rapports dans Configuration Manager.

| CONDITION PRÉALABLE | PLUS D'INFORMATIONS |
|---|---|
| Point de Reporting Services | Vous devez configurer le rôle système de site du point de Reporting Services pour pouvoir utiliser la création de rapports dans Configuration Manager. Pour plus d'informations sur l'installation et la configuration d'un point Reporting Services, consultez Configuration de la création de rapports dans Configuration Manager. |

## Versions de SQL Server prises en charge par le point de Reporting Services

La base de données Reporting Services peut être installée sur l'instance par défaut ou sur une instance nommée d'une installation 64 bits de SQL Server. L'instance SQL Server peut se trouver au même emplacement que le serveur du système de site ou sur un ordinateur distant.

Le tableau ci-dessous indique quelles versions de SQL Server sont prises en charge par le point de Reporting Services.

| VERSION SQL SERVER | POINT DE REPORTING SERVICES |
| --- | --- |
| SQL Server 2017 avec au minimum la mise à jour cumulative 2<br><br>- Standard<br>- Enterprise | Oui, à compter de Configuration Manager version 1710 |
| SQL Server 2016 avec SP1<br><br>- Standard<br>- Enterprise | Oui |
| SQL Server 2016<br><br>- Standard<br>- Enterprise | Oui |
| SQL Server 2014 avec SP2<br><br>- Standard<br>- Enterprise | Oui |
| SQL Server 2014 avec SP1<br><br>- Standard<br>- Enterprise | Oui |
| SQL Server 2012 avec SP4<br><br>- Standard<br>- Enterprise | Oui |
| SQL Server 2012 avec SP3<br><br>- Standard<br>- Enterprise | Oui |
| SQL Server 2008 R2 avec SP3<br><br>- Standard<br>- Enterprise<br>- Datacenter | Oui, pour les versions prises en charge de Configuration Manager antérieures à 1702. |
| SQL Server Express 2008 R2 with SP3 | Non pris en charge |

# Étapes suivantes

Opérations et maintenance pour les rapports

# Pratiques recommandées pour la création de rapports dans System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez les bonnes pratiques suivantes pour les rapports dans System Center Configuration Manager :

## Pour des performances optimales, installez le point de Reporting Services sur un serveur de système de site distant

Même si vous pouvez installer le point de Reporting Services sur le serveur de site ou sur un système de site distant, la performance est meilleure lorsque vous installez le point de Reporting Services sur un serveur de système de site distant.

## Optimiser les requêtes de SQL Server Reporting Services

En règle générale, les délais de création de rapports sont liés à la durée nécessaire à l'exécution des requêtes et à la récupération des résultats. Si vous utilisez Microsoft SQL Server, les outils tels que l'analyseur de requêtes et le générateur de profils peuvent vous aider à optimiser des requêtes.

## Planifier l'exécution du traitement des abonnements aux rapports en dehors des heures de bureau habituelles

Dès que possible, planifiez le traitement des abonnements aux rapports en dehors des heures de bureau habituelles pour minimiser le traitement par le processeur sur le serveur de base de données du site Configuration Manager. Cette pratique améliore également la disponibilité pour les demandes de rapport imprévues.

## Étapes suivantes

Configurer les rapports

# Liste des rapports dans System Center Configuration Manager

10/07/2018 • 128 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Configuration Manager fournit de nombreux rapports intégrés couvrant une grande partie des tâches de création de rapports que vous pourriez souhaiter effectuer. Vous pouvez également utiliser les instructions SQL dans ces rapports pour vous aider à rédiger vos propres rapports.

Les rapports suivants sont fournis avec Configuration Manager. Les rapports sont répartis dans différentes catégories.

## Sécurité administrative

Les six rapports suivants sont répertoriés sous la catégorie **Sécurité administrative**.

| NOM DU RAPPORT | DESCRIPTION |
|---|---|
| **Journal des activités d'administration** | Affiche un enregistrement des modifications administratives apportées aux utilisateurs administratifs, aux rôles de sécurité, aux étendues de sécurité et aux regroupements. |
| **Utilisateurs administratifs et affectations de sécurité** | Affiche les utilisateurs administratifs, leurs rôles de sécurité associés et les étendues de sécurité associées à chaque rôle de sécurité pour chaque utilisateur. |
| **Objets sécurisés par une seule étendue de sécurité** | Affiche les objets assignés par un administrateur à l'étendue de sécurité spécifiée uniquement. Ce rapport n'affiche pas les objets qui sont associés par un administrateur à plusieurs étendues de sécurité. |
| **Sécurité pour un ou plusieurs objets Configuration Manager** | Affiche les objets sécurisables, les étendues de sécurité associées aux objets et les utilisateurs administratifs qui ont des droits sur les objets. |
| **Récapitulatif des rôles de sécurité** | Affiche les rôles de sécurité et les administrateurs Configuration Manager associés à chaque rôle. |
| **Récapitulatif des étendues de sécurité** | Affiche les étendues de sécurité, les utilisateurs administratifs Configuration Manager et les groupes de sécurité associés à chaque étendue. |

## Alertes

Les deux rapports suivants sont répertoriés sous la catégorie **Alertes**.

| NOM DU RAPPORT | DESCRIPTION |
|---|---|
| **Tableau de bord des alertes** | Affiche la synthèse de toutes les alertes différées qui ont été générées entre les dates de début et de fin spécifiées. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Alertes générées le plus souvent** | Affiche la synthèse des alertes qui ont été générées le plus souvent depuis la date spécifiée jusqu'à ce jour pour le composant spécifié. |

## Asset Intelligence

Les 62 rapports suivants sont répertoriés sous la catégorie **Asset Intelligence**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Matériel 01A - Synthèse des ordinateurs d'un regroupement spécifique** | Affiche la vue de synthèse d'Asset Intelligence des ordinateurs inclus dans un regroupement que vous spécifiez. |
| **Matériel 03A - Utilisateurs d'ordinateurs principaux** | Affiche les utilisateurs et le nombre d'ordinateurs sur lesquels ils sont l'utilisateur principal. |
| **Matériel 03B - Ordinateurs d'un utilisateur de console principal spécifique** | Affiche tous les ordinateurs pour lesquels un utilisateur spécifié est l'utilisateur principal de la console. |
| **Matériel 04A - Ordinateurs avec plusieurs utilisateurs (partagés)** | Affiche les ordinateurs qui n'ont pas d'utilisateur principal car aucun utilisateur n'a un pourcentage de temps de connexion à la console supérieur à 66 %. |
| **Matériel 05A - Utilisateurs de la console sur un ordinateur spécifique** | Affiche tous les utilisateurs de la console sur un ordinateur spécifié. |
| **Matériel 06A - Ordinateurs pour lesquels aucun utilisateur de console n'a pu être déterminé** | Aide les utilisateurs administratifs à identifier les ordinateurs pour lesquels la journalisation de sécurité doit être activée. |
| **Matériel 07A - Périphériques USB par fabricant** | Affiche les périphériques USB, regroupés par fabricant. |
| **Matériel 07B - Périphériques USB par fabricant et description** | Affiche les périphériques USB, regroupés par fabricant et description. |
| **Matériel 07C - Ordinateurs munis d'un périphérique USB spécifique** | Affiche tous les ordinateurs munis d'un périphérique USB spécifié. |
| **Matériel 07D - Périphériques USB sur un ordinateur spécifique** | Affiche tous les périphériques USB sur un ordinateur spécifié. |
| **Matériel 08A - Matériel qui n'est pas prêt pour une mise à niveau logicielle** | Affiche le matériel qui ne satisfait pas à la configuration matérielle minimale requise. |
| **Matériel 09A - Recherche d'ordinateurs** | Affiche une synthèse des ordinateurs correspondant aux filtres de mots clés. Ces filtres sont le nom d'ordinateur, le site Configuration Manager, le domaine, l'utilisateur principal de la console, le système d'exploitation, le fabricant ou le modèle. |
| **Matériel 10A - Ordinateurs d'un regroupement spécifié qui ont été modifiés pendant un laps de temps spécifié** | Affiche la liste des ordinateurs inclus dans un regroupement spécifié où une classe de matériel a changé pendant une période spécifiée. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Matériel 10B - Modifications apportées à un ordinateur spécifié pendant un laps de temps spécifié** | Affiche les classes qui ont changé sur l'ordinateur spécifié pendant un laps de temps spécifié. |
| **Licence 01A - Grand livre des licences en volume Microsoft pour les relevés de licences Microsoft** | Affiche un inventaire de tous les logiciels Microsoft qui sont disponibles à partir du programme de licence en volume Microsoft. |
| **Licence 01B - Élément du Grand livre des licences en volume Microsoft par canal de vente** | Identifie et affiche le canal de vente des logiciels de licence en volume Microsoft inventoriés. |
| **Licence 01C - Ordinateurs possédant un élément du Grand livre des licences en volume Microsoft et canaux de vente** | Identifie et affiche les ordinateurs qui ont un élément spécifié du Grand livre des licences en volume Microsoft. |
| **Licence 01D - Produits du Grand livre des licences en volume Microsoft sur un ordinateur spécifique** | Identifie et affiche tous les éléments du Grand livre des licences en volume Microsoft sur un ordinateur spécifié. |
| **Licence 02A - Nombre de licences arrivant à expiration par périodes** | Affiche le nombre de licences arrivant à expiration pour une période spécifiée. Les produits affichés ont leur licence gérée par le service de gestion de licences des logiciels. |
| **Licence 02B - Ordinateurs dont les licences arrivent à expiration** | Affiche les ordinateurs dont les licences arrivent à expiration. |
| **Licence 02C - Informations de licence sur un ordinateur spécifique** | Affiche les produits sur un ordinateur spécifié dont les licences sont gérées par le service de gestion de licences des logiciels. |
| **Licence 03A - Nombre de licences par état de licence** | Affiche les produits, par état de licence, dont les licences sont gérées par le service de gestion de licences des logiciels. |
| **Licence 03B - Ordinateurs avec un état de licence spécifique** | Affiche les produits, avec un état de licence spécifié, dont les licences sont gérées par le service de gestion de licences des logiciels. |
| **Licence 04A - Nombre de produits gérés par le service de gestion de licences des logiciels** | Affiche le nombre de produits dont les licences sont gérées par le service de gestion de licences des logiciels. |
| **Licence 04B - Ordinateurs présentant un produit spécifique géré par le service de gestion des licences** | Affiche les ordinateurs, gérés par le service de gestion de licences des logiciels, qui contiennent un produit donné. |
| **Licence 05A - Ordinateurs agissant en tant que service de gestion de clés** | Affiche les ordinateurs qui agissent en tant que serveurs de gestion de clés. |
| **Licence 06A - Nombre de processeurs pour les produits avec une licence par processeur** | Affiche le nombre total de processeurs sur des ordinateurs qui utilisent des produits Microsoft prenant en charge la gestion des licences pour chaque processeur. |
| **Licence 06B - Ordinateurs équipés d'un produit spécifique prenant en charge la gestion des licences par processeur** | Affiche la liste des ordinateurs sur lesquels est installé un produit Microsoft spécifié qui prend en charge la gestion des licences par processeur. |
| **Licence 14A - Rapport de rapprochement des licences en volume Microsoft** | Affiche le rapprochement entre les licences logicielles achetées via le contrat de licence en volume Microsoft et le nombre réel de logiciels. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Licence 14B - Liste des logiciels Microsoft introuvables dans MVLS** | Ce rapport affiche les logiciels Microsoft en cours d'utilisation qui ne figurent pas dans le contrat de licence en volume Microsoft. |
| **Licence 15A - Rapport de rapprochement des licences générales** | Affiche le rapprochement entre les licences logicielles générales achetées et le nombre réel de logiciels. |
| **Licence 15B - Rapport de rapprochement des licences générales par ordinateur** | Affiche les ordinateurs qui ont installé le produit sous licence avec une version spécifiée. |
| **Logiciel 01A - Synthèse des logiciels installés dans un regroupement spécifique** | Affiche la synthèse des logiciels installés, classés par nombre d'instances, répertoriés dans l'inventaire. |
| **Logiciel 02A - Familles de produits pour un regroupement spécifique** | Affiche les familles de produits et le nombre de logiciels dans la famille pour un regroupement spécifié. |
| **Logiciel 02B - Catégories de produits pour une famille de produits spécifique** | Affiche les catégories de produits dans une famille de produits spécifiée et le nombre de logiciels au sein de la catégorie. |
| **Logiciel 02C - Logiciels dans une famille et une catégorie de produits spécifiques** | Affiche tous les logiciels qui se trouvent dans la famille et la catégorie de produits spécifiées. |
| **Logiciel 02D - Ordinateurs équipés de logiciels spécifiques** | Affiche tous les ordinateurs sur lesquels sont installés les logiciels spécifiés. |
| **Logiciel 02E - Logiciels installés sur un ordinateur spécifique** | Ce rapport affiche tous les logiciels installés sur un ordinateur spécifié. |
| **Logiciel 03A - Logiciels sans catégorie** | Affiche les logiciels dont la catégorie est inconnue ou qui n'ont aucune catégorie. |
| **Logiciel 04A - Logiciels configurés pour s'exécuter automatiquement sur les ordinateurs** | Affiche la liste des logiciels configurés pour s'exécuter automatiquement sur les ordinateurs. |
| **Logiciel 04B - Ordinateurs dotés de logiciels spécifiques configurés pour s'exécuter automatiquement** | Affiche tous les ordinateurs dotés de logiciels spécifiques configurés pour s'exécuter automatiquement |
| **Logiciel 04C - Logiciels configurés pour s'exécuter automatiquement sur un ordinateur spécifique** | Affiche les logiciels installés et configurés pour s'exécuter automatiquement sur un ordinateur spécifié. |
| **Logiciel 05A - Objets d'assistance du navigateur** | Affiche les objets d'assistance du navigateur installés sur les ordinateurs dans un regroupement spécifié. |
| **Logiciel 05B - Ordinateurs équipés d'un objet d'assistance du navigateur spécifique** | Affiche tous les ordinateurs équipés d'un objet d'assistance du navigateur spécifié. |
| **Logiciel 05C - Objets d'assistance du navigateur sur un ordinateur spécifique** | Affiche tous les objets d'assistance du navigateur sur l'ordinateur spécifié. |
| **Logiciel 06A - Recherche des logiciels installés** | Ce rapport fournit un récapitulatif des logiciels installés. La recherche est effectuée selon les critères suivants : nom du produit, éditeur ou version. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Logiciel 06B - Logiciels par nom de produit** | Affiche une synthèse des logiciels installés selon un nom de produit spécifié. |
| **Logiciel 07A - Programmes exécutables récemment utilisés par nombre d'ordinateurs** | Affiche les programmes exécutables que les utilisateurs ont récemment employés. Il inclut également le nombre d'ordinateurs sur lesquels le programme a été utilisé. Le contrôle de logiciel doit être activé pour que ce site affiche ce rapport. |
| **Logiciel 07B - Ordinateurs ayant récemment utilisé un programme exécutable spécifié** | Affiche les ordinateurs sur lesquels un programme exécutable spécifié a récemment été utilisé. Ce rapport exige que vous activiez le paramètre client de contrôle de logiciel. |
| **Logiciel 07C - Programmes exécutables récemment utilisés sur un ordinateur spécifié** | Affiche les fichiers exécutables qui ont été récemment utilisés sur un ordinateur spécifié. Ce rapport exige que vous activiez le paramètre client de contrôle de logiciel. |
| **Logiciel 08A - Programmes exécutables récemment utilisés par nombre d'utilisateurs** | Affiche les programmes exécutables que les utilisateurs ont récemment employés. Il inclut également un nombre d'utilisateurs qui les ont utilisés le plus récemment. Ce rapport exige que vous activiez le paramètre client de contrôle de logiciel. |
| **Logiciel 08B - Utilisateurs ayant récemment utilisé un programme exécutable spécifié** | Affiche les utilisateurs qui ont le plus récemment utilisé un programme exécutable spécifié. Ce rapport exige que vous activiez le paramètre client de contrôle de logiciel. |
| **Logiciel 08C - Programmes exécutables récemment utilisés par un utilisateur spécifié** | Affiche les programmes exécutables récemment utilisés par l'utilisateur spécifié. Ce rapport exige que vous activiez le paramètre client de contrôle de logiciel. |
| **Logiciel 09A - Logiciels rarement utilisés** | Affiche les noms des logiciels qui n'ont pas été utilisés pendant une certaine période. |
| **Logiciel 09B - Ordinateurs sur lesquels sont installés des logiciels rarement utilisés** | Affiche les ordinateurs sur lesquels sont installés des logiciels qui n'ont pas été utilisés pendant une certaine période. La période spécifiée se base sur la valeur spécifiée dans le rapport « Logiciel 09A - Logiciels rarement utilisés ». |
| **Logiciel 10A - Titres des logiciels avec plusieurs légendes personnalisées spécifiques définies** | Affiche les titres des logiciels selon leur correspondance à tous les critères de légende personnalisée spécifiés. Il est possible de sélectionner jusqu'à trois légendes personnalisées pour affiner une recherche de titre de logiciel. |
| **Logiciel 10B - Ordinateurs équipés d'un logiciel avec une légende personnalisée spécifique** | Affiche tous les ordinateurs d'un regroupement sur lesquels est installé un logiciel spécifique avec une légende personnalisée. |
| **Logiciel 11A - Titres des logiciels avec une légende personnalisée spécifique définie** | Affiche les titres des logiciels selon leur correspondance à au moins un des critères de légende personnalisée spécifiés. |
| **Software 12A - Titres des logiciels sans légende personnalisée** | Affiche tous les titres des logiciels qui n'ont pas de légende personnalisée définie. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Logiciel 14A - Recherche de logiciels dont la balise d'identification logicielle est activée** | Affiche le nombre de logiciels installés dont la balise d'identification logicielle est activée. |
| **Logiciel 14B - Ordinateurs sur lesquels sont installés des logiciels dont la balise d'identification logicielle est activée** | Affiche tous les ordinateurs sur lesquels sont installés des logiciels qui ont une balise d'identification logicielle spécifique activée. |
| **Logiciel 14C - Logiciels installés sur un ordinateur spécifique et dont la balise d'identification logicielle est activée** | Affiche tous les logiciels installés qui ont une balise d'identification logicielle spécifiée activée sur un ordinateur spécifié. |

# Installation Push du client

Les quatre rapports suivants sont répertoriés sous la catégorie **Push client**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Détails de l'état de l'installation Push du client** | Affiche des informations sur le processus d'installation Push du client pour tous les sites. |
| **Détails de l'état de l'installation Push du client pour un site spécifié** | Affiche des informations sur le processus d'installation Push du client pour un site spécifié. |
| **Synthèse de l'état de l'installation Push du client** | Affiche la synthèse de l'état de l'installation Push du client pour tous les sites. |
| **Synthèse de l'état de l'installation Push du client pour un site spécifié** | Affiche la synthèse de l'état de l'installation Push du client pour un site spécifié. |

# État du client

Les sept rapports suivants sont répertoriés sous la catégorie **État du client**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Détails des corrections du client** | Affiche les détails des actions de correction du client pour un regroupement que vous spécifiez. |
| **Synthèse des corrections du client** | Affiche la synthèse des actions de correction du client pour un regroupement spécifié. |
| **Historique de l'état du client** | Affiche l'historique de l'état général du client dans le site. |
| **Résumé de l'état du client** | Affiche les résultats de la vérification des clients actifs pour un regroupement donné. |
| **Temps client pour demande de stratégie** | Affiche le pourcentage de clients qui ont demandé une stratégie au moins une fois au cours des 30 derniers jours. Chaque jour représente un pourcentage du nombre total de clients qui ont demandé une stratégie depuis le premier jour du cycle. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Clients avec détails des clients sains ayant échoué** | Affiche des détails sur les clients pour lesquels la vérification de l'intégrité a échoué pour un regroupement spécifié. |
| **Détails des clients inactifs** | Affiche la liste détaillée des clients inactifs pour un regroupement donné. |

## Accès aux ressources d'entreprise

Les trois rapports suivants sont répertoriés sous la catégorie **Accès aux ressources de l'entreprise**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Historique d'émission des certificats** | Affiche l'historique des certificats émis par le point d'enregistrement de certificat pour les utilisateurs et appareils pendant la plage de dates spécifiée. |
| **Liste de biens par état d'émission de certificat** | Affiche les appareils ou utilisateurs qui sont dans un état d'émission de certificat spécifié à la suite de l'évaluation d'un profil de certificat spécifié. |
| **Liste de biens dont la date d'expiration des certificats approche** | Affiche les appareils ou utilisateurs qui ont des certificats qui expirent à la date spécifiée ou avant. |

## Gestion de la conformité et des paramètres

Les 22 rapports suivants sont répertoriés sous la catégorie **Gestion de la conformité et des paramètres**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Historique des compatibilités d'une ligne de base de configuration** | Affiche l'historique des modifications apportées aux compatibilités d'une ligne de base de configuration pendant la plage de dates spécifiée. |
| **Historique des compatibilités d'un élément de configuration** | Affiche l'historique des modifications apportées aux compatibilités d'un élément de configuration pendant la plage de dates spécifiée. |
| **Conformité de l'accès conditionnel pour l'utilisateur** | Affiche la conformité de l'accès conditionnel détaillée pour un utilisateur spécifique. |
| **Rapport de conformité de l'accès conditionnel** | Rapport de conformité de l'accès conditionnel pour chaque stratégie de conformité ciblée. |
| **Détails des règles de compatibilité des éléments de configuration dans la ligne de base de configuration d'un composant** | Affiche des informations sur les règles évaluées comme compatibles pour un élément de configuration spécifié pour un appareil ou un utilisateur spécifié. |
| **Détails des règles en conflit pour les éléments de configuration de la ligne de base de configuration d'un composant** | Affiche des informations sur les règles d'un élément de configuration déployé en conflit avec d'autres règles. Les autres règles peuvent être contenues dans le même élément de configuration déployé ou dans un autre. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Détails des erreurs des éléments de configuration dans la ligne de base de configuration d'un composant** | Affiche des informations sur les erreurs générées par un élément de configuration spécifié pour un utilisateur ou un périphérique spécifié. |
| **Détails des règles de non-compatibilité des éléments de configuration dans la ligne de base de configuration d'un composant** | Affiche des informations sur les règles évaluées comme non compatibles pour un élément de configuration spécifié, pour un périphérique ou un utilisateur spécifié. |
| **Détails des règles corrigées des éléments de configuration dans la ligne de base de configuration d'un composant** | Affiche des informations sur les règles corrigées par un élément de configuration spécifié pour un utilisateur ou un périphérique spécifié. |
| **Liste des composants par état de compatibilité d'une ligne de base de configuration** | Affiche les périphériques ou utilisateurs d'un état de compatibilité spécifié selon l'évaluation d'une ligne de base de configuration spécifié. |
| **Liste des composants par état de compatibilité pour un élément de configuration d'une ligne de base de configuration** | Affiche les périphériques ou utilisateurs d'un état de compatibilité spécifié selon l'évaluation d'un élément de configuration spécifié. |
| **Liste d'applications et de périphériques non conformes pour un utilisateur spécifié** | Affiche des informations sur les utilisateurs et les périphériques qui ont installé des applications non conformes avec une stratégie que vous avez spécifiée. |
| **Liste des règles en conflit avec la règle spécifique d'un composant** | Affiche une liste de règles qui sont en conflit avec une règle spécifiée pour un élément de configuration déployé. |
| **Liste des composants inconnus d'une ligne de base de configuration** | Affiche la liste des périphériques ou utilisateurs qui n'ont pas encore renvoyé de données de compatibilité pour une ligne de base de configuration spécifiée. |
| **Liste des composants inconnus d'un élément de configuration** | Affiche la liste des périphériques ou utilisateurs qui n'ont pas encore renvoyé de données de compatibilité pour un élément de configuration spécifié. |
| **Résumé des règles et des erreurs des éléments de configuration dans une ligne de base de configuration d'un composant** | Affiche une synthèse de l'état de compatibilité des règles et toutes les erreurs de réglage pour un élément de configuration spécifié. L'élément de configuration doit être déployé sur un appareil ou utilisateur. |
| **Résumé de conformité par ligne de base de configuration** | Affiche le résumé de la compatibilité générale des lignes de base de configuration déployées dans la hiérarchie. |
| **Résumé de compatibilité par élément de configuration pour une ligne de base de configuration** | Affiche le résumé de la compatibilité des éléments de configuration dans une ligne de base de configuration spécifiée. |
| **Résumé de la conformité par stratégies de configuration** | Affiche le résumé de la conformité des stratégies de configuration. |
| **Résumé de la compatibilité de la ligne de base de configuration d'un regroupement** | Affiche une synthèse de la compatibilité générale d'une base de référence de configuration spécifiée. L'élément de configuration doit être déployé sur le regroupement spécifié. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Résumé des utilisateurs ayant des applications non conformes** | Affiche des informations sur les utilisateurs qui ont installé des applications non conformes avec une stratégie que vous avez spécifiée. |
| **Acceptation des conditions générales** | Affiche les éléments des conditions générales et la version que chaque utilisateur a acceptés. |

## Gestion des appareils

Les 37 rapports suivants sont répertoriés sous la catégorie **Gestion des périphériques**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Tous les appareils mobiles de l'entreprise** | Affiche tous les appareils mobiles de l'entreprise. |
| **Tous les clients de périphériques mobiles** | Affiche des informations sur tous les clients d'appareils mobiles. Les appareils qui sont gérés par le connecteur Exchange Server ne sont pas inclus. |
| **Problèmes de certificat sur les périphériques mobiles gérés par le client Configuration Manager pour Windows CE et qui ne sont pas sains** | Affiche des informations détaillées sur les problèmes de certificat sur les appareils mobiles gérés par le client Configuration Manager pour Windows CE. |
| **Échecs de déploiement du client pour les périphériques mobiles gérés par le client Configuration Manager pour Windows CE** | Affiche des informations détaillées sur les échecs de déploiement pour les appareils mobiles gérés par le client Configuration Manager pour Windows CE. |
| **Détails sur l'état de déploiement du client pour les périphériques mobiles gérés par le client Configuration Manager pour Windows CE** | Affiche des informations sur l'état de déploiement pour les appareils mobiles gérés par le client Configuration Manager pour Windows CE. |
| **Déploiements réussis du client pour les périphériques mobiles gérés par le client Configuration Manager pour Windows CE** | Affiche des informations détaillées sur la réussite du déploiement pour les appareils mobiles gérés par le client Configuration Manager pour Windows CE. |
| **Problèmes de communication sur les périphériques mobiles gérés par le client Configuration Manager pour Windows CE et qui ne sont pas sains** | Ce rapport contient des informations détaillées sur les problèmes de communication sur les appareils mobiles gérés par le client Configuration Manager pour Windows CE. |
| **État de conformité de la stratégie de boîte aux lettres ActiveSync par défaut pour les appareils mobiles gérés par le connecteur du serveur Exchange Server** | Affiche une synthèse de l'état de compatibilité avec la stratégie de boîte aux lettres Exchange ActiveSync par défaut pour les appareils mobiles gérés par le connecteur du serveur Exchange Server. |
| **Nombre de périphériques mobiles par configurations d'affichage** | Ce rapport affiche le nombre d'appareils mobiles par paramètres d'affichage. |
| **Nombre de périphériques mobiles par système d'exploitation** | Affiche le nombre d'appareils mobiles par système d'exploitation. |
| **Nombre de périphériques mobiles par mémoire programme** | Affiche le nombre d'appareils mobiles par mémoire programme. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Nombre de périphériques mobiles par configurations de mémoire de stockage** | Nombre d'appareils mobiles par configurations de mémoire de stockage |
| **Informations d'intégrité détaillées pour les périphériques mobiles gérés par le client Configuration Manager pour Windows CE** | Affiche des informations d'intégrité détaillées pour les appareils mobiles gérés par le client Configuration Manager pour Windows CE. |
| **Récapitulatif de l'intégrité pour les périphériques mobiles gérés par le client Configuration Manager pour Windows CE** | Affiche des informations de synthèse de l'intégrité pour les appareils mobiles gérés par le client Configuration Manager pour Windows CE. |
| **Périphériques mobiles inactifs qui sont gérés par le connecteur du serveur Exchange Server** | Affiche les appareils mobiles qui sont gérés par le connecteur du serveur Exchange Server et qui ne se sont pas connectés à Exchange Server depuis un nombre de jours spécifié. |
| **Liste des appareils par état d'accès conditionnel** | Affiche des informations sur la conformité actuelle et sur l'état d'accès conditionnel des appareils. Vous pouvez utiliser ce rapport avec les stratégies d'accès conditionnel. Ce rapport est disponible depuis la version 1602 de Configuration Manager. |
| **Liste des appareils par état d'attestation d'intégrité** | Affiche une liste d'appareils avec des attributs signalés par le service d'attestation d'intégrité |
| **Liste des périphériques inscrits par utilisateur dans Windows Intune** | Affiche tous les appareils qu'un utilisateur a inscrits dans Microsoft Intune. |
| **Liste des appareils d'une catégorie spécifique** | Affiche des informations sur tous les appareils d'une catégorie spécifique. |
| **Problèmes de client local sur les périphériques mobiles gérés par le client Configuration Manager pour Windows CE et qui ne sont pas sains** | Ce rapport contient des informations détaillées sur les problèmes de client local sur les appareils mobiles gérés par le client Configuration Manager pour Windows CE. |
| **Informations sur le client de périphérique mobile** | Affiche des informations sur les appareils mobiles sur lesquels le client Gestionnaire de configuration est installé. Vous pouvez utiliser ce rapport pour vérifier quels appareils mobiles peuvent communiquer correctement avec un point de gestion. |
| **Détails de la compatibilité des périphériques mobiles pour le connecteur du serveur Exchange Server** | Affiche les détails de compatibilité de l'appareil mobile pour une stratégie de boîte aux lettres Exchange ActiveSync par défaut qui est configurée à l'aide du connecteur du serveur Exchange Server. |
| **Périphériques mobiles par système d'exploitation** | Affiche les appareils mobiles par système d'exploitation. |
| **Appareils mobiles jailbroken ou rootés** | Affiche les appareils mobiles qui sont jailbreakés ou rootés. |
| **Périphériques mobiles non gérés car inscrits mais non affectés à un site** | Affiche les appareils mobiles qui ont été inscrits dans Configuration Manager et qui possèdent un certificat, mais qui n'ont pas terminé l'attribution de site. |
| **Périphériques mobiles et quantité spécifique de mémoire programme libre** | Affiche tous les appareils mobiles ainsi que la quantité spécifiée de mémoire programme libre. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Périphériques mobiles avec une quantité spécifique de mémoire de stockage amovible libre** | Affiche tous les appareils mobiles ainsi que la quantité spécifiée de mémoire amovible libre. |
| **Périphériques mobiles rencontrant des problèmes de renouvellement de certificat** | Affiche les appareils mobiles inscrits qui n'ont pas réussi à renouveler leur certificat. Si vous ne renouvelez pas le certificat avant la période d'expiration, les appareils mobiles ne sont plus gérés. |
| **Périphériques mobiles avec une mémoire programme faible (inférieure à l'espace libre spécifié en Ko)** | Affiche les appareils mobiles pour lesquels la mémoire programme est inférieure à une taille spécifiée en Ko. |
| **Périphériques mobiles avec une mémoire de stockage amovible faible (inférieure à l'espace libre spécifié en Ko)** | Affiche les appareils mobiles pour lesquels la mémoire de stockage amovible est inférieure à une taille spécifiée en Ko. |
| **Nombre d'appareils inscrits par utilisateur dans Microsoft Intune** | Affiche les utilisateurs activés pour l'abonnement Microsoft Intune. Il indique également le nombre total d'appareils inscrits pour chaque utilisateur. |
| **Demandes de mise hors service et de réinitialisation en attente pour les appareils mobiles** | Affiche les demandes de nettoyage en attente pour des appareils mobiles. |
| **Périphériques mobiles récemment inscrits et affectés** | Ce rapport affiche les appareils mobiles récemment inscrits dans Configuration Manager et affectés avec succès à un site. |
| **Périphériques mobiles récemment nettoyés** | Affiche la liste des appareils mobiles récemment nettoyés avec succès. |
| **Synthèse des paramètres pour les périphériques mobiles gérés par le connecteur du serveur Exchange Server** | Affiche le nombre d'appareils mobiles appliquant les paramètres pour chaque stratégie de boîte aux lettres Exchange ActiveSync par défaut gérée par le connecteur du serveur Exchange Server. |
| **État détaillé de clés de chargement de version test Windows RT** | Affiche des informations d'état détaillées pour une clé de chargement de version test Windows RT spécifiée. |
| **Résumé des clés de chargement de version test Windows RT** | Affiche l'état des clés de chargement de version test Windows RT. |

## Gestion des pilotes

Les 13 rapports suivants sont répertoriés sous la catégorie **Gestion des pilotes**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Tous les pilotes** | Affiche la liste de tous les pilotes. |
| **Tous les pilotes pour une plateforme spécifique** | Affiche tous les pilotes pour une plateforme spécifiée. |
| **Tous les pilotes d'une image de démarrage spécifique** | Affiche tous les pilotes d'une image de démarrage spécifiée. |
| **Tous les pilotes d'une catégorie spécifique** | Affiche tous les pilotes d'une catégorie spécifiée. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Tous les pilotes d'un package spécifique** | Affiche tous les pilotes d'un package spécifié. |
| **Catégories d'un pilote spécifique** | Affiche les catégories d'un pilote spécifié. |
| **Ordinateurs qui n'ont pas pu installer des pilotes pour un regroupement spécifique** | Affiche les ordinateurs qui n'ont pas pu installer des pilotes pour un regroupement spécifique. |
| **Rapport de correspondance du catalogue de pilotes pour un regroupement spécifique** | Affiche le rapport de correspondance du catalogue de pilotes pour un regroupement spécifié. |
| **Rapport de correspondance du catalogue de pilotes pour un ordinateur spécifique** | Affiche le rapport de correspondance du catalogue de pilotes pour un ordinateur spécifié. |
| **Rapport de correspondance du catalogue de pilotes pour un périphérique spécifique sur un ordinateur spécifique** | Affiche le rapport de correspondance du catalogue de pilotes pour un périphérique spécifique sur un ordinateur spécifique. |
| **Rapport de correspondance du catalogue de pilotes pour les ordinateurs d'un regroupement spécifique avec un périphérique spécifique** | Affiche le rapport de correspondance du catalogue de pilotes pour les ordinateurs d'un regroupement spécifique avec un périphérique spécifique. |
| **Pilotes dont l'installation a échoué sur un ordinateur spécifique** | Affiche les pilotes dont l'installation a échoué sur un ordinateur spécifique. |
| **Plateformes prises en charge pour un pilote spécifique** | Affiche les plateformes prises en charge pour un pilote spécifié. |

## Endpoint Protection

Les six rapports suivants sont répertoriés sous la catégorie **Endpoint Protection**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Rapport d'activité des logiciels anti-programme malveillant** | Affiche une vue d'ensemble de l'activité des logiciels anti-programme malveillant. |
| **Historique et état global du logiciel anti-programme malveillant** | Affiche l'historique et l'état global du logiciel anti-programme malveillant. |
| **Détails des programmes malveillants de l'ordinateur** | Affiche les détails relatifs à un ordinateur spécifié ainsi que la liste des programmes malveillants détectés sur cet ordinateur. |
| **Ordinateurs infectés** | Affiche la liste des ordinateurs sur lesquels une menace spécifiée a été détectée. |
| **Utilisateurs récurrents par menace** | Affiche la liste des utilisateurs qui ont le plus grand nombre de menaces détectées. |
| **Liste des menaces utilisateur** | Affiche la liste des menaces trouvées pour un compte d'utilisateur spécifique. |

## Matériel - CD-ROM

Les quatre rapports suivants sont répertoriés sous la catégorie **Matériel - CD-ROM**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Informations de CD-ROM pour un ordinateur spécifique** | Affiche des informations sur les lecteurs de CD-ROM d'un ordinateur spécifié. |
| **Ordinateurs disposant d'un CD-ROM d'un fabricant spécifique** | Affiche la liste des ordinateurs qui contiennent un lecteur de CD-ROM conçu par un fabricant que vous spécifiez. |
| **Compter les lecteurs de CD-ROM par fabricant** | Affiche le nombre de lecteurs de CD-ROM inventoriés par fabricant. |
| **Historique - Historique CD-ROM pour un ordinateur spécifique** | Affiche l'historique de l'inventaire des lecteurs de CD-ROM sur un ordinateur spécifié. |

# Matériel - Disque

Les huit rapports suivants sont répertoriés sous la catégorie **Matériel - disque**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Ordinateurs avec un disque dur d'une taille spécifique** | Affiche la liste des ordinateurs dont les disques durs sont de la taille spécifiée. |
| **Ordinateurs avec un espace disque libre faible (inférieur au pourcentage libre spécifié)** | Affiche la liste des ordinateurs inclus dans un regroupement spécifié dont l'espace disque libre est inférieur à celui spécifié. |
| **Ordinateurs avec un espace disque libre faible (inférieur au nombre de Mo libre spécifié)** | Affiche la liste des ordinateurs dont l'espace disque est faible. La quantité d'espace libre à rechercher est spécifiée en Mo. |
| **Compter les configurations de disque physique** | Affiche le nombre de disques durs inventoriés par capacité du disque. |
| **Informations de disques concernant un ordinateur spécifique - Disques logiques** | Affiche des informations de synthèse sur les disques logiques d'un ordinateur spécifié. |
| **Informations de disques concernant un ordinateur spécifique - Partitions** | Affiche des informations de synthèse sur les partitions de disques d'un ordinateur spécifié. |
| **Informations de disques concernant un ordinateur spécifique - Disques physiques** | Affiche des informations de synthèse sur les disques physiques d'un ordinateur spécifié. |
| **Historique - Historique de l'espace disque logique pour un ordinateur spécifique** | Affiche l'historique de l'inventaire des lecteurs de disques logiques sur un ordinateur spécifié. |

# Matériel – Général

Les cinq rapports suivants sont répertoriés sous la catégorie **Matériel - Général**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Informations concernant un ordinateur spécifique** | Affiche des informations de synthèse pour un ordinateur spécifié. |

| NOM DU RAPPORT | DESCRIPTION |
|---|---|
| **Ordinateurs dans un groupe de travail ou un domaine spécifique** | Affiche la liste des ordinateurs inclus dans un groupe de travail ou un domaine spécifié. |
| **Classes d'inventaire affectées à un regroupement spécifique** | Affiche les classes d'inventaire affectées à un regroupement spécifié. |
| **Classes d'inventaire activées sur un ordinateur spécifique** | Affiche les classes d'inventaire activées sur un ordinateur spécifié. |
| **Informations d'appareil Windows AutoPilot** | Affiche les informations de l'appareil client nécessaires pour l'inscription Windows AutoPilot. |

## Matériel - Mémoire

Les cinq rapports suivants sont répertoriés sous la catégorie **Matériel - Mémoire**.

| NOM DU RAPPORT | DESCRIPTION |
|---|---|
| **Ordinateurs sur lesquels la mémoire physique a changé** | Affiche la liste des ordinateurs dont la quantité de mémoire vive a changé depuis le dernier cycle d'inventaire. |
| **Ordinateurs disposant d'une quantité de mémoire spécifique** | Affiche la liste des ordinateurs disposant d'une quantité spécifiée de mémoire vive (mémoire physique totale arrondie au mégaoctet le plus proche). |
| **Ordinateurs avec peu de mémoire vive (inférieure ou égale à la quantité de Mo spécifiée)** | Affiche la liste des ordinateurs disposant de peu de mémoire. La quantité de mémoire à rechercher est spécifiée en Mo. |
| **Compter les configurations de mémoire** | Affiche le nombre d'ordinateurs inventoriés par quantité de mémoire vive. |
| **Informations de mémoire pour un ordinateur spécifique** | Affiche des informations de synthèse sur la mémoire d'un ordinateur spécifié. |

## Matériel - Modem

Les trois rapports suivants sont répertoriés sous la catégorie **Matériel - Modem**.

| NOM DU RAPPORT | DESCRIPTION |
|---|---|
| **Ordinateurs disposant d'un modem d'un fabricant spécifique** | Affiche la liste des ordinateurs qui disposent d'un modem conçu par un fabricant spécifique. |
| **Compter les modems par fabricant** | Affiche le nombre de modems inventoriés pour chaque fabricant. |
| **Informations de modem pour un ordinateur spécifique** | Affiche des informations de synthèse sur le modem d'un ordinateur spécifié. |

## Matériel - Carte réseau

Les rapports suivants sont répertoriés sous la catégorie **Matériel - Carte réseau**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Ordinateurs équipés d'une carte réseau spécifique** | Affiche la liste des ordinateurs dotés d'une carte réseau spécifiée. |
| **Compter les cartes réseau par type** | Affiche le nombre de cartes réseau inventoriées par type. |
| **Informations de carte réseau pour un ordinateur spécifique** | Affiche des informations sur les cartes réseau installées sur un ordinateur spécifié. |

## Matériel - Processeur

Les cinq rapports suivants sont répertoriés sous la catégorie **Matériel - Processeur**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Ordinateurs ayant une fréquence de processeur spécifique** | Affiche la liste des ordinateurs dont un processeur est cadencé à la fréquence spécifiée. |
| **Ordinateurs équipés de processeurs rapides (d'une fréquence supérieure ou égale à la fréquence spécifiée)** | Affiche la liste des ordinateurs dotés de processeurs dont la fréquence est plus rapide que la fréquence spécifiée. |
| **Ordinateurs équipés de processeurs lents (d'une fréquence inférieure ou égale à la fréquence spécifiée)** | Affiche la liste des ordinateurs dotés de processeurs cadencés à une fréquence inférieure ou égale à la fréquence d'horloge spécifiée. |
| **Compter les vitesses de processeur** | Affiche le nombre d'ordinateurs inventoriés par fréquence de processeur. |
| **Informations de processeur pour un ordinateur spécifique** | Affiche des informations sur les processeurs installés sur un ordinateur spécifié. |

## Matériel - SCSI

Les cinq rapports suivants sont répertoriés sous la catégorie **Matériel - SCSI**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Ordinateurs équipés d'un type de carte SCSI spécifique** | Affiche la liste des ordinateurs sur lesquels une carte SCSI spécifiée est installée. |
| **Compter les types de contrôleurs SCSI** | Affiche le nombre de contrôleurs SCSI inventoriés par type de carte. |
| **Informations de cartes SCSI pour un ordinateur spécifique** | Affiche des informations sur les cartes SCSI installées sur un ordinateur spécifié. |

## Matériel - Sécurité

Le rapport suivant est répertoriés sous la catégorie **Matériel - Sécurité**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Détails des états du microprogramme sur les appareils** | Affiche les détails des états de l'UEFI, de SecureBoot et du TPM |

## Matériel - Carte audio

Les trois rapports suivants sont répertoriés sous la catégorie **Matériel - SCSI**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Ordinateurs équipés d'une carte son spécifique** | Affiche la liste des ordinateurs dotés d'une carte son spécifiée. |
| **Compter les cartes audio** | Affiche le nombre d'ordinateurs inventoriés par type de carte audio. |
| **Informations de cartes son pour un ordinateur spécifique** | Affiche des informations de synthèse sur les cartes son d'un ordinateur spécifié. |

## Matériel – Carte vidéo

Les trois rapports suivants sont répertoriés sous la catégorie **Matériel - Carte vidéo**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Ordinateurs équipés d'une carte vidéo spécifique** | Affiche la liste des ordinateurs dotés d'une carte vidéo spécifiée. |
| **Compter les cartes vidéo par type** | Affiche une liste de toutes les cartes vidéo installées sur les ordinateurs. Il montre également le nombre de chaque type de carte vidéo. |
| **Informations de cartes graphiques pour un ordinateur spécifique** | Affiche des informations de synthèse sur les cartes vidéo installées sur un ordinateur spécifié. |

## Migration

Les cinq rapports suivants sont répertoriés sous la catégorie **Migration**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Clients dans la liste des exclusions** | Affiche les clients exclus de la migration. |
| **Dépendance sur un regroupement Configuration Manager** | Affiche les objets qui dépendent d'un regroupement de la hiérarchie source. |
| **Propriétés de la tâche de migration** | Ce rapport affiche le contenu de la tâche de migration spécifiée. |
| **Tâches de migration** | Ce rapport affiche la liste des tâches de migration. |
| **Objets en échec de migration** | Affiche la liste des objets qui n'a pas pu migrer pendant la dernière tentative. |

# Réseau

Les six rapports suivants sont répertoriés sous la catégorie **Réseau**.

| NOM DU RAPPORT | DESCRIPTION |
|---|---|
| **Compter les adresses IP par sous-réseau** | Affiche le nombre d'adresses IP inventoriées pour chaque sous-réseau IP. |
| **IP - Tous les sous-réseaux par masque de sous-réseau** | Affiche la liste des sous-réseaux IP et des masques de sous-réseau. |
| **IP - Ordinateurs dans un sous-réseau spécifique** | Affiche la liste des ordinateurs et des informations IP pour un sous-réseau IP spécifié. |
| **IP - Informations pour un ordinateur spécifique** | Affiche des informations de synthèse sur le protocole Internet d'un ordinateur spécifié. |
| **IP - Informations pour une adresse IP spécifique** | Affiche des informations de synthèse sur une adresse IP spécifiée. |
| **MAC - Ordinateurs pour une adresse MAC spécifique** | Affiche le nom et l'adresse IP des ordinateurs dont l'adresse MAC est celle spécifiée. |

# Système d'exploitation

Les 10 rapports suivants sont répertoriés sous la catégorie **Système d'exploitation**.

| NOM DU RAPPORT | DESCRIPTION |
|---|---|
| **Historique des versions du système d'exploitation de l'ordinateur** | Affiche l'historique de l'inventaire du système d'exploitation sur un ordinateur spécifié. |
| **Ordinateurs équipés d'un système d'exploitation spécifique** | Affiche les ordinateurs équipés d'un système d'exploitation spécifié. |
| **Ordinateurs équipés d'un système d'exploitation et d'un Service Pack spécifiques** | Affiche les ordinateurs équipés d'un système d'exploitation et d'un Service Pack spécifiés. |
| **Nombre de versions du système d'exploitation** | Affiche le nombre d'ordinateurs inventoriés par système d'exploitation. |
| **Compter les systèmes d'exploitation et les Service Packs** | Affiche le nombre d'ordinateurs inventoriés par combinaison de système d'exploitation et de Service Pack. |
| **Services - Ordinateurs exécutant un service spécifique** | Affiche la liste des ordinateurs qui exécutent un service spécifié. |
| **Services - Ordinateurs exécutant le service d'accès à distance** | Affiche la liste des ordinateurs qui exécutent le serveur d'accès à distance. |
| **Services - Informations de services concernant un ordinateur spécifique** | Affiche des informations de synthèse sur les services d'un ordinateur spécifié. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Détails de la maintenance de Windows 10 pour un regroupement spécifique** | Affiche des informations générales sur la maintenance de Windows 10 pour un regroupement spécifique. |
| **Ordinateurs Windows Server** | Affiche la liste des ordinateurs qui exécutent des systèmes d'exploitation Windows Server. |

## Gestion de l'alimentation

Les 18 rapports suivants sont répertoriés sous la catégorie **Gestion de l'alimentation**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Gestion de l'alimentation - Activité de l'ordinateur** | Affiche un graphique illustrant l'activité du moniteur, de l'ordinateur et de l'utilisateur pour un regroupement spécifique au cours d'une période donnée. |
| **Gestion de l'alimentation - Activité par ordinateur** | Affiche un graphique illustrant l'activité du moniteur, de l'ordinateur et de l'utilisateur pour un ordinateur spécifié à une date spécifiée. |
| **Gestion de l'alimentation - Détails de l'activité de l'ordinateur** | Affiche la liste des fonctions de veille et de sortie de veille pour les ordinateurs d'un regroupement spécifié à une heure et une date données. |
| **Gestion de l'alimentation - Détails de l'ordinateur** | Affiche des informations détaillées sur les fonctions de gestion de l'alimentation, les paramètres d'alimentation et les modes de gestion de l'alimentation appliqués à un ordinateur spécifié. |
| **Gestion de l'alimentation - Pas de rapport détaillé pour l'ordinateur** | Affiche la liste des ordinateurs ne rendant compte d'aucune activité d'alimentation pour une heure et une date données. |
| **Gestion de l'alimentation – Ordinateurs exclus** | Affiche la liste des ordinateurs exclus du mode de gestion de l'alimentation. |
| **Gestion de l'alimentation - Ordinateurs avec plusieurs modes de gestion de l'alimentation** | Affiche la liste des ordinateurs auxquels plusieurs paramètres d'alimentation en conflit sont appliqués. |
| **Gestion de l'alimentation - Consommation énergétique** | Affiche la consommation énergétique mensuelle totale (en kWh) pour un regroupement donné sur une période de temps précise. |
| **Gestion de l'alimentation - Consommation énergétique journalière** | Affiche la consommation énergétique totale (en kWh) au cours des 31 derniers jours pour un regroupement donné. |
| **Gestion de l'alimentation - Coût énergétique** | Affiche le coût de la consommation énergétique mensuelle totale pour un regroupement donné sur une période de temps précise. |
| **Gestion de l'alimentation - Coût énergétique journalier** | Affiche le coût énergétique total pour un regroupement donné au cours des 31 derniers jours. |
| **Gestion de l'alimentation - Incidence sur l'environnement** | Affiche un graphique montrant les émissions de dioxyde de carbone (CO2) générées par un regroupement spécifié sur une période de temps précise. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Gestion de l'alimentation - Incidence journalière sur l'environnement** | Affiche un graphique montrant les émissions de CO2 générées par un regroupement spécifié au cours des 31 derniers jours. |
| **Gestion de l'alimentation - Détails de l'ordinateur non mis en veille** | Affiche des informations détaillées sur les ordinateurs qui ne se sont pas mis en veille ou veille prolongée sur une période donnée. |
| **Gestion de l'alimentation - Rapport sur la non-mise en veille** | Affiche une liste de causes courantes empêchant les ordinateurs de se mettre en veille ou veille prolongée. Il indique également le nombre d'ordinateurs affectés par chaque cause sur une période donnée. |
| **Gestion de l'alimentation - Fonctions de gestion de l'alimentation** | Affiche les fonctions de gestion de l'alimentation des ordinateurs inclus dans le regroupement spécifié. |
| **Gestion de l'alimentation - Paramètres du mode de gestion de l'alimentation** | Affiche la liste globale des paramètres d'alimentation utilisés par les ordinateurs d'un regroupement spécifié. |
| **Gestion de l'alimentation - Détails des paramètres du mode de gestion de l'alimentation** | Permet d'afficher d'autres informations sur les ordinateurs qui ont été spécifiés dans le rapport **Gestion de l'alimentation – Paramètres du mode de gestion de l'alimentation**. |

## Trafic de réplication

Les 10 rapports suivants sont répertoriés sous la catégorie **Trafic de réplication**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Trafic global de réplication des données par lien (courbes)** | Affiche le trafic total global de réplication des données sur un lien spécifié pendant un nombre de jours spécifiés. |
| **Trafic global de réplication des données par lien (secteurs)** | Affiche le trafic total global de réplication des données sur un lien spécifié pendant un nombre de jours spécifiés. |
| **Trafic de réplication par hiérarchie en fonction du lien** | Affiche le trafic de réplication total pour chaque lien de la hiérarchie pendant un nombre de jours spécifié. |
| **Trafic par lien des dix principaux groupes de réplication par hiérarchie (secteurs)** | Affiche le trafic de réplication pour les 10 principaux groupes de réplication sur la totalité de la hiérarchie identifiée par un lien. |
| **Trafic de réplication des liens** | Affiche la totalité du trafic de réplication pour toutes les données pendant un nombre de jours spécifié. |
| **Trafic du groupe de réplication par lien** | Affiche le trafic réseau du groupe de réplication via un lien spécifié de réplication de bases de données pendant un nombre de jours spécifié. |
| **Trafic de réplication de données de site par lien (courbes)** | Affiche le trafic total de réplication de données de site sur un lien spécifié pendant un nombre de jours spécifié. |
| **Trafic de réplication de données de site par lien (secteurs)** | Affiche le trafic total de réplication de données de site sur un lien spécifié pendant un nombre de jours spécifié. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Total du trafic de réplication par hiérarchie (courbes)** | Affiche la réplication de données globales et de site consolidées par hiérarchie pour chaque direction de chaque lien pendant un nombre de jours spécifié. |
| **Total du trafic de réplication par hiérarchie (secteurs)** | Affiche la réplication de données globales et de site consolidées par hiérarchie pour chaque direction de chaque lien pendant un nombre de jours spécifié. |

## Site - Informations client

Les 19 rapports suivants sont répertoriés sous la catégorie **Site - Informations client**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Rapport détaillé d'état d'attribution des clients** | Affiche des informations détaillées sur l'état d'attribution des clients. |
| **Détails sur l'échec de l'attribution des clients** | Affiche des informations détaillées sur les échecs d'attribution de clients. |
| **Détails de l'état d'attribution des clients** | Affiche des informations générales sur l'état d'attribution des clients. |
| **Détails sur la réussite de l'attribution des clients** | Affiche des informations détaillées sur les clients dont l'attribution a réussi. |
| **Rapport d'échec du déploiement des clients** | Affiche des informations détaillées sur les clients dont le déploiement a échoué. |
| **Détails de l'état du déploiement des clients** | Affiche des informations de synthèse sur l'état des installations des clients. |
| **Rapport de réussite du déploiement des clients** | Affiche des informations détaillées sur les clients dont le déploiement a réussi. |
| **Clients non compatibles avec une communication HTTPS** | Affiche des informations détaillées sur chaque client exécutant l'outil HTTPS Communication Readiness et signalé comme étant dans l'impossibilité de communiquer via HTTPS. |
| **Ordinateurs attribués mais non installés pour un site précis** | Affiche une liste d'ordinateurs attribués à un site précis, mais qui ne rendent pas compte à ce site. |
| **Ordinateurs avec une version spécifique du client Configuration Manager** | Affiche une liste d'ordinateurs exécutant une version spécifique du logiciel client Configuration Manager. |
| **Nombre de clients et protocole utilisé pour la communication** | Affiche le résumé des méthodes de communication utilisées par les clients (HTTP ou HTTPS). |
| **Nombre de clients affectés et installés pour chaque site** | Affiche le nombre d'ordinateurs attribués et installés pour chaque site. Les clients possédant un emplacement réseau associé à plusieurs sites ne sont considérés comme installés que s'ils sont sous la supervision de ce site. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Nombre de clients compatibles avec une communication HTTPS** | Affiche des informations détaillées sur chaque client exécutant l'outil HTTPS Communication Readiness et signalé comme étant en mesure ou non de communiquer via HTTPS. |
| **Nombre de clients pour chaque site** | Affiche le nombre de clients de Configuration Manager installés par code de site. |
| **Nombre de clients de Configuration Manager par versions de client** | Affiche le nombre d'ordinateurs découverts par la version de client Configuration Manager. |
| **Détail des problèmes signalés jusqu'au point d'état de secours pour un regroupement spécifié** | Affiche des informations détaillées pour les problèmes signalés par les clients dans un regroupement spécifié. Un point d'état de secours doit avoir été attribué à ces clients. |
| **Détails des problèmes signalés jusqu'au point d'état de secours pour un site spécifié** | Affiche des informations détaillées sur les problèmes signalés par les clients dans un site spécifié. Un point d'état de secours doit avoir été attribué à ces clients. |
| **Récapitulatif des problèmes signalés jusqu'au point d'état de secours** | Affiche des informations sur tous les problèmes signalés par les clients. Un point d'état de secours doit avoir été attribué à ces clients. |
| **Récapitulatif des problèmes signalés jusqu'au point d'état de secours pour un regroupement spécifique** | Affiche des informations de synthèse pour les problèmes signalés par les clients dans un regroupement spécifié. Un point d'état de secours doit avoir été attribué à ces clients. |

## Site - Informations de découverte et d'inventaire

Les 10 rapports suivants sont répertoriés sous la catégorie **Site - Informations de découverte et d'inventaire**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Clients qui n'ont pas émis de rapports récemment (pendant le nombre de jours spécifié)** | Affiche la liste des clients qui n'ont pas signalé de données de découverte, d'inventaire matériel ou d'inventaire logiciel pendant un nombre de jours spécifié. |
| **Ordinateurs découverts par un site spécifique** | Affiche une liste de tous les ordinateurs découverts par le site spécifié. Il montre également la date de la dernière découverte. |
| **Ordinateurs récemment découverts par une méthode de découverte** | Affiche une liste des ordinateurs découverts par le site pendant le nombre de jours spécifié. Il répertorie également les agents qui les ont découverts. Un même ordinateur peut apparaître plusieurs fois dans la liste s'il a été découvert par plusieurs agents. |
| **Ordinateurs non découverts récemment (dans un nombre de jours spécifié)** | Affiche une liste des ordinateurs qui n'ont pas été découverts récemment par le site. Il indique également le nombre de jours depuis leur découverte. |
| **Ordinateurs non inventoriés récemment (dans un nombre de jours spécifié)** | Affiche une liste des ordinateurs qui n'ont pas été inventoriés récemment par le site. Il indique également les dates des derniers inventaires des ordinateurs par le client. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Ordinateurs susceptibles de partager le même identifiant Configuration Manager unique** | Affiche la liste des ordinateurs qui ont modifié leur nom. Un changement de nom est un symptôme possible d'un ordinateur qui partage un identificateur unique Configuration Manager avec un autre ordinateur. |
| **Ordinateurs ayant des adresses MAC en double** | Affiche les ordinateurs qui partagent une adresse MAC. |
| **Compter les ordinateurs dans les domaines de ressources ou groupes de travail** | Affiche le nombre d'ordinateurs dans chaque domaine de ressources ou groupe de travail. |
| **Informations de découverte pour un ordinateur spécifique** | Affiche la liste des agents et des sites qui ont découvert un ordinateur spécifié. |
| **Dates d'inventaire pour un ordinateur spécifique** | Affiche la date et l'heure de la dernière exécution de l'inventaire sur un ordinateur spécifié. |

## Site - Général

Les trois rapports suivants sont répertoriés sous la catégorie **Site - Général**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Ordinateurs dans un site spécifique** | Affiche la liste des ordinateurs clients dans un site spécifié. |
| **État du site pour la hiérarchie** | Affiche la liste des sites de la hiérarchie avec leur version et leurs informations d'état. |
| **État de la mise à jour Configuration Manager au sein de la hiérarchie** | Affiche des informations sur les mises à jour de sites Configuration Manager pour la hiérarchie. |

## Site - Informations sur le serveur

Le rapport suivant est répertorié sous la catégorie **Site - Informations sur le serveur**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Rôles de système de site et serveurs de système de site pour un site spécifique** | Affiche la liste des serveurs et rôles de système de site pour un site spécifié. |

## Logiciel - Sociétés et produits

Les 15 rapports suivants sont répertoriés sous la catégorie **Logiciel - Sociétés et produits**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Tous les produits inventoriés pour un éditeur de logiciels spécifique** | Affiche la liste des produits logiciels inventoriés et de leurs versions pour un éditeur de logiciels spécifié. |
| **Tous les éditeurs de logiciels** | Affiche la liste de toutes les entreprises qui éditent les logiciels inventoriés. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Toutes les applications Windows** | Affiche une synthèse des applications Windows installées. La recherche est effectuée selon les critères suivants : nom de l'application, architecture ou éditeur. |
| **Ordinateurs sur lesquels existe un produit spécifique** | Affiche la liste des ordinateurs sur lesquels un produit spécifié est inventorié, ainsi que les versions de ce produit. |
| **Ordinateurs sur lesquels existe un produit et une version spécifiques** | Affiche la liste des ordinateurs sur lesquels une version spécifiée d'un produit est inventoriée. |
| **Ordinateurs équipés d'un logiciel spécifique inscrit dans Ajout/Suppression de programmes** | Affiche le résumé de tous les ordinateurs équipés d'un logiciel spécifié inscrit dans Ajout/Suppression de programmes ou Programmes et fonctionnalités. |
| **Nombre de tous les produits et versions inventoriés** | Affiche la liste des produits logiciels et versions inventoriés, ainsi que le nombre d'ordinateurs sur lesquels chacun est installé. |
| **Compter les produits et versions inventoriés pour un produit spécifique** | Affiche la liste des versions inventoriées d'un produit spécifié, ainsi que le nombre d'ordinateurs sur lesquels chacune est installée. |
| **Décompte de toutes les instances de logiciels inscrits avec Ajout/Suppression de programmes** | Affiche le résumé de toutes les instances de logiciels installées et inscrites avec Ajout/Suppression de programmes ou Programmes et fonctionnalités sur des ordinateurs au sein du regroupement spécifié. |
| **Décompte des instances d'un logiciel spécifique inscrit avec Ajout/Suppression de programmes** | Affiche le nombre d'instances des packages logiciels spécifiés installés et inscrits dans Ajout/Suppression de programmes ou Programmes et fonctionnalités. |
| **Nombre de navigateurs par défaut** | Affiche le nombre de clients ayant spécifié un certain navigateur web par défaut sous Windows.<br>Utilisez la référence suivante pour les valeurs BrowserProgID courantes :<br>- AppXq0fevzme2pys62n3e0fbqa7peapykr8v : Microsoft Edge<br>- IE.HTTP : Microsoft Internet Explorer<br>- ChromeHTML : Google Chrome<br>- OperaStable : Opera Software<br>- FirefoxURL-308046B0AF4A39CB : Mozilla Firefox<br>- Inconnu : le système d'exploitation client ne prend pas en charge la requête, la requête n'a pas été exécutée ou un utilisateur ne s'est pas connecté |
| **Installations des applications Windows spécifiées** | Ce rapport répertorie tous les ordinateurs dotés d'une application Windows spécifiée. |
| **Produits sur un ordinateur spécifique** | Affiche le résumé des produits logiciels inventoriés et de leurs fabricants sur un ordinateur spécifié. |
| **Logiciels inscrits dans Ajout/Suppression de programmes sur un ordinateur spécifique** | Affiche le résumé des logiciels installés sur un ordinateur spécifié et inscrits dans Ajout/Suppression de programmes ou Programmes et fonctionnalités. |
| **Applications Windows installées pour l'utilisateur spécifié** | Affiche toutes les applications Windows installées pour l'utilisateur spécifié |

# Fichiers logiciels

Les rapports suivants sont répertoriés sous la catégorie **Fichiers logiciels**.

| NOM DU RAPPORT | DESCRIPTION |
|---|---|
| **Tous les fichiers inventoriés pour un produit spécifique** | Affiche le résumé des fichiers inventoriés qui sont associés à un produit logiciel spécifié. |
| **Tous les fichiers inventoriés sur un ordinateur spécifique** | Affiche le résumé de tous les fichiers inventoriés sur un ordinateur spécifié. |
| **Comparer l'inventaire logiciel de deux ordinateurs** | Affiche les différences entre les inventaires logiciels signalés pour deux ordinateurs spécifiés. |
| **Ordinateurs sur lesquels existe un fichier spécifique** | Affiche la liste des ordinateurs qui ont collecté un inventaire logiciel pour un nom de fichier spécifié. Si un ordinateur comporte plusieurs copies du fichier, il peut apparaître plusieurs fois dans la liste. |
| **Compter les ordinateurs avec un nom de fichier spécifique** | Affiche le nombre d'ordinateurs qui ont collecté un inventaire logiciel pour un fichier spécifié. |

# Distribution de logiciels - Surveillance des applications

Les 10 rapports suivants sont répertoriés sous la catégorie **Distribution de logiciels - Surveillance des applications**.

| NOM DU RAPPORT | DESCRIPTION |
|---|---|
| **Tous les déploiements d'applications (avancé)** | Affiche des informations de synthèse approfondies pour tous les déploiements d'applications. |
| **Tous les déploiements d'applications (standard)** | Affiche des informations de synthèse pour tous les déploiements d'applications. |
| **Compatibilité de l'application** | Affiche des informations de compatibilité pour l'application spécifiée au sein du regroupement spécifié. |
| **Déploiements de l'application par bien** | Affiche les applications déployées sur un appareil ou utilisateur spécifié. |
| **Erreurs d'infrastructure de l'application** | Affiche les erreurs d'infrastructure de l'application. Celles-ci peuvent inclure des erreurs d'infrastructure internes ou des erreurs résultant de règles de configuration requise non valides. |
| **État détaillé de l'utilisation de l'application** | Affiche des détails sur l'utilisation des applications installées. |
| **État récapitulatif de l'utilisation de l'application** | Affiche le résumé de l'utilisation des applications installées. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Applications iOS dont le déploiement a échoué (application déjà installée)** | Affiche les informations de conformité pour l'application iOS sélectionnée. Vous avez déployé cette application en tant que « Package d'application pour iOS depuis App Store » que vous avez aussi associée à une stratégie de gestion des applications mobiles. Ce rapport est utilisé pour afficher les utilisateurs et les appareils pour lesquels l'application n'a pas pu être installée, car elle avait déjà été installée manuellement par l'utilisateur. |
| **Déploiements de séquences de tâches contenant l'application** | Affiche les déploiements de séquences de tâches qui installent une application spécifiée. |
| **Demandes d'utilisateur pour une application Android** | Affiche les utilisateurs qui ont demandé à installer une application Android. |

## Distribution de logiciels - Regroupements

Les trois rapports suivants sont répertoriés sous la catégorie **Distribution de logiciels - Regroupements**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Tous les regroupements** | Affiche tous les regroupements inclus dans la hiérarchie. |
| **Toutes les ressources dans un regroupement spécifique** | Affiche toutes les ressources dans un regroupement spécifié. |
| **Fenêtres de maintenance disponibles pour un client spécifié** | Affiche toutes les fenêtres de maintenance applicables au client spécifié. |

## Distribution de logiciels - Contenu

Les 16 rapports suivants sont répertoriés sous la catégorie **Distribution de logiciels - Contenu**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Toutes les distributions de contenus actifs** | Affiche tous les points de distribution sur lesquels du contenu est en cours d'installation ou de suppression. |
| **Tout le contenu** | Affiche toutes les applications et packages d'un site. |
| **Tous les contenus dans un point de distribution spécifique** | Affiche tout le contenu actuellement installé sur un point de distribution spécifié. |
| **Tous les points de distribution** | Affiche des informations sur les points de distribution de chaque site. |
| **Tous les messages d'état pour un package spécifique sur un point de distribution spécifique** | Affiche tous les messages d'état pour un package spécifié sur un point de distribution spécifié. |
| **État de distribution du contenu de l'application** | Affiche des informations sur l'état de distribution du contenu de l'application. |
| **Applications ciblées pour le groupe de points de distribution** | Affiche des informations sur le contenu de l'application qui a été déployé sur un groupe de points de distribution spécifié. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Applications qui ne sont pas synchronisées dans un groupe de points de distribution spécifié** | Affiche les applications pour lesquelles des fichiers de contenu associés n'ont pas été mis à jour avec la version la plus récente sur un groupe de points de distribution spécifié. |
| **Groupe de points de distribution** | Affiche des informations sur un groupe de points de distribution spécifié. |
| **Résumé de l'utilisation des points de distribution** | Affiche le résumé de l'utilisation de chaque point de distribution. |
| **État de distribution d'un package donné** | Affiche l'état de distribution du contenu du package spécifié sur chaque point de distribution. |
| **Packages ciblés pour le groupe de points de distribution** | Affiche des informations sur les packages qui ciblent un groupe de points de distribution spécifié. |
| **Packages non synchronisés sur un groupe de points de distribution spécifié** | Affiche les packages pour lesquels des fichiers de contenu associés n'ont pas été mis à jour avec la version la plus récente sur un groupe de points de distribution spécifié. |
| **Rejet du contenu par une source de cache d'homologue** | Affiche le nombre de rejets par une source de cache d'homologue par groupe de limites. |
| **Rejet du contenu par une source de cache d'homologue par condition** | Affiche les sources de cache d'homologue ayant rejeté la diffusion de contenu en fonction d'une condition. |
| **Détails du rejet du contenu par une source de cache d'homologue** | Affiche le nom du contenu rejeté par une source d'homologue. |

## Distribution de logiciels - Déploiement du package et du programme

Les cinq rapports suivants sont répertoriés sous la catégorie **Distribution de logiciels - Déploiement du package et du programme**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Tous les déploiements d'un package et d'un programme donnés** | Affiche des informations sur tous les déploiements d'un package et d'un programme spécifiés. |
| **Tous les déploiements de packages et de programmes** | Affiche tous les déploiements de packages et de programmes sur ce site. |
| **Tous les déploiements de packages et de programmes dans un regroupement donné** | Affiche tous les déploiements de packages et de programmes dans un regroupement spécifié. |
| **Tous les déploiements de packages et de programmes sur un ordinateur donné** | Affiche tous les déploiements de packages et de programmes qui s'appliquent à un ordinateur spécifié. |
| **Tous les déploiements de programmes et de packages vers un utilisateur spécifique** | Affiche tous les déploiements de packages et de programmes vers un utilisateur spécifié. |

## Distribution de logiciels - État du déploiement du package et du

## programme

Les cinq rapports suivants sont répertoriés sous la catégorie **Distribution de logiciels - État du déploiement du package et du programme**.

| NOM DU RAPPORT | DESCRIPTION |
|---|---|
| **Tous les déploiements de packages et de programmes de ressources système avec leur état** | Affiche tous les déploiements de packages et de programmes pour le site avec l'état récapitulatif de chaque déploiement. |
| **Toutes les ressources système pour un déploiement de packages et de programmes spécifié dans un état spécifié** | Affiche la liste des ressources qui sont dans un état spécifié pour un déploiement de packages et de programmes spécifié. |
| **Graphique - État d'avancement du déploiement de packages et de programmes chaque heure** | Affiche le pourcentage d'ordinateurs ayant installé avec succès le package. La liste classe toutes les heures depuis la création du déploiement de packages et de programmes par un administrateur. Ce pourcentage sert à suivre le temps moyen nécessaire au déploiement de packages et de programmes. |
| **État du déploiement de packages et de programmes pour un client et un déploiement donnés** | Affiche les messages d'état signalés pour un ordinateur et un déploiement de packages et de programmes spécifiés. |
| **État du déploiement d'un package et d'un programme spécifiques** | Affiche la synthèse d'état d'un déploiement de packages et de programmes spécifié. |

# Contrôle de logiciel

Les 13 rapports suivants sont répertoriés sous la catégorie **Contrôle de logiciel**.

| NOM DU RAPPORT | DESCRIPTION |
|---|---|
| **Toutes les règles de contrôle de logiciel appliquées à ce site** | Affiche la liste de toutes les règles de contrôle de logiciel au niveau du site. |
| **Ordinateurs disposant d'un programme contrôlé mais qui ne l'ont pas encore exécuté depuis une date donnée** | Affiche tous les ordinateurs avec l'application contrôlée spécifiée, mais aucun utilisateur n'a exécuté ce programme depuis la date spécifiée. |
| **Ordinateurs ayant exécuté un programme contrôlé spécifique** | Affiche la liste des ordinateurs qui ont exécuté des programmes correspondant à la règle de contrôle de logiciel spécifiée pendant le mois et l'année spécifiés. |
| **Utilisation simultanée de tous les programmes contrôlés** | Affiche le nombre maximal d'utilisateurs qui ont exécuté simultanément chaque logiciel contrôlé pendant le mois et l'année spécifiés. |
| **Analyse de la tendance d'utilisation simultanée d'un programme contrôlé spécifique** | Affiche le nombre maximal d'utilisateurs qui ont exécuté simultanément le logiciel contrôlé spécifié au cours de chaque mois de l'année précédente. |
| **Base d'installation pour tous les logiciels contrôlés** | Affiche le nombre d'ordinateurs qui ont des logiciels contrôlés installés, comme indiqué par l'inventaire logiciel. Ce rapport nécessite que l'ordinateur collecte l'inventaire logiciel. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Progression du résumé du contrôle de logiciel** | Affiche l'heure à laquelle les données de contrôle synthétisées les plus récentes ont été traitées sur le serveur de site. Les rapports de contrôle de logiciel reflètent uniquement les données de contrôle traitées avant ces dates. |
| **Résumé de l'utilisation dans la journée pour un programme de logiciel contrôlé spécifique** | Affiche le nombre moyen d'utilisations d'un programme particulier au cours des 90 derniers jours, par heure et par jour. |
| **Utilisation simultanée de tous les programmes de logiciels contrôlés** | Affiche le nombre d'utilisateurs qui ont exécuté des programmes correspondant à chaque règle de contrôle de logiciel pendant le mois et l'année spécifiés. Ces règles concernent les logiciels installés localement ou l'utilisation des services Terminal Server. |
| **Utilisation totale de tous les logiciels contrôlés sur les serveurs Windows Terminal Server** | Affiche le nombre d'utilisateurs qui ont exécuté des programmes correspondant à chaque règle de contrôle de logiciel à l'aide des services Terminal Server pendant le mois et l'année spécifiés. |
| **Analyse de la tendance d'utilisation totale pour un programme contrôlé spécifique** | Affiche le nombre d'utilisateurs qui ont exécuté des programmes correspondant à la règle de contrôle de logiciel spécifiée pendant chaque mois de l'année précédente. Ces règles concernent les logiciels installés localement ou l'utilisation des services Terminal Server. |
| **Analyse de la tendance d'utilisation totale pour un logiciel contrôlé spécifique sur les serveurs Windows Terminal Server** | Affiche le nombre d'utilisateurs qui ont exécuté des programmes correspondant à la règle de contrôle de logiciel spécifiée pendant chaque mois de l'année précédente. Ces règles concernent l'utilisation des services Terminal Server. |
| **Utilisateurs ayant exécuté un programme contrôlé spécifique** | Affiche une liste d'utilisateurs qui ont exécuté des programmes correspondant à la règle de contrôle de logiciel spécifiée pendant le mois et l'année spécifiés. |

## Mises à jour logicielles - Compatibilité A

Les huit rapports suivants sont répertoriés sous la catégorie **Mises à jour logicielles - Compatibilité A**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Compatibilité 1 - Compatibilité globale** | Affiche les données de compatibilité globale d'un groupe de mises à jour logicielles. |
| **Conformité 2 - Mise à jour logicielle spécifique** | Affiche les données de compatibilité d'une mise à jour logicielle spécifiée. |
| **Compatibilité 3 - Groupe de mises à jour (par mise à jour)** | Affiche les données de compatibilité des mises à jour logicielles définies dans un groupe de mises à jour logicielles. |
| **Compatibilité 4 - Mises à jour par fabricant-mois-année** | Affiche les données de compatibilité des mises à jour logicielles publiées par un fournisseur pendant un mois et une année spécifiés. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Compatibilité 5 - Ordinateur spécifique** | Ce rapport renvoie les données de compatibilité des mises à jour logicielles pour un ordinateur spécifié. Pour limiter la quantité d'informations renvoyées, vous pouvez spécifier le fournisseur et la classification des mises à jour logicielles. |
| **Compatibilité 6 - États de mises à jour logicielles spécifiques (secondaire)** | Affiche le nombre et le pourcentage d'ordinateurs dans chaque état de compatibilité pour la mise à jour logicielle spécifiée. |
| **Compatibilité 7 - Ordinateurs dans un état de compatibilité spécifique pour un groupe de mises à jour (secondaire)** | Affiche tous les ordinateurs d'un regroupement qui sont dans un état de compatibilité globale spécifié par rapport à un groupe de mises à jour logicielles. |
| **Compatibilité 8 - Ordinateurs dans un état de compatibilité spécifique pour une mise à jour (secondaire)** | Affiche tous les ordinateurs d'un regroupement qui sont dans un état de compatibilité spécifié pour une mise à jour logicielle. |

## Mises à jour logicielles - Gestion du déploiement B

Les huit rapports suivants sont répertoriés sous la catégorie **Mises à jour logicielles - Gestion du déploiement B**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Gestion 1 - Déploiements d'un groupe de mises à jour** | Affiche tous les déploiements qui contiennent toutes les mises à jour logicielles définies dans un groupe de mises à jour logicielles spécifié. |
| **Gestion 2 - Mises à jour requises mais non déployées** | Affiche toutes les mises à jour logicielles propres à un fournisseur qui ont été détectées comme obligatoires par les clients, mais qui n'ont pas été déployées sur un regroupement spécifié par un administrateur. |
| **Gestion 3 - Mises à jour dans un déploiement** | Affiche les mises à jour logicielles contenues dans un déploiement spécifié. |
| **Gestion 4 - Déploiements ciblant un regroupement** | Affiche tous les déploiements de mises à jour logicielles qui ciblent un regroupement spécifié. |
| **Gestion 5 - Déploiements ciblant un ordinateur** | Affiche tous les déploiements de mises à jour logicielles sur un ordinateur spécifié. |
| **Gestion 6 - Déploiements contenant une mise à jour spécifique** | Affiche tous les déploiements qui contiennent une mise à jour logicielle spécifiée et le regroupement cible associé au déploiement. |
| **Gestion 7 - Mises à jour dans un déploiement dont le contenu manque** | Affiche les mises à jour logicielles incluses dans un déploiement spécifié qui n'ont pas récupéré tout le contenu associé. Cet état empêche les clients d'installer ces mises à jour et d'atteindre 100 % de compatibilité pour le déploiement. |
| **Gestion 8 - Contenu d'ordinateurs manquant (secondaire)** | Affiche tous les ordinateurs qui nécessitent la mise à jour logicielle spécifiée, mais le contenu associé n'est pas encore distribué à un point de distribution. |

# Mises à jour logicielles - États du déploiement C

Les six rapports suivants sont répertoriés sous la catégorie **Mises à jour logicielles - États du déploiement C**.

| NOM DU RAPPORT | DESCRIPTION |
|---|---|
| **États 1 - États d'application pour un déploiement** | Affiche les états d'application du déploiement de mises à jour logicielles spécifié, qui correspond généralement à la deuxième étape de l'évaluation d'un déploiement. |
| **États 2 - États d'évaluation pour un déploiement** | Affiche l'état d'évaluation du déploiement de mises à jour logicielles spécifié, qui correspond généralement à la première étape de l'évaluation d'un déploiement. |
| **États 3 - États d'un déploiement et d'un ordinateur** | Affiche les états de toutes les mises à jour logicielles incluses dans le déploiement spécifié pour un ordinateur spécifié. |
| **États 4 - Ordinateurs présentant l'état spécifique d'un déploiement (secondaire)** | Affiche tous les ordinateurs présentant un état spécifié pour un déploiement de mises à jour logicielles. |
| **États 5 - États pour une mise à jour dans un déploiement (secondaire)** | Affiche le résumé des états pour une mise à jour logicielle spécifiée ciblée par un déploiement spécifié. |
| **États 6 - Ordinateurs présentant un état d'application spécifique pour une mise à jour (secondaire)** | Affiche tous les ordinateurs dans un état d'application spécifié pour une mise à jour logicielle spécifiée. |

# Mises à jour logicielles - Analyse D

Les quatre rapports suivants sont répertoriés sous la catégorie **Mises à jour logicielles - Analyse D**.

| NOM DU RAPPORT | DESCRIPTION |
|---|---|
| **Analyse 1 - Derniers états d'analyse par regroupement** | Spécifiez un regroupement pour afficher le nombre d'ordinateurs dans chaque état d'analyse de conformité. Les clients retournent l'état pendant la dernière analyse de conformité. |
| **Analyse 2 - Derniers états d'analyse par site** | Spécifiez un site pour afficher le nombre d'ordinateurs dans chaque état d'analyse de conformité. Les clients retournent l'état pendant la dernière analyse de conformité. |
| **Analyse 3 - Clients d'un regroupement signalant un état spécifique (secondaire)** | Affiche tous les ordinateurs d'un regroupement spécifié et dans un état d'analyse de compatibilité spécifié pendant leur dernière analyse de compatibilité. |
| **Analyse 4 - Clients d'un site signalant un état spécifique (secondaire)** | Spécifiez un site pour afficher tous les ordinateurs avec un état d'analyse de conformité spécifié. Les clients retournent l'état pendant leur dernière analyse de conformité. |

# Mises à jour logicielles - Dépannage E

Les quatre rapports suivants sont répertoriés sous la catégorie **Mises à jour logicielles - Dépannage E**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Dépannage 1 - Erreurs d'analyse** | Affiche les erreurs d'analyse au niveau du site et le nombre d'ordinateurs qui rencontrent chaque erreur. |
| **Dépannage 2 – Erreurs de déploiement** | Affiche les erreurs de déploiement au niveau du site et le nombre d'ordinateurs qui rencontrent chaque erreur. |
| **Dépannage 3 - Échecs d'ordinateurs avec une erreur d'analyse spécifique (secondaire)** | Affiche la liste des ordinateurs qui n'ont pas réussi une analyse en raison d'une erreur spécifiée. |
| **Dépannage 4 - Échecs d'ordinateurs avec une erreur de déploiement spécifique (secondaire)** | Affiche la liste des ordinateurs sur lesquels le déploiement de la mise à jour échoue en raison d'une erreur spécifiée. |

## Migration de l'état

Les trois rapports suivants sont répertoriés sous la catégorie **Migration de l'état**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Informations sur la migration de l'état d'un ordinateur source spécifique** | Affiche des informations sur la migration de l'état d'un ordinateur spécifié. |
| **Informations de migration d'état d'un point de migration d'état spécifique** | Affiche des informations sur la migration de l'état d'un point de migration d'état spécifié. |
| **Points de migration d'état d'un site spécifique** | Affiche les points de migration d'état d'un site spécifié. |

## Messages d'état

Les 12 rapports suivants sont répertoriés sous la catégorie **Messages d'état**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Tous les messages pour un ID de message spécifique** | Affiche la liste des messages d'état qui ont un ID de message spécifié. |
| **Clients signalant des erreurs pendant les 12 dernières heures pour un site spécifique** | Affiche la liste des ordinateurs et des composants qui signalent des erreurs pendant les 12 dernières heures et le nombre d'erreurs signalées. |
| **Messages de composants pour les 12 dernières heures** | Affiche la liste des messages de composants pendant les 12 dernières heures pour un code de site, un ordinateur et un composant spécifiés. |
| **Messages de composants pendant la dernière heure** | Affiche une liste des messages d'état créés pendant la dernière heure par un composant donné sur un ordinateur indiqué d'un site spécifié. |
| **Compter les messages de composants pendant la dernière heure pour un site spécifique** | Affiche le nombre de messages d'état par composant et gravité signalés dans la dernière heure dans un site spécifié. |
| **Compter les erreurs survenues dans les 12 dernières heures** | Affiche le nombre de messages d'erreur de composants serveur dans les 12 dernières heures. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Erreurs irrécupérables (par composant)** | Affiche la liste des ordinateurs qui signalent des erreurs irrécupérables par composant. |
| **Erreurs irrécupérables (par nom d'ordinateur)** | Affiche la liste des ordinateurs qui signalent des erreurs irrécupérables par nom d'ordinateur. |
| **Les 1 000 derniers messages pour un ordinateur spécifique (erreurs et avertissements)** | Affiche le résumé des 1000 derniers messages d'état d'erreur et d'avertissement pour un ordinateur spécifié. |
| **1 000 derniers messages pour un ordinateur spécifique (avertissements d'erreur et informations)** | Affiche le résumé des 1000 derniers messages d'état d'erreur, d'avertissement et d'information pour un ordinateur spécifié. |
| **Les 1 000 derniers messages pour un ordinateur spécifique (erreurs)** | Affiche le résumé des 1000 derniers messages d'état d'erreur du composant serveur pour un ordinateur spécifié. |
| **Les 1 000 derniers messages pour un composant serveur spécifique** | Affiche le résumé des 1000 messages d'état les plus récents pour un composant serveur spécifié. |

## Messages d'état - Audit

Les trois rapports suivants sont répertoriés sous la catégorie **Messages d'état - Audit**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Tous les messages d'audit pour un utilisateur spécifique** | Affiche le résumé de tous les messages d'état d'audit pour un utilisateur spécifié. Les messages d'audit décrivent les opérations effectuées dans la console Configuration Manager pour ajouter, modifier ou supprimer des objets dans Configuration Manager. |
| **Contrôle à distance - Tous les ordinateurs contrôlés à distance par un utilisateur spécifique** | Affiche le résumé des messages d'état indiquant un contrôle à distance des ordinateurs clients par un utilisateur spécifié. |
| **Contrôle à distance - Toutes les informations de contrôle à distance** | Affiche le résumé des messages d'état associés au contrôle à distance des ordinateurs clients. |

## État du déploiement de séquence de tâches

Les 11 rapports suivants sont répertoriés sous la catégorie **Séquence de tâches - État du déploiement**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Toutes les ressources système pour un déploiement de séquences de tâches dans un état spécifié** | Affiche la liste des ordinateurs de destination pour le déploiement de séquences de tâches spécifié dans un état de déploiement spécifié. |
| **Toutes les ressources système pour un déploiement de séquences de tâches qui est dans un état spécifique et disponible pour les ordinateurs inconnus** | Affiche la liste des ordinateurs de destination pour le déploiement de séquences de tâches spécifié présentant l'état de déploiement spécifié. |
| **Nombre de ressources système auxquelles des déploiements de séquences de tâches sont affectés mais pas encore exécutés** | Affiche le nombre d'ordinateurs qui ont accepté des séquences de tâches, mais qui n'en ont pas encore exécuté une. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Historique d'un déploiement de séquences de tâches sur un ordinateur** | Affiche l'état de chaque étape du déploiement de séquences de tâches spécifié sur l'ordinateur de destination spécifié. Si aucun rapport n'est créé, la séquence de tâches n'a pas commencé sur l'ordinateur. |
| **Liste des ordinateurs ayant dépassé la durée spécifique d'exécution d'un déploiement de séquences de tâches** | Affiche la liste des ordinateurs de destination qui ont dépassé la durée spécifiée d'exécution d'une séquence de tâches. |
| **Durée d'exécution d'un déploiement de séquences de tâches spécifique sur un ordinateur de destination spécifique** | Affiche le temps total nécessaire pour réussir une séquence de tâches spécifiée sur un ordinateur spécifié. |
| **Durée d'exécution de chaque étape d'un déploiement de séquences de tâches sur un ordinateur de destination spécifique** | Affiche le temps nécessaire pour exécuter chaque chaque étape du déploiement de séquences de tâches spécifié sur l'ordinateur de destination spécifié. |
| **État d'un déploiement de séquences de tâches spécifique pour un ordinateur spécifique** | Affiche la synthèse d'état d'un déploiement de séquences de tâches spécifié sur un ordinateur spécifié. |
| **État d'un déploiement de séquences de tâches sur un ordinateur de destination inconnu** | Affiche l'état du déploiement de séquences de tâches spécifié sur l'ordinateur de destination inconnu spécifié. |
| **Résumé des états d'un déploiement de séquences de tâches spécifique** | Affiche la synthèse d'état de toutes les ressources qui ont été ciblées par un déploiement. |
| **Récapitulatif des états d'un déploiement de séquences de tâches disponible pour des ordinateurs inconnus** | Affiche la synthèse d'état de toutes les ressources ciblées par le déploiement spécifié et disponible pour un regroupement qui contient des ordinateurs inconnus. |

## Séquence de tâches - Déploiements

Les 11 rapports suivants sont répertoriés sous la catégorie **Séquence de tâches - Déploiements**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Toutes les ressources système actuellement dans un groupe ou une phase spécifique du déploiement d'une séquence de tâches spécifique** | Affiche la liste des ordinateurs en cours d'exécution dans un groupe spécifié ou dans une étape de déploiement de séquences de tâches spécifiée. |
| **Toutes les ressources système pour lesquelles un déploiement d'une séquence de tâches a échoué dans un groupe ou une phase spécifique** | Affiche la liste des ordinateurs en échec au sein d'un groupe spécifié ou pendant une phase spécifiée du déploiement de séquences de tâches spécifié. |
| **Tous les déploiements de séquences de tâches** | Affiche les détails de tous les déploiements de séquences de tâches lancés à partir du site actuel. |
| **Tous les déploiements de séquences de tâches disponibles pour les ordinateurs inconnus** | Affiche les détails de tous les déploiements de séquences de tâches lancés à partir du site et déployés sur des regroupements qui contiennent des ordinateurs inconnus. |
| **Nombre d'échecs dans chaque phase ou groupe d'une séquence de tâches spécifique** | Affiche le nombre d'échecs dans chaque phase ou groupe de la séquence de tâches spécifiée. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Nombre d'échecs dans chaque phase ou groupe d'un déploiement de séquences de tâches spécifique** | Affiche le nombre d'échecs dans chaque phase ou groupe du déploiement de séquences de tâches spécifié. |
| **État du déploiement de tous les déploiements de séquences de tâches** | Affiche la progression globale de tous les déploiements de séquences de tâches. |
| **Progression d'une séquence de tâches en cours d'exécution** | Affiche la progression de la séquence de tâches spécifiée. |
| **Progression d'un déploiement de séquences de tâches en cours** | Affiche les informations de synthèse du déploiement de séquences de tâches spécifié. |
| **Progression de tous les déploiements d'une séquence de tâches spécifique** | Affiche la progression de tous les déploiements de la séquence de tâches spécifiée. |
| **Rapport récapitulatif d'un déploiement de séquences de tâches** | Affiche les informations de synthèse du déploiement de séquences de tâches spécifié. |

## Séquence de tâches - Progression

Les cinq rapports suivants sont répertoriés sous la catégorie **Séquence de tâches - Progression**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Graphique - Progression hebdomadaire d'une séquence de tâches** | Affiche la progression hebdomadaire d'une séquence de tâches à partir de la date de déploiement. |
| **Progression d'une séquence de tâches** | Affiche la progression de la séquence de tâches spécifiée. |
| **Progression de toutes les séquences de tâches** | Affiche le résumé de la progression de toutes les séquences de tâches. |
| **Progression des séquences de tâches pour les déploiements de systèmes d'exploitation** | Affiche la progression de toutes les séquences de tâches qui déploient des systèmes d'exploitation. |
| **État de tous les ordinateurs inconnus** | Affiche une liste des ordinateurs qui étaient inconnus au moment où ils ont exécuté un déploiement de séquences de tâches, et indique si ce sont désormais des ordinateurs connus. |

## Séquences de tâches - Références

Le rapport suivant est répertoriés sous la catégorie **Séquence de tâches - Références**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Contenu référencé par une séquence de tâches spécifique** | Affiche le contenu qui est référencé par une séquence de tâches spécifiée. |

## Affinité entre appareil et utilisateur

Les deux rapports suivants sont répertoriés sous la catégorie **Utilisateur - Affinité des périphériques**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Associations d'affinités entre périphérique et utilisateur par regroupement en attente** | Ce rapport affiche toutes les attributions d'affinités entre utilisateur et périphérique en attente, selon les données d'utilisation, pour les membres d'un regroupement. |
| **Associations d'affinités entre périphérique et utilisateur par regroupement** | Affiche toutes les associations entre appareil et utilisateur pour le regroupement spécifié et regroupe les résultats par type de regroupement (par exemple, utilisateur ou appareil). |

## Intégrité du profil et des données utilisateur

Les quatre rapports suivants sont répertoriés sous la catégorie **Intégrité du profil et des données utilisateur**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Rapport d'intégrité de la redirection de dossiers - Détails** | Affiche les détails de l'état d'intégrité de la redirection de dossiers pour chacun des dossiers redirigés d'un utilisateur donné. |
| **Rapport d'intégrité des profils utilisateur itinérants - Détails** | Affiche les détails de l'état d'intégrité du profil utilisateur itinérant d'un utilisateur spécifié. |
| **Rapport d'intégrité des données et profils utilisateur - Détails** | Affiche les détails sur les erreurs ou les avertissements pour la redirection de dossiers ou les profils utilisateur itinérants. Ce rapport est la cible des détails à partir du rapport de synthèse. |
| **Rapport d'intégrité des données et profils utilisateur - Résumé** | Affiche le résumé des états d'intégrité pour la redirection de dossiers et les profils utilisateur itinérants. |

## Utilisateurs

Les trois rapports suivants sont répertoriés sous la catégorie **Utilisateurs**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Ordinateurs pour un nom d'utilisateur spécifique** | Affiche la liste des ordinateurs qui ont été utilisés par un utilisateur spécifié. |
| **Compter les utilisateurs par domaine** | Affiche le nombre d'utilisateurs dans chaque domaine. |
| **Utilisateurs dans un domaine spécifique** | Affiche la liste des utilisateurs et de leurs ordinateurs dans un domaine spécifié. |

## Applications virtuelles

Les sept rapports suivants sont répertoriés sous la catégorie **Applications virtuelles**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Résultats de l'environnement virtuel App-V** | Affiche des informations sur un environnement virtuel spécifié qui se trouve dans un état spécifié pour un regroupement spécifié. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Résultats de l'environnement virtuel App-V pour un composant** | Affiche des informations sur un environnement virtuel spécifié pour un composant donné. Il montre également tous les types de déploiements pour l'environnement virtuel spécifié. |
| **État de l'environnement virtuel App-V** | Affiche des informations de compatibilité d'un environnement virtuel spécifié pour un regroupement spécifié. |
| **Ordinateurs avec une application virtuelle spécifique** | Affiche le résumé des ordinateurs pour lesquels le raccourci de l'application App-V créé est spécifié comme utilisant Application Virtualization Management Sequencer. |
| **Ordinateurs avec un package d'application virtuelle spécifique** | Affiche une synthèse des ordinateurs avec le package d'application App-V spécifié. |
| **Total des instances de packages d'application virtuelle** | Afficher le nombre de packages d'application App-V détectés. |
| **Total des instances d'applications virtuelles** | Affiche le nombre d'applications App-V détectées. |

## Programmes d'achat en volume (VPP) - Apple

Le rapport suivant est répertorié sous la catégorie **Programmes d'achat en volume - Apple**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Applications du programme d'achat en volume (VPP) Apple pour iOS avec les nombres de licences** | Affiche toutes les applications iPhone, iPad et iPod Touch concédées sous licence par le biais du programme d'achat en volume (VPP) d'Apple. Ce rapport inclut également le nombre total de licences achetées ainsi que les licences consommées par application. |

## Évaluation de la vulnérabilité

Le rapport suivant est répertorié sous la catégorie **Évaluation de la vulnérabilité**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Rapport global d'évaluation de la vulnérabilité** | Identifie les vulnérabilités de conformité, de sécurité et d'administration d'un ordinateur spécifique |

## Éveil par appel réseau

Les sept rapports suivants sont répertoriés sous la catégorie **Wake On LAN**.

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Tous les ordinateurs ciblés pour une activité d'éveil par appel réseau** | Indiquez le type de déploiement pour afficher une liste d'ordinateurs ciblés pour une activité Wake On LAN. |
| **Tous les objets en attente de mise en éveil** | Affiche les objets qui sont programmés pour la mise en éveil. |
| **Tous les sites activés pour l'éveil par appel réseau** | Affiche la liste de tous les sites de la hiérarchie qui sont activés pour l'éveil par appel réseau. |

| NOM DU RAPPORT | DESCRIPTION |
| --- | --- |
| **Erreurs reçues lors de l'envoi des paquets de mise en éveil pour une période donnée** | Affiche les erreurs reçues lors de l'envoi des paquets de mise en éveil aux ordinateurs pendant une période donnée. |
| **Historique de l'activité d'éveil par appel réseau** | Affiche l'historique de l'activité d'éveil qui a eu lieu depuis un certain temps. |
| **Détails sur l'état du déploiement de proxy de mise en éveil** | Affiche des informations sur l'état du déploiement de proxy de mise en éveil pour chaque appareil d'un regroupement spécifié. |
| **Résumé de l'état de déploiement du proxy de mise en éveil** | Affiche le résumé de l'état de déploiement du proxy de mise en éveil pour un regroupement spécifié. |

# Configuration des rapports dans System Center Configuration Manager

22/06/2018 • 39 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Avant de créer, modifier et exécuter des rapports dans la console System Center Configuration Manager, vous devez effectuer certaines tâches de configuration. Aidez-vous des sections de cette rubrique pour configurer la génération de rapports dans votre hiérarchie Configuration Manager :

Avant de procéder à l'installation et à la configuration de Reporting Services dans votre hiérarchie, passez en revue les rubriques suivantes sur la génération de rapports Configuration Manager :

- Présentation des rapports dans System Center Configuration Manager
- Planification de la création de rapports dans System Center Configuration Manager

## SQL Server Reporting Services

SQL Server Reporting Services est une plate-forme d'édition de rapport basée sur un serveur qui fournit des fonctionnalités complètes de création de rapports pour une variété de sources de données. Le point de Reporting Services dans Configuration Manager communique avec SQL Server Reporting Services pour copier les rapports Configuration Manager dans un dossier de rapports spécifié, configurer les paramètres de Reporting Services et configurer les paramètres de sécurité de Reporting Services. Reporting Services se connecte à la base de données de site Configuration Manager pour récupérer les données qui sont renvoyées quand vous exécutez des rapports.

Avant d'installer le point de Reporting Services dans un site Configuration Manager, vous devez installer et configurer SQL Server Reporting Services sur le système de site qui héberge le rôle de système de site du point de Reporting Services. Pour plus d'informations sur l'installation de Reporting Services, consultez la bibliothèque TechNet de SQL Server.

Utilisez la procédure suivante pour vérifier que SQL Server Reporting Services est installé et fonctionne correctement.

**Pour vérifier que SQL Server Reporting Services est installé et en cours d'exécution**

1. Sur le Bureau, cliquez sur **Démarrer**, **Tous les programmes**, **Microsoft SQL Server 2008 R2**, **Outils de configuration**, puis sur **Gestionnaire de configuration de Reporting Services**.

2. Dans la boîte de dialogue **Connexion relative à la configuration de Reporting Services** , spécifiez le nom du serveur hôte de SQL Server Reporting Services. Dans le menu déroulant, sélectionnez l'instance de SQL Server sur laquelle vous avez installé SQL Reporting Services, puis cliquez sur **Se connecter**. Le Gestionnaire de Configuration de Reporting Services s'ouvre.

3. Sur la page **État du service de rapport** , vérifiez que l'option **État de Report Server** est définie sur **Démarré**. Sinon, cliquez sur **Démarrer**.

4. Sur la page **URL du service Web** , cliquez sur l'URL dans **URL du service Web de service e rapport** pour tester la connexion au dossier de rapport. La boîte de dialogue **Sécurité de Windows** peut s'ouvrir et vous demander vos informations d'identification de sécurité. Par défaut, votre compte d'utilisateur s'affiche. Entrez votre mot de passe, puis cliquez sur **OK**. Vérifiez que la page Web s'ouvre correctement. Fermez la fenêtre du navigateur.

5. Sur la page **Base de données** , vérifiez que le paramètre **Mode du serveur de rapports** est configuré sur **Natif**.

6. Sur la page **URL du Gestionnaire de rapports** , cliquez sur l'URL dans **Identification du site du Gestionnaire de rapports** pour tester la connexion au répertoire virtuel du Gestionnaire de rapports. La boîte de dialogue **Sécurité de Windows** peut s'ouvrir et vous demander vos informations d'identification de sécurité. Par défaut, votre compte d'utilisateur s'affiche. Entrez votre mot de passe, puis cliquez sur **OK**. Vérifiez que la page Web s'ouvre correctement. Fermez la fenêtre du navigateur.

   > **NOTE**
   > Le Gestionnaire de rapports de Reporting Services n'est pas nécessaire à la génération de rapports dans Configuration Manager, mais il l'est si vous voulez exécuter des rapports sur un navigateur Internet ou gérer des rapports à l'aide du Gestionnaire de rapports.

7. Cliquez sur **Quitter** pour fermer le Gestionnaire de configuration de Reporting Services.

## Configuration de Reporting pour utiliser le Générateur de rapports 3.0

**Pour modifier le nom de manifeste Générateur de rapports en Générateur de rapports 3.0**

1. Sur l'ordinateur exécutant la console Configuration Manager, ouvrez l'Éditeur de Registre Windows.

2. Accédez à **HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/Microsoft/ConfigMgr10/AdminUI/Reporting**.

3. Cliquez deux fois sur la clé **ReportBuilderApplicationManifestName** pour modifier les données de valeur.

4. Modifiez **ReportBuilder_2_0_0_0.application** en **ReportBuilder_3_0_0_0.application**, puis cliquez sur **OK**.

5. Fermez l'Éditeur de Registre Windows.

## Installation d'un point de Reporting Services

Le point de Reporting Services doit être installé sur un site pour gérer les rapports sur le site. Le point de Reporting Services copie les dossiers de rapports et les rapports vers SQL Server Reporting Services, applique la stratégie de sécurité des rapports et des dossiers, et définit des paramètres de configuration dans Reporting Services. L'affichage des rapports dans la console Configuration Manager et leur gestion dans Configuration Manager passent par la configuration préalable d'un point de Reporting Services. Le point de Reporting Services est un rôle de système de site qui doit être configuré sur un serveur sur lequel Microsoft SQL Server Reporting Services est installé et en cours d'exécution. Pour plus d'informations sur la configuration requise, consultez Configuration requise pour la création de rapports.

> **IMPORTANT**
> Lors de la sélection d'un site pour installer le point de Reporting Services, n'oubliez pas que les utilisateurs qui accèderont aux rapports devront se trouver dans la même étendue de sécurité que le site où le point de Reporting Services est installé.

> **NOTE**
> Après avoir installé un point de Reporting Services sur un système de site, ne modifiez pas l'URL du serveur de rapports. Par exemple, si vous créez le point de Reporting Services, puis que vous modifiez l'URL du serveur de rapports dans le Gestionnaire de configuration de Reporting Services, la console Configuration Manager continuera d'utiliser l'ancienne URL, et vous ne pourrez pas exécuter, modifier ou créer de rapports à partir de la console. Lorsque vous devez modifier une URL du serveur de rapports, supprimez le point de Reporting Services, modifiez l'URL, puis réinstallez le point de Reporting Services.

> **IMPORTANT**
> Lorsque vous installez un point de Reporting Services, vous devez spécifier un compte du point de Reporting Services. Plus tard, lorsque les utilisateurs d'un autre domaine tenteront d'exécuter un rapport, le rapport ne pourra pas s'exécuter, sauf s'il existe une relation d'approbation bidirectionnelle entre les domaines.

Utilisez la procédure suivante pour installer le point de Reporting Services.

**Pour installer le point de Reporting Services sur un système de site**

1. Dans la console Configuration Manager, cliquez sur **Administration**.
2. Dans l'espace de travail **Administration** , développez **Configuration du site**, puis cliquez sur **Serveurs et rôles de système de site**.

   > **TIP**
   > Pour répertorier uniquement les systèmes de site hébergeant le rôle de site du point de Reporting Services, cliquez avec le bouton droit sur **Serveurs et rôles de système de site** pour sélectionner **Point de Reporting Services**.

3. Ajoutez le rôle de système de site du point de Reporting Services à un serveur de système de site nouveau ou existant en utilisant l'étape correspondante :

   > **NOTE**
   > Pour plus d'informations sur la configuration de systèmes de site, consultez Ajouter des rôles de système de site pour System Center Configuration Manager.

   - **Nouveau système de site**: sous l'onglet **Accueil** , dans le groupe **Créer** , cliquez sur **Créer un serveur de système de site**. L'Assistant **Création d'un serveur de système de site** s'ouvre.
   - **Système de site existant**: cliquez sur le serveur sur lequel vous souhaitez installer le rôle de système de site du point de Reporting Services. Lorsque vous cliquez sur un serveur, la liste des rôles de système de site déjà installés sur le serveur s'affiche dans le panneau des résultats.

     Sur l'onglet **Accueil** , dans le groupe **Serveur** , cliquez sur **Ajouter des rôles de système de site**. L'Assistant **Ajout des rôles de système de site** s'ouvre.

4. Sur la page **Général** , spécifiez les paramètres généraux du serveur de système de site. Lorsque vous ajoutez le point de Reporting Services à un serveur de système de site existant, vérifiez les valeurs qui ont été précédemment configurées.
5. Sur la page **Sélection du rôle système** , sélectionnez **Point Reporting Services** dans la liste des rôles disponibles, puis cliquez sur **Suivant**.

6. Sur la page **Point de Reporting Services** , configurez les paramètres suivants :

   - **Nom du serveur de base de données de site** : spécifiez le nom du serveur qui héberge la base de données de site Configuration Manager. En règle générale, l'Assistant récupère automatiquement le nom de domaine complet (FQDN) du serveur. Pour spécifier une instance de base de données, utilisez le format *<nom_serveur><nom_instance>*.

   - **Nom de la base de données** : spécifiez le nom de la base de données de site Configuration Manager, puis cliquez sur **Vérifier** pour confirmer que l'Assistant a accès à la base de données de site.

     > **IMPORTANT**
     > Le compte d'utilisateur qui crée le point de Reporting Services doit avoir accès **en lecture** à la base de données de site. Si le test de connexion échoue, une icône d'avertissement rouge s'affiche. Déplacez le curseur sur cette icône afin de lire les informations relatives à la défaillance. Corrigez la défaillance, puis cliquez à nouveau sur **Tester** .

   - **Nom du dossier** : spécifiez le nom de dossier qui est créé et utilisé pour héberger les rapports Configuration Manager dans Reporting Services.

   - **Instance du serveur reporting Services**: sélectionnez dans la liste l'instance de SQL Server Reporting Services. Lorsqu'une seule instance est trouvée, par défaut, elle est répertoriée et sélectionnée. Lorsqu'aucune instance n'est trouvée, vérifiez que SQL Server Reporting Services est installé et configuré, et que le service SQL Server Reporting Services est démarré sur le système de site.

     > **IMPORTANT**
     > Configuration Manager établit une connexion dans le contexte de l'utilisateur actif avec Windows Management Instrumentation (WMI) sur le système de site sélectionné pour récupérer l'instance de SQL Server pour Reporting Services. L'utilisateur actuel doit disposer d'un accès **Lecture** à WMI sur le système de site, sans quoi, les instances de Reporting Services ne peuvent pas être récupérées.

   - **Compte du point de Reporting Services** : cliquez sur **Définir**, puis sélectionnez le compte à utiliser quand SQL Server Reporting Services sur le point de Reporting Services se connecte à la base de données de site Configuration Manager pour récupérer les données qui s'affichent dans un rapport. Sélectionnez **Compte existant** pour spécifier un compte d'utilisateur Windows déjà configuré en tant que compte Configuration Manager ou sélectionnez **Nouveau compte** pour spécifier un compte d'utilisateur Windows qui n'est pas actuellement configuré en tant que compte Configuration Manager. Configuration Manager accorde automatiquement l'accès à la base de données du site pour l'utilisateur spécifié. L'utilisateur est affiché dans le sous-dossier **Comptes** du nœud **Sécurité** dans l'espace de travail **Administration** avec le nom de compte **Point Reporting Services ConfigMgr** .

     Le compte qui exécute Reporting Services doit appartenir au groupe de sécurité de domaine local **Groupe d'accès d'autorisation Windows**et l'autorisation **Read tokenGroupsGlobalAndUniversal** doit être définie sur **Autoriser**. Il doit y avoir une relation d'approbation bidirectionnelle pour les utilisateurs d'un domaine différent de celui du compte du point de Reporting Services pour pouvoir exécuter des rapports.

     Le compte d'utilisateur Windows et le mot de passe spécifiés sont chiffrés et stockés dans la base de données Reporting Services. Reporting Services récupère les données de rapports à partir de la base de données de site à l'aide de ce compte et de ce mot de passe.

> **IMPORTANT**
> Le compte que vous spécifiez doit disposer d'une autorisation **Connexion locale** sur l'ordinateur hébergeant la base de données Reporting Services.

7. Sur la page **Point Reporting Services** , cliquez sur **Suivant**.
8. Sur la page **Résumé** , vérifiez les paramètres, puis cliquez sur **Suivant** pour installer le point de Reporting Services.

   Une fois l'Assistant complété, des dossiers de rapports sont créés, et les rapports Configuration Manager sont copiés dans les dossiers de rapports spécifiés.

> **NOTE**
> Quand les dossiers de rapports sont créés et que les rapports sont copiés sur le serveur de rapports, Configuration détermine la langue adéquate pour les objets. Si le module linguistique correspondant est installé sur le site, Configuration Manager crée les objets dans la langue du système d'exploitation s'exécutant sur le serveur de rapports du site. Si la langue n'est pas disponible, les rapports sont créés et affichés en anglais. Lorsque vous installez un point de Reporting Services sur un site sans module linguistique, les rapports sont installés en anglais. Si vous installez un module linguistique après avoir installé le point de Reporting Services, vous devez désinstaller et réinstaller ce dernier pour que les rapports soient disponibles dans la langue du module linguistique adéquat. Pour plus d'informations sur les modules linguistiques, consultez Modules linguistiques dans System Center Configuration Manager.

**Installation de fichier et droits de sécurité du dossier de rapport**

Configuration Manager effectue les actions suivantes pour installer le point de Reporting Services et configurer Reporting Services :

> **IMPORTANT**
> Les actions dans la liste suivante sont effectuées en utilisant les informations d'identification du compte configuré pour le service SMS_Executive, qui correspond généralement au compte système local du serveur de site.

- Installe le rôle de site de point de Reporting Services.
- Crée la source de données dans Reporting Services avec les informations d'identification stockées que vous avez spécifiées dans l'Assistant. Il s'agit du compte d'utilisateur Windows et du mot de passe que Reporting Services utilise pour se connecter à la base de données de site lorsque vous exécutez des rapports.
- Crée le dossier racine de Configuration Manager dans Reporting Services.
- Ajoute les rôles de sécurité **Utilisateurs de rapports ConfigMgr** et **Administrateurs de rapport ConfigMgr** dans Reporting Services.
- Crée des sous-dossiers et déploie les rapports Configuration Manager de %ProgramFiles%\SMS_SRSRP vers Reporting Services.
- Ajoute le rôle **Utilisateurs de rapports ConfigMgr** de Reporting Services aux dossiers racine pour tous les comptes d'utilisateurs de Configuration Manager qui disposent de droits de **lecture de site**.
- Ajoute le rôle **Administrateurs de rapport ConfigMgr** de Reporting Services aux dossiers racine pour tous les comptes d'utilisateurs de Configuration Manager qui disposent de droits de **modification de site**.

- Récupère le mappage entre les dossiers de rapports et les types d'objets sécurisés Configuration Manager (conservés dans la base de données de site Configuration Manager).
- Configure les droits suivants pour les utilisateurs administratifs de Configuration Manager sur des dossiers de rapports spécifiques de Reporting Services :
  - Ajoute les utilisateurs et attribue le rôle **Utilisateurs de rapports ConfigMgr** au dossier de rapports associé pour les utilisateurs administratifs qui disposent d'autorisations **Exécuter le rapport** pour l'objet Configuration Manager.
  - Ajoute les utilisateurs et attribue le rôle **Administrateurs de rapport ConfigMgr** au dossier de rapports associé pour les utilisateurs administratifs qui disposent d'autorisations **Modifier le rapport** pour l'objet Configuration Manager.

    Configuration Manager se connecte à Reporting Services et définit les autorisations pour les utilisateurs sur les dossiers racine de Configuration Manager et Reporting Services, et sur des dossiers de rapports spécifiques. Après l'installation initiale du point de Reporting Services, Configuration Manager se connecte à Reporting Services dans un intervalle de 10 minutes pour vérifier que les droits d'utilisateur configurés sur les dossiers de rapports sont les droits associés définis pour les utilisateurs de Configuration Manager. Quand des utilisateurs sont ajoutés ou que des droits d'utilisateur sont modifiés sur le dossier de rapports via le Gestionnaire de rapports de Reporting Services, Configuration Manager remplace ces modifications en utilisant les attributions basées sur les rôles qui sont stockées dans la base de données de site. De même, Configuration Manager supprime les utilisateurs qui n'ont pas de droits de génération de rapports dans Configuration Manager.

## Rôles de sécurité de Reporting Services pour Configuration Manager

Quand Configuration Manager installe le point de Reporting Services, les rôles de sécurité suivants sont ajoutés dans Reporting Services :

- **Utilisateurs de rapports ConfigMgr** : les utilisateurs auxquels ce rôle de sécurité est attribué peuvent seulement exécuter des rapports Configuration Manager.
- **Administrateurs de rapport ConfigMgr** : les utilisateurs auxquels ce rôle de sécurité est attribué peuvent exécuter toutes les tâches liées à la génération de rapports dans Configuration Manager.

## Vérifier l'installation du point de Reporting Services

Après avoir ajouté le rôle de site de point de Reporting Services, vous pouvez vérifier l'installation en consultant les messages d'état spécifiques et les entrées de fichiers journaux. Utilisez la procédure suivante pour vérifier que l'installation du point de Reporting Services a réussi.

> **WARNING**
> Vous pouvez ignorer cette procédure si des rapports sont affichés dans le sous-dossier **Rapports** du nœud **Rapport** dans l'espace de travail **Surveillance** de la console Configuration Manager.

**Pour vérifier l'installation du point de Reporting Services**

1. Dans la console Configuration Manager, cliquez sur **Surveillance**.
2. Dans l'espace de travail **Surveillance** , développez **État du système**, puis cliquez sur **État du composant**.
3. Cliquez sur **SMS_SRS_REPORTING_POINT** dans la liste des composants.

4. Dans l'onglet **Accueil** , dans le groupe **Composant** , cliquez sur **Afficher les messages**, puis cliquez sur **Tous**.

5. Spécifiez une date et une heure pour une période avant d'installer le point de Reporting Services, puis cliquez sur **OK**.

6. Vérifiez que le message d'état avec l'ID 1015 est répertorié, ce qui indique que le point de Reporting Services a été installé avec succès. Vous pouvez aussi ouvrir le fichier Srsrp.log situé dans le dossier <*Chemin_Installation_ConfigMgr*>\Logs et attendre le message **L'installation a réussi**.

   Dans l'Explorateur Windows, accédez à <*Chemin_Installation_ConfigMgr*>\Logs.

7. Ouvrez Srsrp.log et parcourez le fichier journal à partir de l'heure à laquelle le point de Reporting Services a été installé avec succès. Vérifiez que les dossiers de rapport ont été créés, que les rapports ont été déployés et que la stratégie de sécurité de chaque dossier a été confirmée. Recherchez la mention **La vérification que le service Web SRS est intègre sur le serveur a réussi** après la dernière ligne des confirmations des stratégies de sécurité.

## Configurer un certificat auto-signé pour les ordinateurs de la console Configuration Manager

Il existe de nombreuses options vous permettant de créer des rapports pour SQL Server Reporting Services. Quand vous créez ou modifiez des rapports dans la console Configuration Manager, Configuration Manager ouvre le générateur de rapports pour l'utiliser comme environnement de création. Quelle que soit la façon dont vous créez vos rapports Configuration Manager, un certificat auto-signé est nécessaire à l'authentification sur le serveur de base de données de site. Configuration Manager installe automatiquement le certificat sur le serveur de site et sur les ordinateurs sur lesquels le fournisseur SMS est installé. Par conséquent, vous pouvez créer ou modifier des rapports à partir de la console Configuration Manager quand elle est exécutée sur l'un de ces ordinateurs. En revanche, quand vous créez ou modifiez des rapports à partir d'une console Configuration Manager qui installée sur un autre ordinateur, vous devez exporter le certificat à partir du serveur de site, puis l'ajouter au magasin de certificats **Personnes autorisées** sur l'ordinateur qui exécute la console Configuration Manager.

> **NOTE**
> Pour plus d'informations sur les autres environnements de création de rapports pour SQL Server Reporting Services, voir Comparaison d'environnements de création de rapport dans la documentation en ligne de SQL Server 2008.

Prenez pour exemple les procédures suivantes pour transférer une copie du certificat auto-signé du serveur de site vers un autre ordinateur exécutant la console Configuration Manager quand les deux ordinateurs exécutent Windows Server 2008 R2. Si vous ne pouvez pas suivre cette procédure car vous avez une version différente du système d'exploitation, consultez la documentation de votre système d'exploitation pour voir la procédure équivalente.

**Pour transférer une copie du certificat auto-signé du serveur de site vers un autre ordinateur**

1. Effectuez les étapes suivantes sur le serveur de site pour exporter le certificat auto-signé :

   a. Cliquez sur **Démarrer**, sur **Exécuter**, puis tapez **mmc.exe**. Dans la console vide, cliquez sur **Fichier**, puis sur **Ajouter/Supprimer un composant logiciel enfichable**.

   b. Dans la boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables** , sélectionnez **Certificats** dans la liste **Composants logiciels enfichables disponibles**, puis cliquez sur **Ajouter**.

   c. Dans la boîte de dialogue **Composant logiciel enfichable des certificats** , cliquez sur **Compte**

**d'ordinateur**, puis sur **Suivant**.

d. Dans la boîte de dialogue **Sélectionner un ordinateur** , vérifiez que **L'ordinateur local (l'ordinateur sur lequel cette console s'exécute)** est sélectionné, puis cliquez sur **Terminer**.

e. Dans la boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables** , cliquez sur **OK**.

f. Dans la console, développez **Certificats (ordinateur local)**, développez **Personnes autorisées**et sélectionnez **Certificats**.

g. Cliquez avec le bouton droit sur le certificat portant le nom convivial *<nom de domaine complet du serveur de site>*, cliquez sur **Toutes les tâches**, puis sélectionnez **Exporter**.

h. Effectuez toutes les étapes de l' **Assistant Exportation de certificat** à l'aide des options par défaut et enregistrez le certificat avec l'extension de nom de fichier **.cer** .

2. Effectuez les étapes suivantes sur l'ordinateur qui exécute la console Configuration Manager pour ajouter le certificat auto-signé au magasin de certificats Personnes autorisées :

a. Répétez les étapes précédentes de 1.a à 1.e pour configurer le composant logiciel enfichable MMC **Certificat** sur l'ordinateur du point de gestion.

b. Dans la console, développez **Certificats (ordinateur local)** et **Personnes autorisées**, cliquez avec le bouton droit sur **Certificats**, sélectionnez **Toutes les tâches**, puis sélectionnez **Importer** pour lancer l' **Assistant Importation de certificat**.

c. Sur la page **Fichier à importer** , cliquez sur le certificat sauvegardé à l'étape 1.h, puis cliquez sur **Suivant**.

d. Sur la page **Magasin de certificats** , sélectionnez **Placer tous les certificats dans le magasin suivant**, lorsque le **Magasin de certificats** est paramétré sur **Personnes autorisées**, puis cliquez sur **Suivant**.

e. Cliquez sur **Terminer** pour fermer l'Assistant et terminer la configuration des certificats sur l'ordinateur.

## Modifier les paramètres du point de Reporting Services

Une fois le point de Reporting Services installé, vous pouvez modifier les paramètres de connexion de base de données de site et d'authentification dans les propriétés du point de Reporting Services. Utilisez la procédure suivante pour modifier les paramètres du point de Reporting Services.

**Pour modifier les paramètres du point de Reporting Services**

1. Dans la console Configuration Manager, cliquez sur **Administration**.

2. Dans l'espace de travail **Administration** , développez **Configuration du site**, puis cliquez sur **Serveurs et rôles de système de site** pour afficher la liste des systèmes de site.

> **TIP**
> Pour répertorier uniquement les systèmes de site hébergeant le rôle de site du point de Reporting Services, cliquez avec le bouton droit sur **Serveurs et rôles de système de site** pour sélectionner **Point de Reporting Services**.

3. Sélectionnez le système de site qui héberge le point de Reporting Services sur lequel vous souhaitez modifier les paramètres et sélectionnez **Point de Reporting Services** dans **Rôles de système de site**.

4. Dans l'onglet **Rôle du site** , dans le groupe **Propriétés** , cliquez sur **Propriétés**.

5. Dans la boîte de dialogue **Propriétés du point de Reporting Services** , vous pouvez modifier les paramètres suivants :

   - **Nom du serveur de base de données de site** : spécifiez le nom du serveur qui héberge la base de données de site Configuration Manager. En règle générale, l'Assistant récupère automatiquement le nom de domaine complet (FQDN) du serveur. Pour spécifier une instance de base de données, utilisez le format *<nom_serveur>*<*nom_instance*>.

   - **Nom de la base de données** : spécifiez le nom de la base de données de site System Center 2012 Configuration Manager, puis cliquez sur **Vérifier** pour confirmer que l'Assistant a accès à la base de données de site.

     > **IMPORTANT**
     > Le compte d'utilisateur qui crée le point de Reporting Services doit avoir accès en lecture à la base de données de site. Si le test de connexion échoue, une icône d'avertissement rouge s'affiche. Déplacez le curseur sur cette icône afin de lire les informations relatives à la défaillance. Corrigez la défaillance, puis cliquez à nouveau sur **Tester** .

   - **Compte d'utilisateur**: cliquez sur **Définir**, puis sélectionnez le compte à utiliser quand SQL Server Reporting Services sur le point de Reporting Services se connecte à la base de données de site Configuration Manager pour récupérer les données affichées dans un rapport. Sélectionnez **Compte existant** pour spécifier un compte d'utilisateur Windows possédant des droits Configuration Manager existants ou sélectionnez **Nouveau compte** pour spécifier un compte d'utilisateur Windows ne possédant pas de droits dans Configuration Manager. Configuration Manager accorde automatiquement au compte d'utilisateur spécifié l'accès à la base de données du site. Le compte est affiché en tant que compte **Point de rapport SRS ConfigMgr** dans le sous-dossier **Comptes** du nœud **Sécurité** dans l'espace de travail **Administration** .

     Le compte d'utilisateur Windows et le mot de passe spécifiés sont chiffrés et stockés dans la base de données Reporting Services. Reporting Services récupère les données de rapports à partir de la base de données de site à l'aide de ce compte et de ce mot de passe.

     > **IMPORTANT**
     > Lorsque la base de données de site se trouve sur un système de site distant, le compte que vous spécifiez doit disposer des autorisations **Ouvrir une session localement** sur l'ordinateur.

6. Cliquez sur **OK** pour enregistrer les modifications et quitter la boîte de dialogue.

## Mise à niveau de SQL Server

Après la mise à niveau de SQL Server et de l'instance SQL Server Reporting Services utilisée comme source de données pour un point de Reporting Services, des erreurs peuvent se produire au moment où vous exécutez ou modifiez des rapports à partir de la console Configuration Manager. Pour que la génération de rapports fonctionne correctement à partir de la console Configuration Manager, vous devez supprimer le rôle de système de site du point de Reporting Services du site, puis le réinstaller. Toutefois, après la mise à niveau, vous pouvez continuer à exécuter et à modifier des rapports à partir d'un navigateur Internet.

## Configurer les options de rapport

Utilisez les options de rapport d'un site Configuration Manager pour sélectionner le point de Reporting

Services par défaut à utiliser pour gérer vos rapports. Même si vous pouvez posséder plusieurs points de Reporting Services sur un site, seul le serveur de rapports par défaut sélectionné dans les options de rapport est utilisé pour gérer les rapports. Pour configurer les options de rapport de votre un site, procédez comme suit.

**Pour configurer des options de rapport**

1. Dans la console Configuration Manager, cliquez sur **Surveillance**.
2. Dans l'espace de travail **Surveillance** , développez **Rapports**, puis cliquez sur **Rapports**.
3. Dans l'onglet **Accueil** , dans le groupe **Paramètres** , cliquez sur **Options du rapport**.
4. Sélectionnez le serveur de rapports par défaut dans la liste, puis cliquez sur **OK**. Si aucun point de Reporting Services n'est répertorié dans la liste, vérifiez que vous disposez d'un point de Reporting Services correctement installé et configuré sur le site.

## Étapes suivantes

Opérations et maintenance pour les rapports

# Opérations et maintenance pour les rapports dans System Center Configuration Manager

22/06/2018 • 39 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Une fois l'infrastructure en place pour la création de rapports dans System Center Configuration Manager, il existe un certain nombre d'opérations que vous pouvez généralement effectuer pour gérer les rapports et les abonnements aux rapports.

## Gérer les rapports Configuration Manager

Configuration Manager offre plus de 400 rapports prédéfinis qui vous aident à recueillir, organiser et présenter des informations relatives aux utilisateurs, à l'inventaire logiciel et matériel, aux mises à jour logicielles, aux applications, à l'état du site et à d'autres opérations de Configuration Manager dans votre organisation. Vous pouvez utiliser les rapports prédéfinis comme ils sont, ou vous pouvez modifier un rapport pour qu'il réponde à vos besoins. Vous pouvez également créer des rapports personnalisés basés sur des modèles ou sur SQL qui répondent à vos besoins. Utilisez les sections suivantes pour mieux gérer les rapports Configuration Manager.

**Exécuter un rapport Configuration Manager**

Rapports dans le Gestionnaire de Configuration sont stockés dans SQL Server Reporting Services et les données affichées dans le rapport sont récupérées à partir de la base de données de site Configuration Manager. Vous pouvez accéder aux rapports dans la console Configuration Manager ou à l'aide du Gestionnaire de rapports dans un navigateur web. Les rapports peuvent être ouverts depuis n'importe quel ordinateur disposant d'un accès à l'ordinateur exécutant SQL Server Reporting Services, si vous possédez les droits vous permettant de consulter les rapports. Lorsque vous exécutez un rapport, le titre du rapport, la description et la catégorie sont affichés dans la langue du système d'exploitation local.

> **NOTE**
> Dans certaines langues autres que l'anglais, les caractères peuvent ne pas apparaître correctement dans les rapports. Dans ce cas, les rapports peuvent être affichés à l'aide du Gestionnaire de rapports basé sur le web ou par le biais de la console Administration à distance.

> **WARNING**
> Pour exécuter des rapports, vous devez disposez des droits de **Lecture** pour l'autorisation **Site** et l'autorisation **Exécuter le rapport** configurée pour des objets spécifiques.

> **IMPORTANT**
> Il doit y avoir une relation d'approbation bidirectionnelle pour les utilisateurs d'un domaine différent de celui du compte du Point de Reporting Servicies pour pouvoir exécuter des rapports.

> **NOTE**
> Le Gestionnaire de rapports est un outil de gestion et d'accès aux rapports basé sur le web que vous utilisez pour administrer une instance de serveur de rapports unique sur un emplacement distant via une connexion HTTP. Vous pouvez utiliser le Gestionnaire de rapports pour les tâches opérationnelles, par exemple, pour afficher des rapports, modifier les propriétés des rapports et gérer les abonnements aux rapports associés. Cette rubrique indique les étapes permettant d'afficher un rapport et de modifier ses propriétés dans le Gestionnaire de rapports. Pour plus d'informations sur les autres options du Gestionnaire de rapports, voir Gestionnaire de rapports dans la documentation en ligne de SQL Server 2008.

Utilisez les procédures suivantes pour exécuter un rapport de Configuration Manager.

**Pour exécuter un rapport dans la console Configuration Manager**

1. Dans la console Configuration Manager, cliquez sur **Surveillance**.
2. Dans l'espace de travail **Surveillance** , développez **Rapports**, puis cliquez sur **Rapports** pour consulter la liste des rapports disponibles.

   > **IMPORTANT**
   > Dans cette version de Configuration Manager, les rapports **Tout le contenu** affichent uniquement les packages, pas les applications.

   > **TIP**
   > Si aucun rapport n'est répertorié, vérifiez que le point de Reporting Services est installé et configuré. Pour plus d'informations, consultez Configuration des rapports.

3. Sélectionnez le rapport à exécuter, puis dans l'onglet **Accueil** , dans la section **Groupe de rapports** , cliquez sur **Exécuter** pour ouvrir le rapport.
4. Lorsque des paramètres sont requis, spécifiez-les, puis cliquez sur **Afficher le rapport**.

**Pour exécuter un rapport depuis un navigateur Web**

1. Dans votre navigateur web, entrez l'URL du Gestionnaire de rapports, par exemple **http://Server1/Reports**. Vous pouvez déterminer l'URL du Gestionnaire de rapports sur le **URL du Gestionnaire de rapports** page dans le Gestionnaire de Configuration de Reporting Services.
2. Dans le Gestionnaire de rapports, cliquez sur le dossier de rapports pour Configuration Manager, par exemple, **ConfigMgr_CAS**.

   > **TIP**
   > Si aucun rapport n'est répertorié, vérifiez que le point de Reporting Services est installé et configuré. Pour plus d'informations, consultez Configuration des rapports.

3. Cliquez sur la catégorie de rapport du rapport que vous souhaitez exécuter, puis cliquez sur le lien du rapport. Le rapport s'ouvre dans le Gestionnaire de rapports.
4. Lorsque des paramètres sont requis, spécifiez-les, puis cliquez sur **Afficher le rapport**.

### Modifier les propriétés d'un rapport Configuration Manager

Dans la console Configuration Manager, vous pouvez afficher les propriétés d'un rapport, telles que son nom et sa description. Si vous souhaitez modifier ces propriétés, utilisez le Gestionnaire de rapports. Utilisez la procédure suivante pour modifier les propriétés d'un rapport Configuration Manager.

#### Pour modifier les propriétés de rapports dans le Gestionnaire de rapports

1. Dans votre navigateur web, entrez l'URL du Gestionnaire de rapports, par exemple **http://Server1/Reports**. Vous pouvez déterminer l'URL du Gestionnaire de rapports sur le **URL du Gestionnaire de rapports** page dans le Gestionnaire de Configuration de Reporting Services.
2. Dans le Gestionnaire de rapports, cliquez sur le dossier de rapports pour Configuration Manager, par exemple, **ConfigMgr_CAS**.

   > **TIP**
   > Si aucun rapport n'est répertorié, vérifiez que le point de Reporting Services est installé et configuré. Pour plus d'informations, consultez Configuration des rapports.

3. Cliquez sur la catégorie du rapport dont vous souhaitez modifier les propriétés, puis cliquez sur son lien. Le rapport s'ouvre dans le Gestionnaire de rapports.
4. Cliquez sur l'onglet **Propriétés** . Vous pouvez modifier le nom et la description du rapport.
5. Lorsque vous avez terminé, cliquez sur **Appliquer**. Les propriétés du rapport sont enregistrées sur le serveur de rapports et la console Configuration Manager récupère les propriétés de rapport mises à jour pour le rapport.

### Modifier un rapport Configuration Manager

Lorsqu'un rapport Configuration Manager existant ne récupère pas les informations dont vous devez disposer ou qu'il ne donne pas la mise en page ou l'aspect que vous souhaitez, vous pouvez le modifier dans le Générateur de rapports.

> **NOTE**
> Vous pouvez aussi choisir de cloner un rapport existant en l'ouvrant pour le modifier et en cliquant sur **Enregistrer sous** pour l'enregistrer en tant que nouveau rapport.

> **IMPORTANT**
> Le compte d'utilisateur doit disposer des autorisations **Site - Modifier** et **Modifier le rapport** sur les objets spécifiques associés au rapport que vous souhaitez modifier.

> **IMPORTANT**
> Lorsque Configuration Manager est mis à niveau vers une version plus récente, les nouveaux rapports remplacent les rapports prédéfinis. Si vous modifiez un rapport prédéfini, vous devez sauvegarder le rapport avant d'installer la nouvelle version, puis restaurer le rapport dans Reporting Services. Si vous apportez des modifications importantes à un rapport prédéfini, envisagez plutôt de créer un nouveau rapport. Les nouveaux rapports que vous créez avant la mise à niveau d'un site ne sont pas remplacés.

Utilisez la procédure suivante pour modifier les propriétés d'un rapport Configuration Manager.

#### Pour modifier les propriétés d'un rapport

1. Dans la console Configuration Manager, cliquez sur **Surveillance**.
2. Dans l'espace de travail **Surveillance** , développez **Rapports**, puis cliquez sur **Rapports** pour consulter la liste des rapports disponibles.
3. Sélectionnez le rapport à modifier, puis dans l'onglet **Accueil** , dans la section **Groupe de rapports** ,

cliquez sur **Modifier**. Entrez votre compte d'utilisateur et votre mot de passe si vous y êtes invité, puis cliquez sur **OK**. Si le Générateur de rapports n'est pas installé sur l'ordinateur, vous êtes invité à l'installer. Cliquez sur **Exécuter** pour installer le Générateur de rapports, qui est requis pour modifier et créer des rapports.

4. Dans le Générateur de rapports, modifiez les paramètres de rapport appropriés, puis cliquez sur **Enregistrer** pour enregistrer le rapport sur le serveur de rapports.

**Créer un rapport basé sur un modèle**

Un rapport basé sur un modèle vous permet de sélectionner les éléments que vous souhaitez inclure dans votre rapport de manière interactive. Pour plus d'informations sur la création de modèles de rapport personnalisés, consultez Création de modèles de rapport personnalisés pour System Center Configuration Manager dans SQL Server Reporting Services.

> **IMPORTANT**
> Pour pouvoir créer un rapport, le compte d'utilisateur doit disposer d'une autorisation **Site - Modifier** . L'utilisateur peut créer un rapport uniquement dans les dossiers pour lesquels il dispose d'autorisations **Modifier le rapport** .

Pour créer un rapport Configuration Manager basé sur un modèle, procédez comme suit.

**Pour créer un rapport basé sur un modèle**

1. Dans la console Configuration Manager, cliquez sur **Surveillance**.
2. Dans l'espace de travail **Surveillance** , développez **Rapports** et cliquez sur **Rapports**.
3. Dans l'onglet **Accueil** , dans la section **Créer** , cliquez sur **Créer un rapport** pour ouvrir l' **Assistant Création de rapport**.
4. Sur la page **Informations** , configurez les paramètres suivants :
   - **Type** : Sélectionnez **Rapport basé sur un modèle** pour créer un rapport dans le Générateur de rapports en utilisant un modèle de Reporting Services.
   - **Nom**: Spécifiez le nom du rapport.
   - **Description**: Spécifiez la description du rapport.
   - **Serveur**: Permet d'afficher le nom du serveur sur lequel le rapport est créé.
   - **Chemin**: Cliquez sur **Parcourir** pour spécifier un dossier dans lequel vous souhaitez stocker le rapport.

     Cliquez sur **Suivant**.
5. Sur la page **Sélection de modèle** , sélectionnez un modèle disponible dans la liste que vous utilisez pour créer ce rapport. Lorsque vous sélectionnez le modèle de rapport, la section **Aperçu** affiche les vues et les entités de SQL Server qui sont rendues disponibles par le modèle de rapport sélectionné.
6. Dans la page **Résumé** , vérifiez les paramètres. Cliquez sur **Précédent** pour modifier les paramètres ou cliquez sur **Suivant** pour créer le rapport dans Configuration Manager.
7. Sur la page **Confirmation** , cliquez sur **Fermer** pour quitter l'Assistant, puis ouvrez le Générateur de rapports pour configurer les paramètres du rapport. Entrez votre compte d'utilisateur et votre mot de passe si vous y êtes invité, puis cliquez sur **OK**. Si le Générateur de rapports n'est pas installé sur l'ordinateur, vous êtes invité à l'installer. Cliquez sur **Exécuter** pour installer le Générateur de rapports, qui est requis pour modifier et créer des rapports.
8. Dans le Générateur de rapports Microsoft, effectuez la mise en page du rapport, sélectionnez des données

dans les vues SQL Server disponibles, ajoutez des paramètres au rapport et ainsi de suite. Pour plus d'informations sur l'utilisation du Générateur de rapports pour créer un nouveau rapport, consultez l'aide du Générateur de rapports.

9. Cliquez sur **Exécuter** pour exécuter le rapport. Vérifiez que le rapport fournit les informations désirées. Cliquez sur **Création** pour revenir au mode Création pour modifier le rapport, si nécessaire.
10. Cliquez sur **Enregistrer** pour enregistrer le rapport sur le serveur de rapports. Vous pouvez exécuter et modifier le nouveau rapport dans le nœud **Rapports** de l'espace de travail **Surveillance** .

### Créer un rapport basé sur SQL

Un rapport basé sur SQL vous permet de récupérer des données basées sur une instruction SQL de rapport.

> **IMPORTANT**
> Lorsque vous créez une instruction SQL pour un rapport personnalisé, ne faites pas directement référence aux tables SQL Server. Faites plutôt référence aux vues SQL Server de rapports (noms de vues qui commencent par v_) à partir de la base de données de site. Vous pouvez également faire référence aux procédures stockées publiques (noms de procédures stockées qui commencent par sp_) à partir de la base de données de site.

> **IMPORTANT**
> Pour pouvoir créer un rapport, le compte d'utilisateur doit disposer d'une autorisation **Site - Modifier** . L'utilisateur peut créer un rapport uniquement dans les dossiers pour lesquels il dispose d'autorisations **Modifier le rapport** .

Pour créer un rapport Configuration Manager basé sur SQL, procédez comme suit.

#### Pour créer un rapport basé sur SQL

1. Dans la console Configuration Manager, cliquez sur **Surveillance**.
2. Dans l'espace de travail **Surveillance** , développez **Rapports**, puis cliquez sur **Rapports**.
3. Dans l'onglet **Accueil** , dans la section **Créer** , cliquez sur **Créer un rapport** pour ouvrir l' **Assistant Création de rapport**.
4. Sur la page **Informations** , configurez les paramètres suivants :
   - **Type** : Sélectionnez **Rapport basé sur SQL** pour créer un rapport dans le Générateur de rapports en utilisant une instruction SQL.
   - **Nom**: Spécifiez le nom du rapport.
   - **Description**: Spécifiez la description du rapport.
   - **Serveur**: Permet d'afficher le nom du serveur sur lequel le rapport est créé.
   - **Chemin**: Cliquez sur **Parcourir** pour spécifier un dossier dans lequel vous souhaitez stocker le rapport.

     Cliquez sur **Suivant**.
5. Dans la page **Résumé** , vérifiez les paramètres. Cliquez sur **Précédent** pour modifier les paramètres ou cliquez sur **Suivant** pour créer le rapport dans Configuration Manager.
6. Sur la page **Confirmation** , cliquez sur **Fermer** pour quitter l'Assistant et ouvrez le Générateur de rapports pour configurer les paramètres du rapport. Entrez votre compte d'utilisateur et votre mot de passe si vous y êtes invité, puis cliquez sur **OK**. Si le Générateur de rapports n'est pas installé sur l'ordinateur, vous êtes invité à l'installer. Cliquez sur **Exécuter** pour installer le Générateur de rapports, qui

est requis pour modifier et créer des rapports.

7. Dans le Générateur de rapports Microsoft, renseignez l'instruction SQL pour le rapport ou créez une instruction SQL à l'aide des colonnes dans les vues de SQL Server disponibles, puis ajoutez des paramètres au rapport et ainsi de suite.

8. Cliquez sur **Exécuter** pour exécuter le rapport. Vérifiez que le rapport fournit les informations désirées. Cliquez sur **Création** pour revenir au mode Création pour modifier le rapport, si nécessaire.

9. Cliquez sur **Enregistrer** pour enregistrer le rapport sur le serveur de rapports. Vous pouvez exécuter le nouveau rapport dans le nœud **Rapports** de l'espace de travail **Surveillance** .

# Gérer les abonnements aux rapports

Les abonnements aux rapports dans SQL Server Reporting Services permettent de configurer la remise automatique des rapports spécifiés par courrier électronique ou vers une solution de partage de fichiers, à des intervalles de temps planifiés. Utilisez l'**Assistant Création d'abonnement** dans System Center 2012 Configuration Manager pour configurer les abonnements aux rapports.

**Créer un abonnement aux rapports pour remettre un rapport à un partage de fichiers**

Lorsque vous créez un abonnement aux rapports pour remettre un rapport à un partage de fichiers, le rapport est copié au format spécifié pour le partage de fichiers que vous avez indiqué. Vous ne pouvez vous abonner et demander la remise que pour un seul rapport à la fois.

À la différence des rapports qui sont hébergés et gérés par un serveur de rapports, les rapports qui sont remis à un dossier partagé sont des fichiers statiques. Les fonctionnalités interactives définies pour le rapport ne fonctionnent pas pour les rapports qui sont stockés sous forme de fichiers sur le système de fichiers. Les fonctionnalités d'interaction sont représentées comme des éléments statiques. Si le rapport comprend des graphiques, la présentation par défaut est utilisée. Si le rapport contient des liens renvoyant à un autre rapport, le lien est restitué sous forme de texte statique. Si vous souhaitez conserver les fonctionnalités interactives dans un rapport remis, utilisez plutôt la remise par courrier électronique. Pour plus d'informations sur la remise de courrier électronique, consultez la section Créer un abonnement aux rapports pour remettre un rapport par courrier électronique plus loin dans cette rubrique.

Lorsque vous créez un abonnement qui utilise la remise par partage de fichiers, vous devez spécifier un dossier existant comme dossier de destination. Le serveur de rapports ne crée pas de dossiers sur le système de fichiers. Le dossier que vous spécifiez doit être accessible via une connexion réseau. Lorsque vous spécifiez le dossier de destination dans un abonnement, utilisez un chemin UNC et n'incluez pas de barres obliques inverses à la fin du chemin du dossier. Voici un exemple de chemin UNC valide pour le dossier de destination : \\<nom_serveur>\reportfiles\operations\2011.

Les rapports peuvent être rendus dans une variété de formats de fichier, tels que MHTML ou Excel. Pour enregistrer le rapport dans un format de fichier spécifique, sélectionnez ce format de rendu lors de la création de votre abonnement. Par exemple, choisir Excel enregistre le rapport sous forme de fichier Microsoft Excel. Même s'il est possible de sélectionner n'importe quel format de rendu pris en charge, certains formats fonctionnent mieux que d'autres lors du rendu d'un fichier.

Utilisez la procédure suivante pour créer un abonnement aux rapports pour remettre un rapport à un partage de fichiers.

**Pour créer un abonnement à un rapport en vue de remettre un rapport à un partage de fichiers**

1. Dans la console Configuration Manager, cliquez sur **Surveillance**.

2. Dans l'espace de travail **Surveillance** , développez **Rapports** , puis cliquez sur **Rapports** pour consulter la liste des rapports disponibles. Vous pouvez sélectionner un dossier de rapports pour répertorier uniquement les rapports associés à ce dossier.

3. Sélectionnez le rapport que vous souhaitez ajouter à l'abonnement, puis dans l'onglet **Accueil** , dans la section **Groupe de rapports** , cliquez sur **Créer un abonnement** pour ouvrir l' **Assistant Création d'abonnement**.

4. Sur la page **Remise d'abonnement** , configurez les paramètres suivants :

   - Rapport remis par : Sélectionnez **Partage de fichiers Windows** pour remettre le rapport à un partage de fichiers.
   - **Nom du fichier**: Spécifiez le nom de fichier du rapport. Par défaut, le fichier de rapport n'inclut pas d'extension de nom de fichier. Sélectionnez **Ajouter une extension de fichier à la création** pour ajouter automatiquement une extension de nom de fichier à ce rapport, en fonction du format de rendu.
   - **Chemin** : Spécifiez un chemin UNC vers un dossier existant, dans lequel vous souhaitez remettre ce rapport (par exemple, \\<nom_serveur>\<partage_serveur>\<dossier_rapport>).

     > **NOTE**
     > Le nom d'utilisateur spécifié ultérieurement sur cette page doit avoir accès à ce partage de serveur et disposer des autorisations d'écriture sur le dossier de destination.

   - **Format de rendu**: Sélectionnez l'un des formats suivants pour le fichier de rapport :
     - **Fichier XML avec données de rapport**: Enregistre le rapport au format Extensible Markup Language.
     - **CSV (délimité par des virgules)** : Enregistre le rapport au format de valeurs séparées par des virgules.
     - **Fichier TIFF**: Enregistre le rapport au format de fichier TIFF (Tagged Image File Format).
     - **Fichier Acrobat (PDF)** : Enregistre le rapport au format Acrobat Portable Document Format.
     - **HTML 4.0**: Enregistre le rapport sous la forme d'une page Web affichable uniquement dans les navigateurs qui prennent en charge le langage HTML 4.0. Internet Explorer 5 et versions ultérieures prennent en charge le langage HTML 4.0.

       > **NOTE**
       > Si votre rapport contient des images, le format HTML 4.0 ne les inclut pas dans le fichier.

     - **MHTML (archive web)** : Enregistre le rapport au format MIME HTML (mhtml) pouvant être consulté avec de nombreux navigateurs web.
     - **Convertisseur RPL** : Enregistre le rapport au format RPL (Report Page Layout).
     - **Excel**: Enregistre le rapport sous forme de feuille de calcul Microsoft Excel.
     - **Word**: Enregistre le rapport sous forme de document Microsoft Word.
   - **Nom d'utilisateur**: Spécifiez un compte d'utilisateur Windows disposant des autorisations pour accéder au partage de serveur et au dossier de destination. Le compte d'utilisateur doit avoir accès à ce partage de serveur ainsi que l'autorisation d'écriture sur le dossier de destination.
   - **Mot de passe**: Spécifiez le mot de passe du compte d'utilisateur Windows. Dans **Confirmer le mot de passe**, retapez le mot de passe.

- Sélectionnez l'une des options suivantes pour configurer le comportement, lorsqu'un fichier du même nom existe déjà dans le dossier de destination :
  - **Remplacer un fichier existant par une version plus récente**: Spécifie que la nouvelle version remplace le fichier de rapport lorsqu'il existe déjà.
  - **Ne pas remplacer un fichier existant**: Spécifie qu'aucune action n'est effectuée lorsque le fichier de rapport existe déjà.
  - **Incrémenter des noms de fichier dès que des versions plus récentes sont ajoutées**: Spécifie qu'un numéro est ajouté au nom de fichier du nouveau rapport pour le différencier des autres versions lorsque le fichier de rapport existe déjà.
- **Description**: Spécifie la description de cet abonnement au rapport.

  Cliquez sur **Suivant**.

5. Sur la page **Planification d'abonnement** , sélectionnez l'une des options de planification de remise suivantes pour l'abonnement aux rapports :
   - **Utiliser une planification partagée**: Une planification partagée est une planification prédéfinie pouvant être utilisée avec d'autres abonnements à des rapports. Activez cette case à cocher, puis sélectionnez une planification partagée dans la liste si un élément a été spécifié.
   - **Créer une nouvelle planification**: Configurez la planification selon laquelle ce rapport doit s'exécuter, y compris l'intervalle, l'heure et la date de début et la date de fin de cet abonnement.
6. Sur la page **Paramètres d'abonnement** , spécifiez les paramètres pour ce rapport qui seront utilisés lorsqu'il est exécuté en mode sans assistance. Lorsqu'il n'y a aucun paramètre pour le rapport, cette page n'est pas affichée.
7. Sur la page **Résumé** , passez en revue les paramètres d'abonnement au rapport. Cliquez sur **Précédent** pour modifier les paramètres ou cliquez sur **Suivant** pour créer un abonnement à un rapport.
8. Sur la page **Dernière étape** , cliquez sur **Fermer** pour quitter l'Assistant. Vérifiez que l'abonnement au rapport a été créé avec succès. Vous pouvez afficher et modifier des abonnements aux rapports dans le nœud **Abonnements** sous **Rapports** dans l'espace de travail **Surveillance** .

**Créer un abonnement aux rapports pour remettre un rapport par e-mail**

Lorsque vous créez un abonnement aux rapports afin de remettre un rapport par courrier électronique, un message qui contient le rapport en pièce jointe est envoyé aux destinataires que vous aurez configurés. Le serveur de rapports ne valide pas les adresses de messagerie et n'obtient pas d'adresses à partir d'un serveur de messagerie. Vous devez connaître à l'avance les adresses de messagerie que vous souhaitez utiliser. Par défaut, vous pouvez envoyer des rapports à n'importe quel compte de messagerie électronique valide au sein ou en dehors de votre organisation. Vous pouvez sélectionner une ou les deux options de remise par courrier électronique suivantes :

- Envoyer une notification et un lien hypertexte vers le rapport généré.
- Envoyer un rapport incorporé ou joint au message. Le format de rendu et le navigateur déterminent si le rapport est incorporé ou joint. Si votre navigateur prend en charge HTML 4.0 et MHTML et que vous sélectionnez le format de rendu MHTML (archive web), le rapport est incorporé dans le corps du message. Tous les autres formats de rendu (CSV, PDF, Word, etc.) sont ajoutés au message sous forme de pièces jointes. Reporting Services ne vérifie pas la taille de la pièce jointe ni du message avant d'envoyer le rapport. Si le message ou la pièce jointe dépasse la limite maximale autorisée par votre serveur de messagerie, le rapport n'est pas remis.

> **IMPORTANT**
> Vous devez configurer les paramètres de courrier électronique dans Reporting Services pour que l'option de remise **Courrier électronique** soit disponible. Pour plus d'informations sur la configuration des paramètres de courrier électronique dans Reporting Services, voir Configuration d'un serveur de rapport pour la remise par courrier électronique dans la documentation en ligne de SQL Server.

Utilisez la procédure suivante pour créer un abonnement aux rapports permettant de remettre un rapport par courrier électronique.

**Pour créer un abonnement aux rapports permettant de remettre un rapport par courrier électronique**

- Dans la console Configuration Manager, cliquez sur **Surveillance**.
- Dans l'espace de travail **Surveillance** , développez **Rapports** , puis cliquez sur **Rapports** pour consulter la liste des rapports disponibles. Vous pouvez sélectionner un dossier de rapports pour répertorier uniquement les rapports associés à ce dossier.
- Sélectionnez le rapport que vous souhaitez ajouter à l'abonnement, puis dans l'onglet **Accueil** , dans la section **Groupe de rapports** , cliquez sur **Créer un abonnement** pour ouvrir l' **Assistant Création d'abonnement**.
- Sur la page **Remise d'abonnement** , configurez les paramètres suivants :
  - **Rapport remis par** : Sélectionnez **E-mail** pour remettre le rapport en tant que pièce jointe dans un message électronique.
  - **À**: Spécifiez une adresse de messagerie valide du destinataire du rapport.

    > **NOTE**
    > Vous pouvez saisir plusieurs destinataires en séparant chaque adresse de messagerie par un point-virgule.

  - **Cc**: Spécifiez l'adresse de messagerie d'un autre destinataire d'une copie du rapport (facultatif).
  - **Cci**: Spécifiez l'adresse de messagerie d'un autre destinataire d'une copie confidentielle du rapport (facultatif).
  - **Répondre à**: Spécifiez l'adresse de réponse à utiliser au cas où le destinataire déciderait de répondre au message électronique.
  - **Objet**: Spécifiez une ligne d'objet pour le message électronique d'abonnement.
  - **Priorité**: Sélectionnez l'indicateur de priorité pour ce message électronique. Sélectionnez **Faible**, **Normale**ou **Haute**. Le paramètre de priorité est utilisé par Microsoft Exchange pour définir un indicateur dans le but de spécifier l'importance du message électronique.
  - **Commentaire**: Spécifiez un texte à ajouter au corps du message électronique d'abonnement.
  - **Description**: Spécifiez la description de l'abonnement à un rapport.
  - **Inclure un lien**: Inclut une URL au rapport d'abonnement dans le corps du message électronique.
  - **Inclure un rapport** : Spécifiez que le rapport est joint au message électronique. Le format à utiliser pour joindre le rapport est indiqué dans la liste **Format de rendu** .
  - **Format de rendu**: Sélectionnez l'un des formats suivants pour le rapport joint :
    - **Fichier XML avec données de rapport**: Enregistre le rapport au format Extensible Markup Language.

- **CSV (délimité par des virgules)** : Enregistre le rapport au format de valeurs séparées par des virgules.
- **Fichier TIFF**: Enregistre le rapport au format de fichier TIFF (Tagged Image File Format).
- **Fichier Acrobat (PDF)** : Enregistre le rapport au format Acrobat Portable Document Format.
- **MHTML (archive web)** : Enregistre le rapport au format MIME HTML (mhtml) pouvant être consulté avec de nombreux navigateurs web.
- **Excel**: Enregistre le rapport sous forme de feuille de calcul Microsoft Excel.
- **Word**: Enregistre le rapport sous forme de document Microsoft Word.

- Sur la page **Planification d'abonnement** , sélectionnez l'une des options de planification de remise suivantes pour l'abonnement aux rapports :
  - **Utiliser une planification partagée**: Une planification partagée est une planification prédéfinie pouvant être utilisée avec d'autres abonnements à des rapports. Activez cette case à cocher, puis sélectionnez une planification partagée dans la liste si un élément a été spécifié.
  - **Créer une nouvelle planification**: Configurez la planification selon laquelle ce rapport s'exécutera, y compris l'intervalle, l'heure et la date de début et la date de fin de cet abonnement.
- Sur la page **Paramètres d'abonnement** , spécifiez les paramètres pour ce rapport qui seront utilisés lorsqu'il est exécuté en mode sans assistance. Lorsqu'il n'y a aucun paramètre pour le rapport, cette page n'est pas affichée.
- Sur la page **Résumé** , passez en revue les paramètres d'abonnement au rapport. Cliquez sur **Précédent** pour modifier les paramètres ou cliquez sur **Suivant** pour créer un abonnement à un rapport.
- Sur la page **Dernière étape** , cliquez sur **Fermer** pour quitter l'Assistant. Vérifiez que l'abonnement au rapport a été créé avec succès. Vous pouvez afficher et modifier des abonnements aux rapports dans le nœud **Abonnements** sous **Rapports** dans l'espace de travail **Surveillance** .

# Création de modèles de rapport personnalisés pour System Center Configuration Manager dans SQL Server Reporting Services

22/06/2018 • 36 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Des exemples de modèles de rapport sont inclus dans System Center Configuration Manager, mais vous pouvez également définir des modèles de rapport qui répondent aux besoins de votre activité, puis déployer le modèle de rapport sur Configuration Manager pour l'utiliser quand vous créez des rapports basés sur des modèles. Le tableau suivant indique les étapes à suivre pour créer et déployer un modèle de rapport basique.

> **NOTE**
> Pour connaître les étapes à suivre pour créer un modèle de rapport plus avancé, voir la section Étapes de création d'un modèle de rapport avancé dans SQL Server Reporting Services dans cette rubrique.

| ÉTAPE | DESCRIPTION | PLUS D'INFORMATIONS |
|---|---|---|
| Vérifier que SQL Server Business Intelligence Development Studio est installé | Les modèles de rapport sont conçus et créés à l'aide de SQL Server Business Intelligence Development Studio. Vérifiez que SQL Server Business Intelligence Development Studio est installé sur l'ordinateur sur lequel vous créez le modèle de rapport personnalisé. | Pour plus d'informations sur SQL Server Business Intelligence Development Studio, consultez la documentation de SQL Server 2008. |
| Création d'un projet de modèle de rapport | Un projet de modèle de rapport comprend un fichier de définition de la source de données (.ds), un fichier de définition d'une vue de source de données (.dsv) et un fichier de modèle de rapport (.smdl). | Pour plus d'informations, voir la section Pour créer le projet de modèle de rapport de cette rubrique. |
| Définition d'une source de données pour un modèle de rapport | Une fois que vous avez créé un projet de modèle de rapport, vous devez définir une source de données à partir de laquelle extraire les données d'entreprise. Il s'agit en général de la base de données du site Configuration Manager. | Pour plus d'informations, voir la section Pour définir la source de données du modèle de rapport de cette rubrique. |

| ÉTAPE | DESCRIPTION | PLUS D'INFORMATIONS |
| --- | --- | --- |
| Définition d'une vue de source de données pour un modèle de rapport | Après avoir défini les sources de données utilisées dans le projet de modèle de rapport, la prochaine étape consiste à définir une vue de source de données pour le projet. Une vue de source de données est un modèle de données logique basé sur une ou plusieurs sources de données. Les vues de source de données incluent l'accès aux objets physiques (tableaux et vues) contenus dans les sources de données sous-jacentes. SQL Server Reporting Services génère le modèle de rapport à partir de la vue de source de données.<br><br>Les vues de la source de données simplifient le processus de conception du modèle en mettant à votre disposition une représentation efficace des données spécifiées. Sans modifier la source de données sous-jacente, vous pouvez renommer les tables et les champs et ajouter l'ensemble des champs et des tables dérivées à une vue de source de données. Pour obtenir un modèle efficace, ajoutez ces tables uniquement à la vue de source de données à utiliser. | Pour plus d'informations, voir la section Pour définir la vue de la source de données du modèle de rapport de cette rubrique. |
| Créer un modèle de rapport | Un modèle de rapport correspond à une couche située en haut de la base de données et qui permet d'identifier les entités, les champs, ainsi que les rôles. Une fois publiés à l'aide de ces modèles, les utilisateurs du générateur de rapports peuvent développer des rapports sans avoir à connaître les structures de la base de données et sans devoir comprendre ou composer des requêtes. Les modèles contiennent des ensembles d'éléments de rapport associés et regroupés sous un nom convivial. Ils contiennent également des liens prédéfinis entre les éléments d'entreprise et des calculs prédéfinis. Vous pouvez définir des modèles à l'aide d'un langage XML appelé Semantic Model Definition Language (SMDL). L'extension de fichier du modèle de rapport est .smdl. | Pour plus d'informations, voir la section Pour créer le modèle de rapport de cette rubrique. |
| Publication d'un modèle de rapport | Pour générer un rapport via le modèle créé, vous devez publier ce dernier dans un serveur de rapport. La source de données ainsi que la vue de source de données sont incluses dans le modèle lors de sa publication. | Pour plus d'informations, voir la section Pour publier le modèle de rapport en vue de son utilisation dans SQL Server Reporting Services de cette rubrique. |

| ÉTAPE | DESCRIPTION | PLUS D'INFORMATIONS |
| --- | --- | --- |
| Déployer le modèle de rapport sur Configuration Manager | Avant de pouvoir utiliser un modèle de rapport personnalisé dans l'**Assistant Création de rapport** pour créer un rapport basé sur un modèle, vous devez déployer le modèle de rapport sur Configuration Manager. | Pour plus d'informations, voir la section To deploy the custom report model to Configuration Manager de cette rubrique. |

# Étapes de création d'un modèle de rapport basique dans SQL Server Reporting Services

Vous pouvez utiliser les procédures suivantes pour créer un modèle de rapport basique dont les utilisateurs de votre site peuvent se servir pour générer des rapports spécifiques basés sur des modèles et sur des données d'une seule vue de la base de données Configuration Manager. Créez un modèle de rapport destiné à l'auteur du rapport et présentant les informations relatives aux ordinateurs clients de votre site. Ces informations sont extraites de la vue **v_R_System** de la base de données Configuration Manager.

Vérifiez que SQL Server Business Intelligence Development Studio est installé sur l'ordinateur où vous effectuez ces procédures et que cet ordinateur dispose d'une connectivité réseau avec le serveur du point de Reporting Services. Pour plus de détails sur SQL Server Business Intelligence Development Studio, consultez la documentation de SQL Server 2008.

**To create the report model project**

1. Sur le bureau, cliquez sur **Démarrer**, sur **Microsoft SQL Server 2008**, puis sur **SQL Server Business Intelligence Development Studio**.
2. Une fois **SQL Server Business Intelligence Development Studio** ouvert dans Microsoft Visual Studio, cliquez sur **Fichier**, **Nouveau**, puis sur **Projet**.
3. Dans la boîte de dialogue **Nouveau projet** , sélectionnez **Projet de modèle de rapport** dans la liste **Modèles** .
4. Dans la zone **Nom** , spécifiez un nom pour ce modèle de rapport. Dans cet exemple, tapez **Modèle_simple**.
5. Pour créer le projet de modèle de rapport, cliquez sur **OK**.
6. La solution **Modèle_simple** est créée et s'affiche dans l' **Explorateur de solutions**.

> **NOTE**
> Si le volet **Explorateur de solutions** n'est pas visible, cliquez sur **Afficher**, puis sur **Explorateur de solutions**.

**Pour définir la source de données du modèle de rapport**

1. Dans le volet **Explorateur de solutions** de **SQL Server Business Intelligence Development Studio**, cliquez avec le bouton droit sur **Sources de données** pour sélectionner **Ajouter une nouvelle source de données**.
2. Sur la page **Bienvenue dans l'Assistant Sources de données** , cliquez sur **Suivant**.
3. Dans la page **Sélectionner la méthode de définition de la connexion** , vérifiez que l'option **Créer une source de données basée sur une connexion existante ou nouvelle** est sélectionnée, puis cliquez sur **Nouveau**.
4. Dans la boîte de dialogue **Connection Manager** , spécifiez les propriétés de connexion suivantes pour la

source de données :

- **Nom du serveur** : tapez le nom du serveur de base de données du site Configuration Manager ou sélectionnez-le dans la liste. Si vous utilisez une instance nommée au lieu de celle par défaut, tapez *<serveur_base_de_données>\<nom_instance>*.
- Sélectionnez **Utiliser l'authentification Windows**.
- Dans la liste **Sélectionner ou entrer un nom de base de données**, sélectionnez le nom de la base de données du site Configuration Manager.

5. Pour vérifier la connexion à la base de données, cliquez sur **Tester la connexion**.
6. Si la connexion fonctionne, cliquez sur **OK** pour fermer la boîte de dialogue **Connection Manager** . Si ce n'est pas le cas, vérifiez que les informations entrées sont correctes, puis cliquez à nouveau sur **Tester la connexion** .
7. Sur la page **Sélectionner la méthode de définition de la connexion** , vérifiez que l'option **Créer une source de données basée sur une connexion existante ou nouvelle** est sélectionnée. Vérifiez également que la source de données que vous venez de spécifier est sélectionnée dans **Connexions de données**, puis cliquez sur **Suivant**.
8. Dans **Nom de la source de données**, spécifiez un nom pour la source de données et cliquez sur **Terminer**. Dans cet exemple, tapez **Modèle_simple**.
9. La source de données **Modèle_simple.ds** s'affiche désormais dans l' **Explorateur de solutions** sous le nœud **Sources de données** .

> **NOTE**
> Pour modifier les propriétés d'une source de données existante, cliquez deux fois dessus dans le dossier **Sources de données** du panneau **Explorateur de solutions** pour afficher les propriétés de la source de données dans Concepteur de sources de données.

**Pour définir la vue de la source de données du modèle de rapport**

1. Dans le volet **Explorateur de solutions**, cliquez avec le bouton droit sur **Vues des sources de données** pour sélectionner **Ajouter une nouvelle vue de source de données**.
2. Sur la page **Bienvenue dans l'Assistant Sources de données** , cliquez sur **Suivant**. La page **Sélectionner une source de données** s'affiche.
3. Dans la fenêtre **Sources de données relationnelles** , vérifiez que la source de données **Modèle_simple** est sélectionnée, puis cliquez sur **Suivant**.
4. Dans la page **Sélectionner des tables et des vues** , dans la liste **Objets disponibles** , sélectionnez la vue suivante à utiliser dans le modèle de rapport : **v_R_System (dbo)**.

> **TIP**
> Pour localiser aisément des vues dans la liste **Objets disponibles** , cliquez sur l'en-tête **Nom** situé en haut de la liste pour trier les objets par ordre alphabétique.

5. Après avoir sélectionné la vue, cliquez sur **>** pour transférer l'objet dans la liste **Objets inclus** .
6. Si la page **Correspondance de noms** s'affiche, acceptez les sélections par défaut, puis cliquez sur **Suivant**.
7. Lorsque vous avez sélectionné les objets dont vous avez besoin, cliquez sur **Suivant**, puis spécifiez un nom pour la vue de la source de données. Dans cet exemple, tapez **Modèle_simple**.

8. Cliquez sur **Terminer**. La vue de la source de données **Modèle_simple.dsv** s'affiche dans le dossier **Vues des sources de données** de l' **Explorateur de solutions**.

**To create the report model**

1. Dans l' **Explorateur de solutions**, cliquez avec le bouton droit sur **Modèles de rapport** pour sélectionner **Ajouter un nouveau rapport de modèle**.
2. Sur la page **Bienvenue dans l'Assistant Modèle de rapport** , cliquez sur **Suivant**.
3. Sur la page **Sélectionner des vues de source de données** , sélectionnez la vue de source de données dans la liste **Vues de source de données disponibles** , puis cliquez sur **Suivant**. Dans cet exemple, sélectionnez **Modèle_simple.dsv**.
4. Sur la page **Sélectionner règles de génér. du modèle de rapport** , acceptez les valeurs par défaut, puis cliquez sur **Suivant**.
5. Sur la page **Collecter les statistiques du modèle** , vérifiez que **Mettre à jour les statistiques du modèle avant la production** est sélectionné, puis cliquez sur **Suivant**.
6. Sur la page **Fin de l'Assistant** , spécifiez un nom pour le modèle de rapport. Pour cet exemple, vérifiez que **Modèle_simple** s'affiche.
7. Pour terminer l'Assistant et créer le modèle de rapport, cliquez sur **Exécuter**.
8. Pour quitter l'assistant, cliquez sur **Terminer**. Le modèle de rapport est affiché dans la fenêtre de conception.

**Pour publier le modèle de rapport en vue de son utilisation dans SQL Server Reporting Services**

1. Dans l' **Explorateur de solutions**, cliquez avec le bouton droit sur le modèle de rapport pour sélectionner **Déployer**. Pour cet exemple, le modèle de rapport est **Modèle_simple.smdl**.
2. Examinez l'état du déploiement dans l'angle inférieur gauche de la fenêtre **SQL Server Business Intelligence Development Studio** . Lorsque le déploiement est terminé, **Déploiement réussi** s'affiche. En cas d'échec du déploiement, la raison de l'échec s'affiche dans la fenêtre **Sortie** . Le nouveau modèle de rapport est maintenant disponible sur votre site Web SQL Server Reporting Services.
3. Cliquez sur **Fichier**, cliquez sur **Enregistrer tout**, puis fermez **SQL Server Business Intelligence Development Studio**.

**To deploy the custom report model to Configuration Manager**

1. Localisez le dossier dans lequel vous avez créé le projet du modèle de rapport. Par exemple, %*PROFIL_UTILISATEUR*%\Documents\Visual Studio 2008\Projects\<*nom_projet*>.
2. Copiez les fichiers suivants du dossier du projet de modèle de rapport dans un dossier temporaire sur votre ordinateur :
   - <*nom_modèle*> **.dsv**
   - <*nom_modèle*> **.smdl**
3. Ouvrez les fichiers mentionnés précédemment dans un éditeur de texte tel que le Bloc-notes.
4. Dans le fichier <*nom_modèle*>**.dsv**, localisez la première ligne, qui est la suivante :

   **<DataSourceView xmlns="http://schemas.microsoft.com/analysisservices/2003/engine">**

   Modifiez cette ligne de la manière suivante :

   **<DataSourceView xmlns="http://schemas.microsoft.com/analysisservices/2003/engine"**

**xmlns:xsi="RelationalDataSourceView">**

5. Copiez le contenu entier du fichier dans le Presse-papiers Windows.
6. Fermez le fichier <*nom_modèle*>**.dsv**.
7. Dans le fichier <*nom_modèle*>**.smdl**, localisez les trois dernières lignes, qui sont les suivantes :

   ```
   </Entity>
   ```

   ```
   </Entities>
   ```

   ```
   </SemanticModel>
   ```

8. Collez le contenu du fichier <*nom_modèle*>**.dsv** juste avant la dernière ligne du fichier(**<SemanticModel>**).
9. Enregistrez et fermez le fichier <*nom_modèle*>**.smdl**.
10. Copiez le fichier <*nom_modèle*>**.smdl** dans le dossier *%programfiles%* \Microsoft Configuration Manager\AdminConsole\XmlStorage\Other du serveur de site Configuration Manager.

    > **IMPORTANT**
    > Après avoir copié le fichier du modèle de rapport sur le serveur de site Configuration Manager, vous devez quitter et redémarrer la console Configuration Manager avant de pouvoir utiliser le modèle de rapport à partir de l'**Assistant Création de rapport**.

# Étapes de création d'un modèle de rapport avancé dans SQL Server Reporting Services

Vous pouvez utiliser les procédures suivantes pour créer un modèle de rapport avancé dont les utilisateurs de votre site peuvent se servir pour générer des rapports spécifiques basés sur des modèles et sur des données de plusieurs vues de la base de données Configuration Manager. Vous allez créer un modèle de rapport destiné à l'auteur du rapport et présentant les informations relatives aux ordinateurs clients et au système d'exploitation installé sur ces derniers. Ces informations sont extraites des vues suivantes de la base de données Configuration Manager :

- **V_R_System** : contient des informations sur les ordinateurs découverts et sur le client Configuration Manager.
- **V_GS_OPERATING_SYSTEM**: contient des informations sur le système d'exploitation installé sur l'ordinateur client.

  Les éléments sélectionnés dans les vues précédentes vont être consolidés dans une liste de noms conviviaux, puis présentés à l'auteur du rapport dans le générateur de rapports afin de pouvoir être ajoutés dans des rapports particuliers.

  Vérifiez que SQL Server Business Intelligence Development Studio est installé sur l'ordinateur où vous effectuez ces procédures et que cet ordinateur dispose d'une connectivité réseau avec le serveur du point de Reporting Services. Pour plus de détails sur SQL Server Business Intelligence Development Studio, consultez la documentation de SQL Server.

**To create the report model project**

1. Sur le bureau, cliquez sur **Démarrer**, sur **Microsoft SQL Server 2008**, puis sur **SQL Server Business Intelligence Development Studio**.
2. Une fois **SQL Server Business Intelligence Development Studio** ouvert dans Microsoft Visual Studio,

cliquez sur **Fichier**, **Nouveau**, puis sur **Projet**.

3. Dans la boîte de dialogue **Nouveau projet** , sélectionnez **Projet de modèle de rapport** dans la liste **Modèles** .
4. Dans la zone **Nom** , spécifiez un nom pour ce modèle de rapport. Dans cet exemple, tapez **Modèle_avancé**.
5. Pour créer le projet de modèle de rapport, cliquez sur **OK**.
6. La solution **Modèle_avancé** est créée et s'affiche dans l' **Explorateur de solutions**.

> **NOTE**
> Si le volet **Explorateur de solutions** n'est pas visible, cliquez sur **Afficher**, puis sur **Explorateur de solutions**.

**Pour définir la source de données du modèle de rapport**

1. Dans le volet **Explorateur de solutions** de **SQL Server Business Intelligence Development Studio**, cliquez avec le bouton droit sur **Sources de données** pour sélectionner **Ajouter une nouvelle source de données**.
2. Sur la page **Bienvenue dans l'Assistant Sources de données** , cliquez sur **Suivant**.
3. Dans la page **Sélectionner la méthode de définition de la connexion** , vérifiez que l'option **Créer une source de données basée sur une connexion existante ou nouvelle** est sélectionnée, puis cliquez sur **Nouveau**.
4. Dans la boîte de dialogue **Connection Manager** , spécifiez les propriétés de connexion suivantes pour la source de données :
   - **Nom du serveur** : tapez le nom du serveur de base de données du site Configuration Manager ou sélectionnez-le dans la liste. Si vous utilisez une instance nommée au lieu de celle par défaut, tapez *<serveur_base_de_données>**<nom_instance>*.
   - Sélectionnez **Utiliser l'authentification Windows**.
   - Dans la liste **Sélectionner ou entrer un nom de base de données**, sélectionnez le nom de la base de données du site Configuration Manager.
5. Pour vérifier la connexion à la base de données, cliquez sur **Tester la connexion**.
6. Si la connexion fonctionne, cliquez sur **OK** pour fermer la boîte de dialogue **Connection Manager** . Si ce n'est pas le cas, vérifiez que les informations entrées sont correctes, puis cliquez à nouveau sur **Tester la connexion** .
7. Sur la page **Sélectionner la méthode de définition de la connexion** , vérifiez que l'option **Créer une source de données basée sur une connexion existante ou nouvelle** est sélectionnée. Vérifiez également que la source de données, spécifiée dernièrement, est sélectionnée dans la liste **Connexions de données** , puis cliquez sur **Suivant**.
8. Dans **Nom de la source de données**, spécifiez un nom pour la source de données et cliquez sur **Terminer**. Dans cet exemple, tapez **Modèle_avancé**.
9. La source de données **Modèle_avancé.ds** s'affiche désormais dans l' **Explorateur de solutions** sous le nœud **Sources de données** .

> **NOTE**
> Pour modifier les propriétés d'une source de données existante, cliquez deux fois dessus dans le dossier **Sources de données** du panneau **Explorateur de solutions** pour afficher les propriétés de la source de données dans Concepteur de sources de données.

**Pour définir la vue de la source de données du modèle de rapport**

1. Dans le volet **Explorateur de solutions**, cliquez avec le bouton droit sur **Vues des sources de données** pour sélectionner **Ajouter une nouvelle vue de source de données**.
2. Sur la page **Bienvenue dans l'Assistant Sources de données** , cliquez sur **Suivant**. La page **Sélectionner une source de données** s'affiche.
3. Dans la fenêtre **Sources de données relationnelles** , vérifiez que la source de données **Modèle_avancé** est sélectionnée, puis cliquez sur **Suivant**.
4. Sur la page **Sélectionner des tables et des vues** , dans la liste **Objets disponibles** , sélectionnez les vues suivantes à utiliser dans le modèle de rapport :
   - **v_R_System (dbo)**
   - **v_GS_OPERATING_SYSTEM (dbo)**

   Une fois que vous avez sélectionné chaque vue, cliquez sur **>** pour transférer l'objet dans la liste **Objets inclus** .

   > **TIP**
   > Pour localiser aisément des vues dans la liste **Objets disponibles** , cliquez sur l'en-tête **Nom** situé en haut de la liste pour trier les objets par ordre alphabétique.

5. Si la boîte de dialogue **Correspondance de noms** s'affiche, acceptez les sélections par défaut, puis cliquez sur **Suivant**.
6. Lorsque vous avez sélectionné les objets dont vous avez besoin, cliquez sur **Suivant**, puis spécifiez un nom pour la vue de la source de données. Dans cet exemple, tapez **Modèle_avancé**.
7. Cliquez sur **Terminer**. La vue de la source de données **Modèle_avancé.dsv** s'affiche dans le dossier **Vues des sources de données** de l' **Explorateur de solutions**.

**Pour définir des liens dans la vue de source de données**

1. Dans l' **Explorateur de solutions**, double-cliquez sur **Modèle_avancé.dsv** pour ouvrir la fenêtre de conception.
2. Cliquez avec le bouton droit sur la barre de titre de la fenêtre **v_R_System** pour sélectionner **Remplacer la table**, puis cliquez sur **Par la nouvelle requête nommée**.
3. Dans la boîte de dialogue **Créer une requête nommée** , cliquez sur l'icône **Ajouter une table** (généralement la dernière icône sur le ruban).
4. Dans la boîte de dialogue **Ajouter une table** , cliquez sur l'onglet **Vues** , sélectionnez **V_GS_OPERATING_SYSTEM** dans la liste, puis cliquez sur **Ajouter**.
5. Cliquez sur **Fermer** pour quitter la boîte de dialogue **Ajouter une table** .
6. Dans la boîte de dialogue **Créer une requête nommée** , indiquez ce qui suit :
   - **Nom :** spécifiez le nom de la requête. Dans cet exemple, tapez **Modèle_avancé**.

- **Description :** spécifiez la description de la requête. Dans cet exemple, tapez **Exemple de modèle de rapport de Reporting Services**.

7. Dans la fenêtre **v_R_System** , sélectionnez les éléments suivants dans la liste d'objets à afficher dans le modèle de rapport :
   - **ResourceID**
   - **ResourceType**
   - **Active0**
   - **AD_Domain_Name0**
   - **AD_SiteName0**
   - **Client0**
   - **Client_Type0**
   - **Client_Version0**
   - **CPUType0**
   - **Hardware_ID0**
   - **User_Domain0**
   - **User_Name0**
   - **Netbios_Name0**
   - **Operating_System_Name_and0**
8. Dans la zone **v_GS_OPERATING_SYSTEM** , sélectionnez les éléments suivants dans la liste d'objets à afficher dans le modèle de rapport :
   - **ResourceID**
   - **Caption0**
   - **CountryCode0**
   - **CSDVersion0**
   - **Description0**
   - **InstallDate0**
   - **LastBootUpTime0**
   - **Locale0**
   - **Manufacturer0**
   - **Version0**
   - **WindowsDirectory0**
9. Pour que les objets de ces vues s'affichent dans une même liste proposée à l'auteur du rapport, vous devez spécifier une relation entre les deux tables ou vues à l'aide d'une jointure. Pour joindre les deux vues, utilisez l'objet **ResourceID**qui apparaît dans chacune d'elles.
10. Dans la fenêtre **v_R_System** , cliquez sur l'objet **ResourceID** et, tout en maintenant le bouton de la souris enfoncé, faites-le glisser vers l'objet **ResourceID** de la fenêtre **v_GS_OPERATING_SYSTEM** .

11. Cliquez sur **OK**.
12. La fenêtre **Modèle_avancé** , qui remplace la fenêtre **v_R_System** , contient tous les objets nécessaires pour le modèle de rapport des vues **v_R_System** et **v_GS_OPERATING_SYSTEM** . Vous pouvez à présent supprimer la fenêtre **v_GS_OPERATING_SYSTEM** dans le concepteur de vue de source de données. Cliquez avec le bouton droit sur la barre de titre de la fenêtre **v_GS_OPERATING_SYSTEM** pour sélectionner **Supprimer la table de la vue de source de données**. Dans la boîte de dialogue **Supprimer les objets** , cliquez sur **OK** pour confirmer la suppression.
13. Cliquez sur **Fichier**, puis sur **Enregistrer tout**.

**To create the report model**

1. Dans l' **Explorateur de solutions**, cliquez avec le bouton droit sur **Modèles de rapport** pour sélectionner **Ajouter un nouveau rapport de modèle**.
2. Sur la page **Bienvenue dans l'Assistant Modèle de rapport** , cliquez sur **Suivant**.
3. Sur la page **Sélectionner une vue de source de données** , sélectionnez la vue de source de données dans la liste **Vues de source de données disponibles** , puis cliquez sur **Suivant**. Dans cet exemple, sélectionnez **Modèle_simple.dsv**.
4. Sur la page **Sélectionner règles de génér. du modèle de rapport** , ne modifiez pas les valeurs par défaut, puis cliquez sur **Suivant**.
5. Sur la page **Collecter les statistiques du modèle** , vérifiez que **Mettre à jour les statistiques du modèle avant la production** est sélectionné, puis cliquez sur **Suivant**.
6. Sur la page **Fin de l'Assistant** , spécifiez un nom pour le modèle de rapport. Pour cet exemple, vérifiez que **Modèle_avancé** s'affiche.
7. Pour terminer l'Assistant et créer le modèle de rapport, cliquez sur **Exécuter**.
8. Pour quitter l'assistant, cliquez sur **Terminer**.
9. Le modèle de rapport est affiché dans la fenêtre de conception.

**Pour modifier des noms d'objet dans le modèle de rapport**

1. Dans l' **Explorateur de solutions**, cliquez avec le bouton droit sur un modèle de rapport pour sélectionner **Concepteur de vue**. Dans cet exemple, sélectionnez **Modèle_avancé.smdl**.
2. Dans la vue de conception de modèle de rapport, cliquez avec le bouton droit sur le nom de n'importe quel objet pour sélectionner **Renommer**.
3. Entrez un nouveau nom pour l'objet sélectionné, puis appuyez sur Entrée. Par exemple, vous pouvez renommer l'objet **CSD_Version_0** en **Version du service pack Windows**.
4. Après avoir renommé les objets, cliquez sur **Fichier**, puis sur **Enregistrer tout**.

**Pour publier le modèle de rapport en vue de son utilisation dans SQL Server Reporting Services**

1. Dans l' **Explorateur de solutions**, cliquez avec le bouton droit sur **Modèle_avancé.smdl** pour sélectionner **Déployer**.
2. Examinez l'état du déploiement dans l'angle inférieur gauche de la fenêtre **SQL Server Business Intelligence Development Studio** . Lorsque le déploiement est terminé, **Déploiement réussi** s'affiche. En cas d'échec du déploiement, la raison de l'échec s'affiche dans la fenêtre **Sortie** . Le nouveau modèle de rapport est maintenant disponible sur votre site Web SQL Server Reporting Services.
3. Cliquez sur **Fichier**, cliquez sur **Enregistrer tout**, puis fermez **SQL Server Business Intelligence Development Studio**.

**To deploy the custom report model to Configuration Manager**

1. Localisez le dossier dans lequel vous avez créé le projet du modèle de rapport. Par exemple, %*PROFIL_UTILISATEUR*%\Documents\Visual Studio 2008\Projects\<*nom_projet*>.
2. Copiez les fichiers suivants du dossier du projet de modèle de rapport dans un dossier temporaire sur votre ordinateur :
   - <*nom_modèle*> **.dsv**
   - <*nom_modèle*> **.smdl**
3. Ouvrez les fichiers mentionnés précédemment dans un éditeur de texte tel que le Bloc-notes.
4. Dans le fichier <*nom_modèle*>**.dsv**, localisez la première ligne, qui est la suivante :

   **<DataSourceView xmlns="http://schemas.microsoft.com/analysisservices/2003/engine">**

   Modifiez cette ligne de la manière suivante :

   **<DataSourceView xmlns="http://schemas.microsoft.com/analysisservices/2003/engine" xmlns:xsi="RelationalDataSourceView">**
5. Copiez le contenu entier du fichier dans le Presse-papiers Windows.
6. Fermez le fichier <*nom_modèle*>**.dsv**.
7. Dans le fichier <*nom_modèle*>**.smdl**, localisez les trois dernières lignes, qui sont les suivantes :

   ```
   </Entity>
   ```

   ```
   </Entities>
   ```

   ```
   </SemanticModel>
   ```
8. Collez le contenu du fichier <*nom_modèle*>**.dsv** juste avant la dernière ligne du fichier(**<SemanticModel>**).
9. Enregistrez et fermez le fichier <*nom_modèle*>**.smdl**.
10. Copiez le fichier <*nom_modèle*>**.smdl** dans le dossier *%programfiles%* \Microsoft Configuration Manager\AdminConsole\XmlStorage\Other du serveur de site Configuration Manager.

> **IMPORTANT**
> Après avoir copié le fichier du modèle de rapport sur le serveur de site Configuration Manager, vous devez quitter et redémarrer la console Configuration Manager avant de pouvoir utiliser le modèle de rapport à partir de l'**Assistant Création de rapport**.

# Sécurité et confidentialité pour les rapports dans System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cette rubrique contient les bonnes pratiques de sécurité et les informations de confidentialité pour la création de rapports dans System Center Configuration Manager.

Les rapports Configuration Manager affichent des informations recueillies lors d'opérations standard de gestion de Configuration Manager. Par exemple, vous pouvez afficher un rapport d'informations ayant été collectées à partir de la découverte ou de l'inventaire. Les rapports peuvent également contenir des informations sur l'état actuel pour les opérations de gestion de client, telles que le déploiement de logiciels et la vérification de la conformité.

Pour plus d'informations sur les bonnes pratiques de sécurité et les informations de confidentialité pour les opérations Configuration Manager susceptibles de générer des données pouvant être affichées dans des rapports, consultez Bonnes pratiques de sécurité et informations de confidentialité de System Center Configuration Manager.

# Le point de service de l'entrepôt de données pour System Center Configuration Manager

09/05/2018 • 22 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez le point de service de l'entrepôt de données pour stocker des données d'historique à long terme et créer des rapports sur celles-ci pour votre déploiement de Configuration Manager.

**TIP**

Cette fonctionnalité a été introduite dans la version 1702 en tant que fonctionnalité en préversion. À compter de la version 1706, cette fonctionnalité n'est plus une fonctionnalité en préversion.

**NOTE**

Par défaut, Configuration Manager n'active pas cette fonctionnalité facultative. Vous devez activer cette fonctionnalité avant de l'utiliser. Pour plus d'informations, consultez Activer les fonctionnalités facultatives des mises à jour.

L'entrepôt de données prend en charge jusqu'à 2 To de données, avec des horodatages pour le suivi des modifications. Pour stocker des données, vous utilisez des synchronisations automatisées entre la base de données du site Configuration Manager et la base de données de l'entrepôt de données. Ces informations seront ensuite accessibles à partir de votre point de Reporting Services. Les données qui sont synchronisées avec la base de données de l'entrepôt de données sont conservées pendant trois ans. Périodiquement, une tâche intégrée supprime les données datant de plus de trois ans.

Les données synchronisées incluent les éléments suivants, qui proviennent des groupes des données de site et des données globales :

- Intégrité de l'infrastructure
- Sécurité
- Compatibilité
- Programme malveillant
- Déploiements de logiciels
- Détails d'inventaire (toutefois, l'historique d'inventaire n'est pas synchronisé)

Une fois installé, le rôle de système de site installe et configure la base de données de l'entrepôt de données. Il installe également plusieurs rapports, afin que vous puissiez facilement rechercher ces données et créer des rapports les concernant.

## Prérequis du point de service de l'entrepôt de données

- Le rôle de système de site d'entrepôt de données est pris en charge uniquement sur le site de niveau supérieur de la hiérarchie. (Un site d'administration centrale ou site principal autonome.)
- L'ordinateur sur lequel vous installez le rôle de système de site nécessite .NET Framework 4.5.2 ou version ultérieure.
- Accordez au **compte du point de Reporting Services** l'autorisation d'accès **db_datareader** à la base de données de l'entrepôt de données.

- Le compte de l'ordinateur sur lequel vous installez le rôle de système de site est utilisé pour synchroniser les données avec la base de données de l'entrepôt de données. Ce compte nécessite les autorisations suivantes :
  - des autorisations de niveau **Administrateur** sur l'ordinateur qui héberge la base de données de l'entrepôt de données ;
  - une autorisation **DB_Creator** sur la base de données de l'entrepôt de données ;
  - **DB_owner** ou **DB_reader** avec une autorisation **execute** sur la base de données du site de niveau supérieur.
- La base de données de l'entrepôt de données nécessite l'utilisation de SQL Server 2012 ou version ultérieure. L'édition peut être Standard, Entreprise ou Datacenter.
- Les configurations de SQL Server suivantes sont prises en charge pour héberger la base de données de l'entrepôt :
  - Une instance par défaut
  - Instance nommée
  - Groupe de disponibilité SQL Server AlwaysOn
  - Cluster de basculement SQL Server
- Si vous utilisez des vues distribuées, le rôle de système de site de point de service de l'entrepôt de données doit être installé sur le serveur qui héberge la base de données du site d'administration centrale.

Pour plus d'informations sur la gestion des licences SQL Server pour la base de données de l'entrepôt de données, consultez la FAQ sur les produits et la gestion des licences.

> **IMPORTANT**
>
> L'entrepôt de données n'est pas pris en charge lorsque l'ordinateur qui exécute le point de service de l'entrepôt de données ou qui héberge la base de données de l'entrepôt de données fonctionne avec l'une des langues suivantes :
>
> - JPN – Japonais
> - KOR – Coréen
> - CHS – Chinois simplifié
> - CHT – Chinois traditionnel Ce problème sera résolu dans une version à venir.

## Installer l'entrepôt de données

Chaque hiérarchie prend en charge une seule instance de ce rôle, sur n'importe quel système de site du site de niveau supérieur. L'instance SQL Server qui héberge la base de données de l'entrepôt peut être locale ou distante par rapport au rôle de système de site. L'entrepôt de données fonctionne avec le point de Reporting Services installé sur le même site. Il n'est pas obligatoire d'installer les deux rôles de système de site sur le même serveur.

Pour installer le rôle, vous pouvez utiliser deux assistants : **l'Assistant Ajout des rôles de système de site** ou **l'Assistant Création d'un serveur de système de site**. Pour plus d'informations, consultez la section Installer des rôles de système de site.

Quand vous installez le rôle, Configuration Manager crée la base de données de l'entrepôt de données pour vous sur l'instance de SQL Server que vous spécifiez. Si vous spécifiez le nom d'une base de données existante (comme vous le feriez si vous déplaciez la base de données de l'entrepôt de données vers un nouveau serveur SQL Server), Configuration Manager ne crée pas une base de données, mais utilise à la place celle que vous spécifiez.

**Configurations utilisées lors de l'installation**

Page **Sélection du rôle système** :

Page **Général** :

- **Paramètres de connexion de la base de données de l'entrepôt de données Configuration Manager** :

- **Nom de domaine complet SQL Server** : spécifiez le nom de domaine complet (FQDN) du serveur qui héberge la base de données du point de service de l'entrepôt de données.
- **Nom de l'instance de SQL Server, le cas échéant** : si vous n'utilisez pas l'instance par défaut de SQL Server, vous devez spécifier l'instance utilisée.
- **Nom de la base de données** : spécifiez le nom de la base de données de l'entrepôt de données. Le nom de la base de données ne doit pas dépasser 10 caractères. (La longueur du nom prise en charge sera augmentée dans une version ultérieure.) Configuration Manager crée la base de données de l'entrepôt de données en lui donnant ce nom. Si vous spécifiez un nom de base de données qui existe déjà sur l'instance de SQL Server, Configuration Manager utilise cette base de données.
- **Port SQL Server utilisé pour la connexion** : spécifiez le numéro de port TCP/IP utilisé par l'instance de SQL Server qui héberge la base de données de l'entrepôt de données. Ce port est utilisé par le service de synchronisation de l'entrepôt de données pour se connecter à la base de données de ce dernier.
- **Compte de point de service de l'entrepôt de données** : Depuis la version 1802, indiquez le compte que SQL Server Reporting Services utilise lors de la connexion à la base de données de l'entrepôt de données.

Page **Calendrier des synchronisations** :

- **Calendrier des synchronisations** :
  - **Heure de début** : indiquez l'heure de début de la synchronisation de l'entrepôt de données.
  - **Périodicité** :
    - **Tous les jours** : permet d'indiquer que la synchronisation doit s'exécuter chaque jour.
    - **Hebdomadaire** : permet de spécifier une seule journée chaque semaine ainsi qu'une périodicité hebdomadaire pour la synchronisation.

## Rapports

Une fois que vous aurez installé un point de service de l'entrepôt de données, plusieurs rapports seront accessibles sur le point de Reporting Services installé sur le même site. Si vous installez le point de service de l'entrepôt de données avant d'installer un point de Reporting Services, les rapports seront automatiquement ajoutés lors de l'installation du point de Reporting Services.

> **WARNING**
> Dans Configuration Manager version 1802, une prise en charge d'autres informations d'identification a été ajoutée pour le point de l'entrepôt de données. Si vous avez effectué une mise à niveau à partir d'une version précédente de Configuration Manager, vous devez spécifier les informations d'identification que SQL Server Reporting Services utilise pour se connecter à la base de données de l'entrepôt de données. Les rapports des entrepôts de données ne s'ouvrent pas tant que les informations d'identification ne sont pas spécifiées. Pour indiquer un compte, accédez à **Administration** > **Configuration du site** > **Serveurs et rôles de système de site**. Cliquez sur le serveur avec le point de service de l'entrepôt de données, puis avec le bouton droit sur le rôle de point de service de l'entrepôt de données. Sélectionnez les **propriétés** puis spécifiez le **compte de point de service de l'entrepôt de données**.

Le rôle de système de site de l'entrepôt de données comprend les rapports suivants, qui appartiennent à la catégorie **Entrepôt de données** :

- **Déploiement de l'application – Historique** : détails du déploiement d'une application donnée pour une machine en particulier.
- **Endpoint Protection et Compatibilité des mises à jour logicielles - Historique** : affiche les ordinateurs sur lesquels des mises à jour logicielles n'ont pas été effectuées.
- **Inventaire matériel général – Historique** : tout l'inventaire matériel d'une machine en particulier.
- **Inventaire logiciel général – Historique** : tout l'inventaire logiciel d'une machine en particulier.

- **Vue d'ensemble de l'intégrité de l'infrastructure – Historique** : vue d'ensemble de l'intégrité de l'infrastructure Configuration Manager.
- **Liste des programmes malveillants détectés – Historique** : programmes malveillants détectés dans l'organisation.
- **Synthèse de la distribution de logiciels – Historique** : synthèse de la distribution de logiciels pour une publication et une machine en particulier.

## Étendre un site principal autonome existant vers une hiérarchie

Avant d'installer un site d'administration centrale pour étendre un site principal autonome existant, vous devez désinstaller le rôle de point de service de l'entrepôt de données. Après avoir installé le site d'administration centrale, vous pouvez installer le rôle de système de site sur ce site.

Contrairement au déplacement de la base de données de l'entrepôt de données, cette modification entraîne une perte des données historiques que vous avez synchronisées sur le site principal. La sauvegarde de la base de données à partir du site principal et sa restauration sur le site d'administration centrale ne sont pas prises en charge.

## Déplacer la base de données de l'entrepôt de données

Procédez comme suit pour déplacer la base de données de l'entrepôt de données vers un nouveau serveur SQL Server :

1. Utilisez SQL Server Management Studio pour sauvegarder la base de données de l'entrepôt de données. Ensuite, restaurez cette base de données sur un serveur SQL Server sur le nouvel ordinateur qui héberge l'entrepôt de données.

   > **NOTE**
   > Après avoir restauré la base de données sur le nouveau serveur, vérifiez que les autorisations d'accès à la base de données sont les mêmes sur la nouvelle base de données de l'entrepôt de données que sur la base de données de l'entrepôt de données d'origine.

2. Utilisez la console de Configuration Manager pour supprimer du serveur actuel le rôle de système de site du point de service de l'entrepôt de données.
3. Réinstallez le point de service de l'entrepôt de données. Spécifiez le nom du nouveau serveur SQL Server et de l'instance qui hébergera la base de données de l'entrepôt de données que vous avez restaurée.
4. Une fois le rôle de système de site installé, le déplacement est terminé.

## Résolution des problèmes relatifs à l'entrepôt de données

**Fichiers journaux**
Utilisez les journaux suivants pour examiner les problèmes d'installation du point de service de l'entrepôt de données ou de synchronisation des données :

- *DWSSMSI.log* et *DWSSSetup.log* : utilisez ces journaux pour examiner les erreurs survenues lors de l'installation du point de service de l'entrepôt de données.
- *Microsoft.ConfigMgrDataWarehouse.log* : utilisez ce journal pour examiner la synchronisation des données entre la base de données de site et la base de données de l'entrepôt de données.

**Échec d'installation**
L'installation du point de service de l'entrepôt de données échoue sur un serveur de système de site distant quand le premier rôle de système de site installé sur cet ordinateur est celui de l'entrepôt de données.

- **Solution** : assurez-vous que l'ordinateur sur lequel vous installez le point de service de l'entrepôt de données héberge déjà au moins un autre rôle de système de site.

**Problèmes de synchronisation connus**
La synchronisation échoue et génère le message suivant dans le fichier *Microsoft.ConfigMgrDataWarehouse.log* : **« Impossible de remplir des objets de schéma ».**

- **Solution** : assurez-vous que le compte de l'ordinateur qui héberge le rôle de système de site est bien **db_owner** sur la base de données de l'entrepôt de données.

Les rapports de l'entrepôt de données ne s'ouvrent pas lorsque la base de données de l'entrepôt de données et le point de Reporting Services se trouvent sur des systèmes de site différents.

- **Solution** : accordez au **compte du point de Reporting Services** l'autorisation d'accès **db_datareader** à la base de données de l'entrepôt de données.

Lorsque vous ouvrez un rapport de l'entrepôt de données, l'erreur suivante est renvoyée :

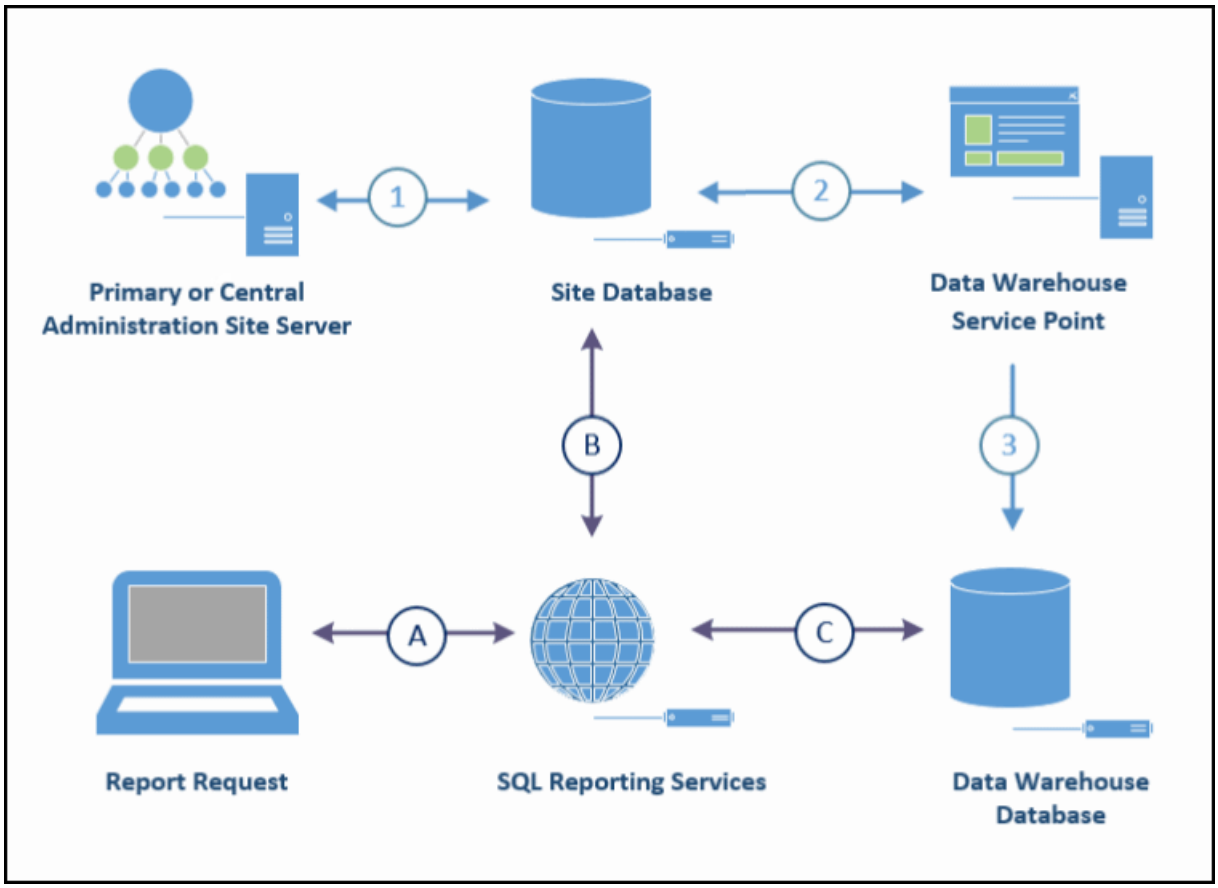
*Une erreur s'est produite lors du traitement du rapport. (rsProcessingAborted) Impossible de créer une connexion à la source de données 'AutoGen__39B693BB_524B_47DF_9FDB_9000C3118E82_'. (rsErrorOpeningConnection) Une connexion a été établie avec le serveur, mais une erreur s'est ensuite produite pendant la négociation préalable à l'ouverture de session. (Fournisseur : fournisseur SSL, erreur : 0 - La chaîne de certificats a été fournie par une autorité qui n'est pas approuvée.)*

- **Solution** : procédez comme suit pour configurer les certificats.

  1. Sur l'ordinateur qui héberge la base de données de l'entrepôt de données :

     a. Ouvrez IIS, cliquez sur **Certificats de serveur**, puis cliquez avec le bouton droit sur **Créer un certificat auto-signé** et spécifiez le « nom convivial » du nom du certificat en tant que **certificat d'identification SQL Server de l'entrepôt de données**. Sélectionnez le magasin de certificats en tant que **Applications personnelles**.
     b. Ouvrez le **Gestionnaire de configuration SQL Server**. Sous **Configuration du réseau SQL Server**, cliquez avec le bouton droit pour sélectionner **Propriétés** sous **Protocoles pour MSSQLSERVER**. Ensuite, sur l'onglet **Certificat**, sélectionnez le **certificat d'identification SQL Server de l'entrepôt de données** et enregistrez les modifications.
     c. Ouvrez le **Gestionnaire de configuration SQL Server**. Sous **Services SQL Server**, redémarrez le **service SQL Server** et le service **Reporting Service**.
     d. Ouvrez la console MMC (Microsoft Management Console) et ajoutez le composant logiciel enfichable relatif aux **certificats**, puis sélectionnez la gestion du certificat pour le **compte d'ordinateur** de la machine locale. Ensuite, dans la console MMC, développez le dossier **Applications personnelles** > **Certificats** et exportez le **certificat d'identification SQL Server de l'entrepôt de données** en tant que fichier **Binaire codé DER X.509 (.cer)**.
  2. Sur l'ordinateur qui héberge SQL Server Reporting Services, ouvrez la console MMC et ajoutez le composant logiciel enfichable **Certificats**. Ensuite, sélectionnez la gestion du certificat pour le **Compte d'ordinateur**. Sous le dossier **Autorités de certification racine reconnues**, importez le **certificat d'identification SQL Server de l'entrepôt de données**.

## Flux de données de l'entrepôt de données




### Synchronisation et stockage des données

| ÉTAPE | DÉTAILS |
|---|---|
| **1** | Le serveur de site transfère et stocke les données dans la base de données de site. |
| **2** | Selon sa planification et sa configuration, le point de service de l'entrepôt de données récupère des données auprès de la base de données de site. |
| **3** | Le point de service de l'entrepôt de données transfère et stocke une copie des données synchronisées dans la base de données de l'entrepôt de données. |

### Rapports

| ÉTAPE | DÉTAILS |
|---|---|
| **A** | Via des rapports intégrés, un utilisateur demande des données. La demande est transmise au point de Reporting Services à l'aide de SQL Server Reporting Services. |
| **B** | La plupart des rapports concernent des informations actuelles et ces demandes sont exécutées sur la base de données de site. |
| **C** | Quand un rapport demande des données d'historique, à l'aide de l'un des rapports de la *Catégorie* **Entrepôt de données**, la demande s'exécute sur la base de données de l'entrepôt de données. |

# Méthodes d'installation du client dans System Center Configuration Manager

22/06/2018 • 8 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez utiliser différentes méthodes pour installer le logiciel client Configuration Manager. Utilisez une ou plusieurs méthodes combinées. Cet article décrit chaque méthode de sorte que vous puissiez vous approprier celle qui convient le mieux à votre organisation.

## Installation poussée du client

**Plateforme cliente prise en charge :** Windows

**Avantages**

- Peut être utilisée pour installer le client sur un seul ordinateur, un regroupement d'ordinateurs ou pour les résultats d'une requête.
- Peut être utilisée pour installer automatiquement le client sur tous les ordinateurs découverts.
- Utilise automatiquement les propriétés d'installation du client définies sous l'onglet **Client** de la boîte de dialogue **Propriétés de l'installation poussée du client** .

**Inconvénients**

- Une installation poussée vers des regroupements volumineux peut entraîner un trafic réseau excessif.
- Peut être utilisée uniquement sur les ordinateurs ayant été découverts par Configuration Manager.
- Ne peut pas être utilisée pour installer des clients dans un groupe de travail.
- Vous devez spécifier un compte d'installation poussée du client disposant des droits d'administration sur l'ordinateur client souhaité.
- Le pare-feu Windows doit être configuré avec des exceptions sur les ordinateurs clients.
- Vous ne pouvez pas annuler une installation Push du client. Configuration Manager tente d'installer le client sur toutes les ressources découvertes. En cas d'échec, il renouvelle les tentatives pendant sept jours, au maximum.

Pour plus d'informations, consultez Comment installer des clients selon la méthode d'installation Push du client.

## Installation basée sur un point de mise à jour logicielle

**Plateforme cliente prise en charge :** Windows

**Avantages**

- Peut utiliser votre infrastructure de mises à jour logicielles existante pour gérer le logiciel client.
- Si Windows Server Update Services (WSUS) et les paramètres de stratégie de groupe d'Active Directory Domaine Services sont correctement configurés, il peut installer automatiquement le logiciel client sur de nouveaux ordinateurs.
- N'exige pas la découverte des ordinateurs avant l'installation du client.
- Les ordinateurs peuvent lire les propriétés de l'installation du client ayant été publiées dans les services de

domaine Active Directory.

- Si le client est supprimé, cette méthode le réinstalle.
- Ne nécessite pas de configuration ni la présence d'un compte d'installation pour l'ordinateur client choisi.

**Inconvénients**

- Nécessite une infrastructure de mises à jour logicielles opérationnelle.
- Doit utiliser le même serveur pour l'installation du client et les mises à jour logicielles. Ce serveur doit résider sur un site principal.
- Pour installer de nouveaux clients, vous devez configurer un objet de stratégie de groupe dans Active Directory Domain Services avec le port et le point de mise à jour logicielle actifs du client.
- Si le schéma Active Directory n'est pas étendu pour Configuration Manager, vous devez utiliser les paramètres de stratégie de groupe pour fournir les propriétés d'installation du client aux ordinateurs.

Pour plus d'informations, consultez Comment installer des clients via une installation basée sur des mises à jour logicielles.

## Installation via la stratégie de groupe

**Plateforme cliente prise en charge :** Windows

**Avantages**

- N'exige pas la découverte des ordinateurs avant l'installation du client.
- Peut être utilisée pour l'installation de nouveaux clients ou pour les mises à niveau.
- Les ordinateurs peuvent lire les propriétés de l'installation du client ayant été publiées dans les services de domaine Active Directory.
- Ne nécessite pas de configuration ni la présence d'un compte d'installation pour l'ordinateur client choisi.

**Inconvénients**

- L'installation simultanée d'un grand nombre de clients peut en engendrer un trafic réseau important.
- Si le schéma Active Directory n'est pas étendu pour Configuration Manager, vous devez utiliser les paramètres de stratégie de groupe pour ajouter les propriétés d'installation du client aux ordinateurs de votre site.

Pour plus d'informations, consultez Comment installer des clients à l'aide d'une stratégie de groupe.

## Installation via un script d'ouverture de session

**Plateforme cliente prise en charge :** Windows

**Avantages**

- N'exige pas la découverte des ordinateurs avant l'installation du client.
- Prend en charge les propriétés de ligne de commande de CCMSetup.

**Inconvénients**

- L'installation simultanée d'un grand nombre de clients sur une courte période peut engendrer un trafic réseau important.
- Si certains utilisateurs ne se connectent pas fréquemment au réseau, l'installation sur tous les ordinateurs clients peut prendre beaucoup de temps.

Pour plus d'informations, consultez Comment installer des clients à l'aide de scripts d'ouverture de session.

## Installation manuelle

**Plateformes clientes prises en charge :** Windows, UNIX/Linux, Mac OS X

**Avantages**

- N'exige pas la découverte des ordinateurs avant l'installation du client.
- Peut être utile dans le cadre de tests.
- Prend en charge les propriétés de ligne de commande de CCMSetup.

**Inconvénients**

- Aucune automatisation, peut prendre du temps.

Pour plus d'informations sur la façon d'installer manuellement le client sur chaque plateforme, consultez les articles suivants :

- Guide pratique pour déployer des clients sur des ordinateurs Windows
- Guide pratique pour déployer des clients sur des serveurs UNIX et Linux
- Guide pratique pour déployer des clients sur des ordinateurs Mac

## Installation de Microsoft Intune MDM

**Plateformes clientes prises en charge :** Windows 10

**Avantages**

- N'exige pas la découverte des ordinateurs avant l'installation du client.
- Ne nécessite pas de configuration ni la présence d'un compte d'installation pour l'ordinateur client choisi.
- Peut utiliser l'authentification moderne avec Azure Active Directory.
- Peut installer et attribuer des ordinateurs sur Internet.
- Peut être automatisée avec Windows AutoPilot et Microsoft Intune pour la cogestion.

**Inconvénients**

- Nécessite des technologies supplémentaires en dehors de Configuration Manager.
- Exige que l'appareil ait accès à Internet, même s'il n'est pas basé sur Internet.

Pour plus d'informations, consultez les articles suivants :

- Guide pratique pour installer des clients sur des appareils Windows gérés par Intune MDM
- Installer et affecter des clients Windows 10 Configuration Manager à l'aide d'Azure AD à des fins d'authentification

# Configuration requise pour le déploiement de clients sur des ordinateurs Windows dans System Center Configuration Manager

22/06/2018 • 24 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Le déploiement de clients Configuration Manager dans votre environnement présente des dépendances externes et internes au produit, comme décrit ci-dessous. En outre, chaque méthode de déploiement client possède ses propres dépendances qui doivent être respectées pour le bon déroulement des installations clients.

Veillez à consulter aussi la rubrique Configurations prises en charge pour vérifier que les appareils sont conformes à la configuration minimale requise du point de vue du matériel et du système d'exploitation pour le client Configuration Manager.

Pour plus d'informations sur les prérequis concernant le client Configuration Manager pour Linux et UNIX, consultez Planification du déploiement de clients sur des ordinateurs Linux et UNIX.

> **NOTE**
> Les numéros de version de logiciel mentionnés dans cet article indiquent uniquement les numéros de version minimale requise.

## Prérequis pour les ordinateurs clients

Aidez-vous des informations suivantes pour déterminer la configuration requise pour installer le client Configuration Manager sur des ordinateurs.

**Dépendances externes à Configuration Manager**

| | |
|---|---|
| Windows Installer version 3.1.4000.2435 | Obligatoire pour prendre en charge l'utilisation des fichiers de mise à jour (.msp) Windows Installer pour les packages et les mises à jour logicielles. |
| KB2552033 | Installez ce correctif sur les serveurs de site exécutant Windows Server 2008 R2 quand l'installation Push du client est activée. |
| Service Microsoft BITS (Background Intelligent Transfer Service) version 2.5 | Requis pour autoriser le transfert contrôlé des données entre l'ordinateur client et les systèmes de site Configuration Manager. BITS n'est pas automatiquement téléchargé lors de l'installation du client. Lorsque le service BITS est installé sur les ordinateurs, un redémarrage est généralement nécessaire pour terminer l'installation.<br><br>La plupart des systèmes d'exploitation intègrent le service BITS. Si cela n'est pas le cas, comme Windows Server 2003 R2 SP2, par exemple, vous devez installer ce service avant d'installer le client Configuration Manager. |

| | |
|---|---|
| Planificateur de tâches Microsoft | Activez ce service sur le client pour accomplir l'installation du client. |

**Dépendances extérieures à Configuration Manager et téléchargées automatiquement pendant l'installation**

Le client Configuration Manager présente plusieurs dépendances externes potentielles. Ces dépendances dépendent du système d'exploitation et du logiciel installé sur l'ordinateur client.

Si elles sont nécessaires à l'installation du client, ces dépendances sont installées automatiquement avec le logiciel client.

| | |
|---|---|
| Agent Windows Update version 7.0.6000.363 | Requis par Windows pour prendre en charge la détection et le déploiement des mises à jour. |
| Microsoft Core XML Services (MSXML) version 6.20.5002 ou supérieure | Obligatoire pour prendre en charge le traitement des documents XML dans Windows. |
| Microsoft Remote Differential Compression (RDC) | Requis pour optimiser la transmission de données sur le réseau. |
| Microsoft Visual C++ 2013 Redistributable version 12.0.21005.1 | Requis pour prendre en charge les opérations de clients. Lorsque cette mise à jour est installée sur les ordinateurs clients, un redémarrage peut être nécessaire pour terminer l'installation. |
| Microsoft Visual C++ 2005 Redistributable version 8.0.50727.42 | Pour la version 1606 et les versions antérieures, exigé pour prendre en charge les opérations de Microsoft SQL Server Compact. |
| API d'image Windows 6.0.6001.18000 | Requis pour permettre à Configuration Manager de gérer les fichiers image Windows (.wim). |
| Microsoft Policy Platform 1.2.3514.0 | Requis pour autoriser les clients à évaluer les paramètres de conformité. |
| Microsoft Silverlight 5.1.41212.0 | Requis pour prendre en charge l'expérience utilisateur du site Web du catalogue d'applications. Depuis Configuration Manager 1802, Silverlight n'est plus installé automatiquement. La fonctionnalité principale du catalogue des applications est désormais incluse dans le Centre logiciel. La prise en charge du site web du catalogue des applications prend fin avec la première mise à jour publiée après le 1er juin 2018. |
| Microsoft .NET Framework version 4.5.2. | Requis pour prendre en charge les opérations de clients. Installé automatiquement sur l'ordinateur client si le Microsoft .NET Framework 4.5 ou version ultérieure n'est pas installé. Pour plus d'informations, consultez Détails supplémentaires sur Microsoft .NET Framework version 4.5.2. |
| Composants Microsoft SQL Server Compact 3.5 SP2 | Requis pour conserver les informations liées aux opérations du client. |
| Microsoft Windows Imaging Components | Requis par Microsoft .NET Framework 4.0 pour Windows Server 2003 ou Windows XP SP2 pour les ordinateurs 64 bits. |

| | |
|---|---|
| Client logiciel PC Microsoft Intune | Vous ne pouvez pas exécuter le client logiciel Intune PC et le client Configuration Manager sur le même ordinateur. Assurez-vous que le client Intune a été supprimé avant d'installer le client Configuration Manager. |

**Informations supplémentaires sur Microsoft .NET Framework version 4.5.2**

> **NOTE**
> Le 12 janvier 2016, la prise en charge de .NET 4.0, 4.5 et 4.5.1 a expiré. Pour plus d'informations, consultez Questions fréquentes (FAQ) sur la politique de support - Microsoft .NET Framework.

Un redémarrage peut être nécessaire pour achever l'installation de Microsoft .NET Framework version 4.5.2. Une notification **Redémarrage requis** s'affiche dans la barre d'état système. Scénarios courants qui nécessitent le redémarrage des ordinateurs clients :

- Des services ou des applications .NET sont en cours d'exécution sur l'ordinateur.
- Il manque une ou plusieurs mises à jour logicielles nécessaires pour l'installation de .NET.
- L'ordinateur doit être redémarré suite à une précédente installation de mises à jour logicielles du .NET Framework.

  Après l'installation du .NET Framework 4.5.2, des mises à jour supplémentaires peuvent être installées par la suite et nécessiter des redémarrages de l'ordinateur.

### Dépendances de Configuration Manager

Pour plus d'informations, consultez Déterminer les rôles système de site pour les clients.

| | |
|---|---|
| Point de gestion | Un point de gestion n'est pas nécessaire pour déployer le client Configuration Manager, mais il l'est pour transférer des informations entre les ordinateurs clients et les serveurs Configuration Manager. Sans point de gestion, vous ne pouvez pas gérer les ordinateurs clients. |
| Point de distribution | Le point de distribution est un rôle de système de site facultatif, mais recommandé dans le cadre du déploiement de clients. Tous les points de distribution hébergent les fichiers sources du client, ce qui permet aux ordinateurs de trouver le point de distribution le plus proche d'où ils peuvent télécharger ces fichiers sources au cours du déploiement du client. Si le site ne possède pas de point de distribution, les ordinateurs téléchargent les fichiers sources du client auprès de leur point de gestion. |
| Point d'état de secours | Le point d'état de secours est un rôle de système de site facultatif, mais recommandé dans le cadre du déploiement de clients. Le point d'état de secours surveille le déploiement des clients et permet aux ordinateurs du site Configuration Manager d'envoyer des messages d'état quand ils ne peuvent pas communiquer avec un point de gestion. |

| | |
|---|---|
| Point de Reporting Services | Le point de Reporting Services est un rôle de système de site, facultatif mais recommandé, qui peut afficher des rapports liés au déploiement et à la gestion du client. Pour plus d'informations, consultez Génération de rapports dans System Center Configuration Manager. |

### Dépendances liées aux méthodes d'installation

Les conditions requises suivantes sont spécifiques aux différentes méthodes d'installation du client.

#### Installation poussée du client

- Les comptes d'installation poussée du client sont utilisés pour se connecter aux ordinateurs pour l'installation du client et sont spécifiés dans l'onglet **Comptes** de la boîte de dialogue **Propriétés de l'installation poussée du client** . Le compte doit être membre du groupe d'administrateurs local sur l'ordinateur de destination.

  Si vous ne spécifiez pas de compte d'installation Push du client, le compte d'ordinateur du serveur de site est utilisé.

- L'ordinateur sur lequel vous installez le client doit avoir été découvert par au moins une méthode de découverte de Configuration Manager.
- L'ordinateur dispose d'un partage ADMIN$.
- L'option **Activer l'installation push du client aux ressources attribuées** doit être sélectionnée dans la boîte de dialogue **Propriétés de l'installation push du client** si vous souhaitez transférer (push) automatiquement le client Configuration Manager vers les ressources découvertes.
- L'ordinateur client doit être capable de contacter un point de distribution ou un point de gestion pour télécharger les fichiers de prise en charge.

Vous devez disposer des autorisations de sécurité suivantes pour installer le client Configuration Manager à l'aide de l'installation push du client :

- Pour configurer le compte d'installation poussée du client : autorisation **Modifier** et Lire pour l'objet **Site** .
- Pour utiliser l'installation poussée du client pour installer le client sur les regroupements, les appareils et les requêtes : autorisation **Modifier la ressource** et **Lire** pour l'objet Collection.

Le rôle de sécurité **Administrateur d'infrastructure** comprend les autorisations requises pour la gestion de l'installation poussée du client.

#### Installation basée sur un point de mise à jour logicielle

- Si le schéma Active Directory n'a pas été étendu ou si vous installez des clients à partir d'une autre forêt, les propriétés d'installation de CCMSetup.exe doivent être configurées dans le Registre de l'ordinateur à l'aide d'une stratégie de groupe. Pour plus d'informations, consultez Comment fournir des propriétés d'installation du client (installation basée sur une stratégie de groupe et sur les mises à jour logicielles).
- Le client Configuration Manager doit être publié sur le point de mise à jour logicielle.
- L'ordinateur client doit être capable de contacter un point de distribution ou un point de gestion pour télécharger les fichiers de prise en charge.

Pour en savoir plus sur les autorisations de sécurité nécessaires à la gestion des mises à jour logicielles Configuration Manager, consultez Prérequis pour les mises à jour logicielles.

#### Installation basée sur une stratégie de groupe

- Si le schéma Active Directory n'a pas été étendu ou si vous installez des clients à partir d'une autre forêt, les propriétés d'installation de CCMSetup.exe doivent être configurées dans le Registre de l'ordinateur à l'aide

d'une stratégie de groupe. Pour plus d'informations, consultez Comment fournir des propriétés d'installation du client (installation basée sur une stratégie de groupe et sur les mises à jour logicielles).

- L'ordinateur client doit être en mesure de contacter un point de gestion pour télécharger les fichiers de prise en charge.

**Installation basée sur un script d'ouverture de session**

L'ordinateur client doit être capable de contacter un point de distribution ou un point de gestion pour télécharger les fichiers de prise en charge. Sauf si vous avez spécifié CCMSetup.exe avec la propriété de ligne de commande **ccmsetup/source**.

**Installation manuelle**

L'ordinateur client doit être capable de contacter un point de distribution ou un point de gestion pour télécharger les fichiers de prise en charge. Sauf si vous avez spécifié CCMSetup.exe avec la propriété de ligne de commande **ccmsetup/source**.

**Installation de Microsoft Intune MDM**

- Nécessite un abonnement Microsoft Intune et les licences appropriées.
- Nécessite un appareil disposant d'un accès à Internet, même s'il n'est pas basé sur internet.
- Selon le cas d'utilisation, peut aussi nécessiter l'une des deux technologies suivantes (ou les deux à la fois) :
  - Azure Active Directory
  - Passerelle de gestion cloud

**Installation d'ordinateurs d'un groupe de travail**

Pour accéder aux ressources du domaine du serveur de site Configuration Manager, le compte d'accès réseau doit être configuré pour le site.

Pour plus d'informations sur la configuration du compte d'accès réseau, consultez Concepts fondamentaux de la gestion de contenu.

**Installation basée sur la distribution de logiciels (pour les mises à niveau uniquement)**

- Si le schéma Active Directory n'a pas été étendu ou si vous installez des clients à partir d'une autre forêt, les propriétés d'installation de CCMSetup.exe doivent être configurées dans le Registre de l'ordinateur à l'aide d'une stratégie de groupe. Pour plus d'informations, consultez Comment fournir des propriétés d'installation du client (installation basée sur une stratégie de groupe et sur les mises à jour logicielles).
- L'ordinateur client doit être capable de contacter un point de distribution ou un point de gestion pour télécharger les fichiers de prise en charge.

Pour en savoir plus sur les autorisations de sécurité nécessaires à la mise à niveau du client Configuration Manager à l'aide de la gestion d'applications, consultez Sécurité et confidentialité pour la gestion des applications.

**Mises à niveau automatiques des clients**

Vous devez avoir le rôle de sécurité **Administrateur complet** pour pouvoir configurer des mises à niveau automatiques des clients.

### Configuration requise du pare-feu

S'il existe un pare-feu entre les serveurs du système de site et les ordinateurs sur lesquels vous souhaitez installer le client Configuration Manager, consultez Paramètres de port et de pare-feu Windows pour les clients.

## Prérequis pour les appareils mobiles clients

Quand vous installez le client Configuration Manager sur des appareils mobiles et que vous les inscrivez, servez-vous de ces informations pour déterminer les prérequis.

**Dépendances externes à Configuration Manager**

- Autorité de certification d'entreprise Microsoft avec des modèles de certificats pour déployer et gérer les certificats requis pour les appareils mobiles.

  L'autorité de certification émettrice doit automatiquement approuver les demandes de certificat de la part d'utilisateurs d'appareils mobiles lors du processus d'inscription.

  Pour plus d'informations sur la configuration requise pour les certificats, consultez Sécurité et confidentialité pour les profils de certificat.

- Groupe de sécurité qui contient les utilisateurs pouvant inscrire leurs appareils mobiles.

  Ce groupe de sécurité est utilisé pour configurer le modèle de certificat utilisé lors de l'inscription d'appareils mobiles.

- Facultatif mais recommandé : un alias DNS (enregistrement CNAME) nommé **ConfigMgrEnroll**. Configurez cet alias pour le nom de serveur du point proxy d'inscription.

  Cet alias DNS est nécessaire à la prise en charge de la découverte automatique pour le service d'inscription. Si vous ne configurez pas cet enregistrement DNS, les utilisateurs doivent spécifier manuellement le nom du point proxy d'inscription pendant le processus d'inscription.

- Dépendances du rôle système de site pour les ordinateurs qui exécutent les rôles système de site point d'inscription et point proxy d'inscription.

  Consultez Systèmes d'exploitation pris en charge pour les serveurs de système de site.

**Dépendances de Configuration Manager**

Pour plus d'informations, consultez Déterminer les rôles système de site pour les clients.

- Point de gestion configuré pour les connexions client HTTPS et activé pour les appareils mobiles

  Un point de gestion est toujours nécessaire pour installer le client Configuration Manager sur des appareils mobiles. En plus des exigences de configuration et d'activation de HTTPS pour les appareils mobiles, le point de gestion doit être configuré avec un nom de domaine complet Internet et accepter les connexions client en provenance d'Internet.

- Point d'inscription et point proxy d'inscription

  Un point proxy d'inscription gère les demandes d'inscription de la part d'appareils mobiles et le point d'inscription termine le processus d'inscription. Le point d'inscription doit être dans la même forêt Active Directory que le serveur de site, mais le point proxy d'inscription peut être dans une autre forêt.

- Paramètres client pour l'inscription d'appareils mobiles

  Configurez des paramètres client pour permettre aux utilisateurs d'inscrire des appareils mobiles et de configurer au moins un profil d'inscription.

- Point de Reporting Services

  Le point de Reporting Services est un rôle de système de site, facultatif mais recommandé, qui peut afficher des rapports liés à l'inscription d'appareils mobiles et à la gestion de clients.

  Pour plus d'informations, consultez Génération de rapports dans System Center Configuration Manager.

- Pour configurer l'inscription pour les appareils mobiles, vous devez disposer des autorisations de sécurité suivantes :

  - Pour ajouter, modifier et supprimer les rôles de système de site d'inscription : autorisation **Modifier** pour l'objet **Site** .

- Pour configurer les paramètres clients de l'inscription : les paramètres clients par défaut nécessitent l'autorisation **Modifier** pour l'objet **Site** et les paramètres clients personnalisés nécessitent des autorisations **Agent client** .

  Le rôle de sécurité **Administrateur complet** comprend les autorisations requises pour configurer les rôles de système de site d'inscription.

  Pour gérer des appareils mobiles inscrits, vous devez disposer des autorisations de sécurité suivantes :

- Pour réinitialiser ou retirer un appareil mobile : **Supprimer la ressource** pour l'objet **Collection** .
- Pour annuler une réinitialisation ou retirer une commande : **Supprimer la ressource** pour l'objet **Collection** .
- Pour autoriser et bloquer des appareils mobiles : **Modifier la ressource** pour l'objet **Collection** .
- Pour verrouiller à distance ou réinitialiser le mot de passe sur un appareil mobile : **Modifier la ressource** pour l'objet **Collection** .

  Le rôle de sécurité **Administrateur d'opérations** comprend les autorisations nécessaires pour la gestion des appareils mobiles.

  Pour plus d'informations sur la configuration des autorisations de sécurité, consultez Principes de base de l'administration basée sur des rôles et Configurer l'administration basée sur des rôles.

**Configuration requise du pare-feu**

Les appareils réseau intervenants, tels que des routeurs et des pare-feu, ainsi que le Pare-feu Windows, le cas échéant, doivent autoriser le trafic associé à l'inscription d'appareils mobiles :

- Entre les appareils mobiles et le point proxy d'inscription : HTTPS (par défaut, TCP 443)
- Entre le point proxy d'inscription et le point d'inscription : HTTPS (par défaut, TCP 443)

Si vous utilisez un serveur Web proxy, il doit être configuré pour un tunnel SSL. Le pontage SSL n'est pas pris en charge pour les appareils mobiles.

# Paramètres de port et de pare-feu Windows pour les clients dans System Center Configuration Manager

22/06/2018 • 18 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Dans System Center Configuration Manager, les ordinateurs clients qui exécutent le Pare-feu Windows exigent souvent que des exceptions soient configurées pour permettre la communication avec leur site. Les exceptions que vous devez configurer dépendent des fonctionnalités de gestion que vous utilisez avec le client Configuration Manager.

Utilisez les sections suivantes pour identifier ces fonctionnalités de gestion et pour obtenir plus d'informations sur la configuration du Pare-feu Windows pour ces exceptions.

## Modification des ports et programmes autorisés par le Pare-feu Windows

Utilisez la procédure suivante pour modifier les ports et les programmes sur le Pare-feu Windows pour le client Configuration Manager.

**Pour modifier les ports et programmes autorisés par le Pare-feu Windows**

1. Sur l'ordinateur exécutant le Pare-feu Windows, ouvrez le Panneau de configuration.
2. Cliquez avec le bouton droit sur **Pare-feu Windows**, puis cliquez sur **Ouvrir**.
3. Configurez toutes les exceptions nécessaires et tous les programmes et ports personnalisés dont vous avez besoin.

## Programmes et ports dont Configuration Manager a besoin

Les fonctionnalités de Configuration Manager suivantes nécessitent des exceptions sur le Pare-feu Windows :

### Requêtes

Si vous exécutez la console Configuration Manager sur un ordinateur qui exécute le Pare-feu Windows, les requêtes échouent à leur première exécution et le système d'exploitation affiche une boîte de dialogue vous demandant si vous voulez débloquer statview.exe. Si vous débloquez statview.exe, les requêtes ultérieures s'exécuteront sans erreur. Vous pouvez également ajouter manuellement le fichier Statview.exe à la liste des programmes et services dans l'onglet **Exceptions** du Pare-feu Windows avant d'exécuter une requête.

### Installation poussée du client

Pour procéder à une installation Push du client Configuration Manager, ajoutez les éléments suivants en tant qu'exceptions au Pare-feu Windows :

- Entrant et sortant : **Partage de fichiers et d'imprimantes**
- Entrant : **Windows Management Instrumentation (WMI)**

### Installation du client à l'aide de la stratégie de groupe

Pour installer le client Configuration Manager à l'aide de la stratégie de groupe, ajoutez **Partage de fichiers et d'imprimantes** en tant qu'exception au Pare-feu Windows.

### Requêtes client

Pour permettre aux ordinateurs clients de communiquer avec les systèmes de site Configuration Manager, ajoutez les éléments suivants en tant qu'exceptions au Pare-feu Windows :

Sortant : Port TCP **80** (pour communications HTTP)

Sortant : Port TCP **443** (pour communications HTTPS)

> **IMPORTANT**
> Ces numéros de port sont les valeurs par défaut. Elles peuvent être modifiées dans Configuration Manager. Pour plus d'informations, consultez Guide pratique pour configurer les ports de communication des clients dans System Center Configuration Manager. Si ces ports ont été modifiés par rapport aux valeurs par défaut, vous devez également configurer des exceptions correspondantes pour le Pare-feu Windows.

**Notification du client**

Pour que le point de gestion signale aux ordinateurs clients les actions qu'ils doivent entreprendre quand un utilisateur administratif sélectionne une action de client dans la console Configuration Manager (téléchargement d'une stratégie d'ordinateur, démarrage d'une recherche de programmes malveillants, etc.), ajoutez l'exception suivante au Pare-feu Windows :

Sortant : Port TCP **10123**

Si la communication n'aboutit pas, Configuration Manager recommence automatiquement à utiliser le port de communication HTTP ou HTTPS existant entre le client et le point de gestion :

Sortant : Port TCP **80** (pour communications HTTP)

Sortant : Port TCP **443** (pour communications HTTPS)

> **IMPORTANT**
> Ces numéros de port sont les valeurs par défaut. Elles peuvent être modifiées dans Configuration Manager. Pour plus d'informations, consultez Guide pratique pour configurer les ports de communication des clients dans System Center Configuration Manager. Si ces ports ont été modifiés par rapport aux valeurs par défaut, vous devez également configurer des exceptions correspondantes pour le Pare-feu Windows.

**Contrôle à distance**

Pour utiliser la fonctionnalité de contrôle à distance de Configuration Manager, autorisez le port suivant :

- Entrant : Port TCP**2701**

**Assistance à distance et Bureau à distance**

Pour lancer l'assistance à distance à partir de la console Configuration Manager, ajoutez le programme personnalisé **Helpsvc.exe** et le port personnalisé entrant TCP **135** à la liste des programmes et services autorisés dans le Pare-feu Windows de l'ordinateur client. Vous devez également autoriser l' **Assistance à distance** et le **Bureau à distance**. Si vous lancez l'assistance à distance depuis l'ordinateur client, le Pare-feu Windows configure et autorise automatiquement l' **Assistance à distance** et le **Bureau à distance**.

**Proxy de mise en éveil**

Si vous activez le paramètre client du proxy de mise en éveil, un nouveau service appelé ConfigMgr Wake-up Proxy utilise un protocole pair à pair pour savoir si d'autres ordinateurs du sous-réseau sont en éveil et pour les mettre en éveil, le cas échéant. Cette communication utilise les ports suivants :

Sortant : Port UDP **25536**

Sortant : Port UDP **9**

Ces numéros correspondent aux ports par défaut qui peuvent être modifiés dans Configuration Manager en utilisant les paramètres client de **Gestion de l'alimentation** appelés **Numéro de port du proxy de mise en éveil (UDP)** et **Numéro de port Wake On LAN (UDP)**. Si vous spécifiez le paramètre client **Gestion de l'alimentation**: **Exception du Pare-feu Windows pour le proxy de mise en éveil** , ces ports sont configurés automatiquement dans le Pare-feu Windows des clients. Toutefois, si les clients exécutent un autre pare-feu, vous devez configurer manuellement les exceptions pour ces numéros de port.

En plus de ces ports, le proxy de mise en éveil utilise également des messages de demande d'écho ICMP (Internet Control Message Protocol) entre un ordinateur client et un autre ordinateur client. Cette communication permet de savoir si l'autre ordinateur client est en éveil sur le réseau. ICMP est parfois appelé commandes ping TCP/IP.

Pour plus d'informations sur le proxy de mise en éveil, consultez Planifier la sortie de veille des clients dans System Center Configuration Manager.

**Observateur d'événements de Windows, Analyseur de performances de Windows et Diagnostics Windows**

Pour accéder à l'Observateur d'événements Windows, à l'Analyseur de performances Windows et à Diagnostics Windows à partir de la console Configuration Manager, activez **Partage de fichiers et d'imprimantes** en tant qu'exception sur le Pare-feu Windows.

## Ports utilisés lors du déploiement du client de Configuration Manager

Les tableaux suivants référencent les ports utilisés lors du processus d'installation du client.

> **IMPORTANT**
> S'il existe un pare-feu entre les serveurs de système de site et l'ordinateur client, confirmez si le pare-feu autorise le trafic pour les ports requis pour la méthode d'installation du client que vous avez choisie. Par exemple, les pare-feu causent souvent l'échec d'une installation poussée du client car ils bloquent le protocole SMB et les appels de procédure distante (RPC). Dans ce cas, utilisez une méthode d'installation du client différente, telle que l'installation manuelle (en exécutant CCMSetup.exe) ou l'installation du client basée sur une stratégie de groupe. Ces méthodes alternatives d'installation du client ne nécessitent pas de protocole SMB ou RPC.

Pour plus d'informations sur la configuration du Pare-feu Windows sur l'ordinateur client, voir la section Modification des ports et programmes autorisés par le Pare-feu Windows.

**Ports utilisés pour toutes les méthodes d'installation**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| Protocole HTTP (Hypertext Transfer) à partir de l'ordinateur client vers un point d'état de secours, lorsqu'un point d'état de secours est affecté au client. | -- | 80 (Voir remarque 1, **Port alternatif disponible**) |

**Ports utilisés avec l'installation poussée du client**

Outre les ports répertoriés dans le tableau ci-après, l'installation poussée du client utilise également les messages de demande echo Internet Control Message Protocol (ICMP) à partir du serveur du site vers l'ordinateur client pour vérifier si l'ordinateur client est disponible sur le réseau. ICMP est parfois appelé commandes ping TCP/IP. ICMP ne dispose pas d'un numéro de protocole UDP ou TCP, et par conséquent, il ne figure pas dans le tableau suivant. Toutefois, tous les périphériques réseau concernés, tels que les pare-feux, doivent autoriser le trafic ICMP pour l'installation poussée du client.

| DESCRIPTION | UDP | TCP |
|---|---|---|
| Server Message Block (SMB) entre le serveur de site et l'ordinateur client. | -- | 445 |
| Mappeur de point de terminaison RPC entre le serveur de site et l'ordinateur client. | 135 | 135 |
| Ports dynamiques RPC entre le serveur de site et l'ordinateur client. | -- | DYNAMIC |
| Protocole HTTP depuis l'ordinateur client vers un point de gestion lorsque la connexion est effectuée via HTTP. | -- | 80 (Voir remarque 1, **Port alternatif disponible**) |
| Protocole HTTPS depuis l'ordinateur client vers un point de gestion lorsque la connexion est effectuée via HTTPS. | -- | 443 (Voir remarque 1, **Port alternatif disponible**) |

### Ports utilisés avec l'installation basée sur le point de mise à jour logicielle

| DESCRIPTION | UDP | TCP |
|---|---|---|
| Protocole HTTP (Hypertext Transfer Protocol) à partir de l'ordinateur client vers le point de mise à jour logicielle. | -- | 80 ou 8530 (Voir remarque 2, **Windows Server Update Services**) |
| Protocole HTTPS (Secure Hypertext Transfer Protocol) à partir de l'ordinateur client vers le point de mise à jour logicielle. | -- | 443 ou 8531 (Voir remarque 2, **Windows Server Update Services**) |
| SMB (Server Message Block) entre le serveur source et l'ordinateur client quand vous spécifiez la propriété de ligne de commande CCMSetup **/source:<Chemin>**. | -- | 445 |

### Ports utilisés avec l'installation basée sur une stratégie de groupe

| DESCRIPTION | UDP | TCP |
|---|---|---|
| Protocole HTTP depuis l'ordinateur client vers un point de gestion lorsque la connexion est effectuée via HTTP. | -- | 80 (Voir remarque 1, **Port alternatif disponible**) |
| Protocole HTTPS depuis l'ordinateur client vers un point de gestion lorsque la connexion est effectuée via HTTPS. | -- | 443 (Voir remarque 1, **Port alternatif disponible**) |
| SMB (Server Message Block) entre le serveur source et l'ordinateur client quand vous spécifiez la propriété de ligne de commande CCMSetup **/source:<Chemin>**. | -- | 445 |

### Ports utilisés avec l'installation manuelle et l'installation basée sur un script d'ouverture de session

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SMB (Server Message Block) entre l'ordinateur client et un partage réseau à partir duquel vous exécutez CCMSetup.exe.<br><br>Quand vous installez Configuration Manager, les fichiers sources d'installation du client sont copiés et partagés automatiquement à partir du dossier <*Chemin_Installation*> \Client sur les points de gestion. Toutefois, vous pouvez copier ces fichiers et créer un nouveau partage sur n'importe quel ordinateur du réseau. Vous pouvez également éliminer ce trafic réseau en exécutant CCMSetup.exe localement, par exemple, à l'aide d'un support amovible. | -- | 445 |
| Protocole HTTP de l'ordinateur client vers un point de gestion quand la connexion est effectuée via HTTP et que vous ne spécifiez pas la propriété de ligne de commande CCMSetup **/source:<Chemin>**. | -- | 80 (Voir remarque 1, **Port alternatif disponible**) |
| Protocole HTTPS de l'ordinateur client vers un point de gestion quand la connexion est effectuée via HTTPS et que vous ne spécifiez pas la propriété de ligne de commande CCMSetup **/source:<Chemin>**. | -- | 443 (Voir remarque 1, **Port alternatif disponible**) |
| SMB (Server Message Block) entre le serveur source et l'ordinateur client quand vous spécifiez la propriété de ligne de commande CCMSetup **/source:<Chemin>**. | -- | 445 |

**Ports utilisés avec l'installation basée sur la distribution de logiciels**

| DESCRIPTION | UDP | TCP |
|---|---|---|
| SMB (Server Message Block) entre le point de distribution et l'ordinateur client. | -- | 445 |
| Protocole HTTP depuis le client vers un point de distribution lorsque la connexion est effectuée via HTTP. | -- | 80 (Voir remarque 1, **Port alternatif disponible**) |
| Protocole HTTPS depuis le client vers un point de distribution lorsque la connexion est effectuée via HTTPS. | -- | 443 (Voir remarque 1, **Port alternatif disponible**) |

# Remarques

**Port alternatif disponible** Dans Configuration Manager, vous pouvez définir un port alternatif pour cette valeur. Si un port personnalisé a été défini, remplacez-le quand vous définissez les informations de filtre IP pour les stratégies IPsec ou pour la configuration de pare-feu.

**2 Windows Server Update Services** Vous pouvez installer Windows Server Update Services (WSUS) sur le site Web par défaut (port 80) ou sur un site Web personnalisé (port 8530).

Après l'installation, vous pouvez modifier le port. Vous n'avez pas à utiliser le même numéro de port dans l'ensemble de la hiérarchie du site.

Si le numéro de port HTTP est 80, le numéro de port HTTPS doit être 443.

S'il s'agit d'un autre numéro de port HTTP, le numéro de port HTTPS doit être supérieur de 1 (par exemple, 8530 et 8531).

# Déterminer les rôles de système de site pour les clients System Center Configuration Manager

22/06/2018 • 11 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cette rubrique peut vous aider à déterminer les rôles de système de site dont vous avez besoin pour déployer les clients Configuration Manager :

Pour plus d'informations sur l'emplacement d'installation des rôles de système de site requis dans la hiérarchie, consultez Concevoir une hiérarchie de sites pour System Center Configuration Manager.

Pour plus d'informations sur l'installation et la configuration des rôles de système de site dont vous avez besoin, consultez Installer des rôles de système de site.

## Déterminer si vous avez besoin d'un point de gestion

Par défaut, tous les ordinateurs clients Windows utilisent un point de distribution pour installer le client Configuration Manager. En cas d'indisponibilité du point de distribution, ils peuvent basculer sur un point de gestion. Toutefois, vous pouvez installer des clients Windows sur les ordinateurs à partir d'une autre source, en utilisant la propriété de ligne de commande CCMSetup **/source:<chemin_accès>**. Par exemple, ceci peut être approprié si vous installez des clients sur Internet. Un autre scénario est d'éviter l'envoi des paquets réseau entre les ordinateurs et le point de gestion lors de l'installation du client, par exemple car un pare-feu bloque les ports nécessaires ou que vous disposez d'une connexion à faible bande passante. Tous les clients doivent cependant communiquer avec un point de gestion à affecter à un site et pour être gérés par Configuration Manager.

Pour plus d'informations sur la propriété de ligne de commande CCMSetup **/source:<chemin_accès>**, consultez À propos des propriétés d'installation du client dans System Center Configuration Manager.

Quand vous installez plusieurs points de gestion dans la hiérarchie, les clients se connectent automatiquement à une seul point en fonction des forêts auxquelles ils appartiennent et de leur emplacement réseau. Vous ne pouvez pas installer plusieurs points de gestion dans un site secondaire.

Les ordinateurs clients Mac et les clients d'appareil mobile que vous inscrivez à l'aide de Configuration Manager nécessitent dans tous les cas un point de gestion pour l'installation du client. Ce point de gestion doit se trouver dans un site principal. Il doit en outre être configuré pour prendre en charge les appareils mobiles et doit accepter les connexions de clients via Internet. Ces clients ne peuvent pas utiliser les points de gestion des sites secondaires ni se connecter aux points de gestion d'autres sites principaux.

## Déterminer si un point d'état de secours est nécessaire

Vous pouvez utiliser un point d'état de secours pour surveiller le déploiement du client pour les ordinateurs Windows. Vous pouvez également identifier les ordinateurs clients Windows qui ne sont pas gérés car ils ne peuvent pas communiquer avec un point de gestion. Les ordinateurs Mac, les appareils mobiles inscrits par le biais de Configuration Manager et les appareils mobiles gérés à l'aide du connecteur du serveur Exchange Server n'utilisent pas de point d'état de secours.

Un point d'état de secours n'est pas nécessaire pour surveiller l'activité et l'intégrité du client.

Le point d'état de secours communique toujours avec les clients via HTTP, qui utilise des connexions non authentifiées et envoie les données en texte clair. Ainsi, le point d'état de secours est vulnérable aux attaques, en particulier lorsqu'il est utilisé avec la gestion de clients basés sur Internet. Pour réduire la surface d'attaque, dédiez

toujours un serveur à l'exécution du point d'état de secours et n'installez aucun autre rôle de système de site sur le même serveur, dans un environnement de production.

Installez un point d'état de secours si tout ce qui suit s'applique :

- Vous souhaitez que les erreurs de communication avec les clients des ordinateurs Windows soient envoyées au site, même si ces ordinateurs clients ne peuvent pas communiquer avec un point de gestion.
- Vous souhaitez utiliser les rapports de déploiement de client Configuration Manager, qui contiennent les données envoyées par le point d'état de secours.
- Vous disposez d'un serveur dédié pour ce rôle de système de site et avez en outre mis en place des mesures de sécurité pour renforcer la protection du serveur contre les attaques.
- Les avantages que présentent l'utilisation d'un point d'état de secours compensent les risques de sécurité liés aux connexions non authentifiées et aux transferts de texte en clair, sur du trafic HTTP.

  N'installez pas un point d'état de secours si les risques de sécurité liés à l'exécution d'un site web avec des connexions non authentifiées et des transferts de texte en clair dépassent les avantages de l'identification des problèmes de communication du client.

## Déterminer si un point Reporting Services est nécessaire

Configuration Manager fournit de nombreux rapports pour vous aider à surveiller l'installation, l'attribution et la gestion des clients sur la console Configuration Manager. Certains rapports sur le déploiement du client exigent que des clients soient attribués à un point d'état de secours.

Même si les rapports ne sont pas nécessaires pour déployer des clients et si vous pouvez consulter des informations sur le déploiement dans la console Configuration Manager ou des informations détaillées dans les fichiers journaux du client, les rapports du client donnent des informations importantes pour vous aider à surveiller et à résoudre les problèmes de déploiement du client.

## Déterminer si un point d'inscription et un point proxy d'inscription sont nécessaires

Configuration Manager a besoin du point d'inscription et du point proxy d'inscription pour inscrire les appareils mobiles et les certificats des ordinateurs Mac. Ces rôles de système de site ne sont pas nécessaires dans les trois cas suivants : si vous avez l'intention de gérer les appareils mobiles à l'aide du connecteur du serveur Exchange Server, si vous installez le client d'appareil mobile hérité (par exemple Windows CE), ou si vous demandez et installez le certificat client sur des ordinateurs Mac indépendamment de Configuration Manager.

## Déterminer si un point de distribution est nécessaire

Vous n'avez pas besoin d'un point de distribution pour installer les clients Configuration Manager sur les ordinateurs Windows. Cependant, par défaut, Configuration Manager utilise un point de distribution pour installer les fichiers sources du client sur ces ordinateurs. Si nécessaire, il peut également télécharger ces fichiers à partir d'un point de gestion. Les points de distribution ne sont pas utilisés pour installer des clients d'appareils mobiles qui sont inscrits auprès de Configuration Manager, mais ils sont utilisés si vous installez le client hérité de l'appareil mobile. Si vous installez le client Configuration Manager dans le cadre d'un déploiement de système d'exploitation, l'image du système d'exploitation est stockée et récupérée à partir d'un point de distribution.

Bien que les points de distribution ne soient pas indispensables pour installer la plupart des clients Configuration Manager, vous en avez besoin pour installer des logiciels comme des applications et des mises à jour logicielles sur les clients.

## Déterminer si un point du site web du catalogue des applications et un point de service web du catalogue des applications sont nécessaires

Le point du site web du catalogue des applications et le point de service web du catalogue des applications ne sont pas nécessaires pour le déploiement du client. Cependant, il peut être utile de les installer dans le cadre du processus de déploiement des clients, pour que les utilisateurs puissent effectuer les actions suivantes dès que le client Configuration Manager est installé sur les ordinateurs Windows :

- Réinitialiser les appareils mobiles.
- Recherchez et installez des applications à partir du catalogue d'applications.
- Déployez des applications auprès des utilisateurs et des appareils en utilisant l'objet de déploiement **Disponible**.

## Déterminer si un point de connecteur de passerelle de gestion cloud est nécessaire

Vous avez besoin d'un point de connecteur de passerelle de gestion cloud si vous configurez une passerelle de gestion cloud pour gérer les clients sur Internet.

# Sécurité et confidentialité pour les clients dans System Center Configuration Manager

22/06/2018 • 50 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cet article contient des informations de sécurité et de confidentialité pour les clients de System Center Configuration Manager et pour les appareils mobiles qui sont gérés par le connecteur Exchange Server :

## Bonnes pratiques de sécurité pour les clients

Quand Configuration Manager accepte les données provenant d'appareils qui exécutent le client Configuration Manager, il existe un risque que les clients attaquent le site. Par exemple, ils pourraient envoyer un inventaire incorrect ou tenter de surcharger les systèmes de site. Déployez le client Configuration Manager uniquement sur les appareils auxquels vous faites confiance. En outre, utilisez les meilleures pratiques de sécurité suivantes pour contribuer à protéger le site des appareils non autorisés ou compromis :

**Utilisez des certificats d'infrastructure à clé publique (PKI) pour les communications client avec les systèmes de site exécutant IIS.**

- Comme propriété de site, configurez **Paramètres du système de site** pour **HTTPS uniquement**.
- Installer des clients avec la propriété CCMSetup **/UsePKICert**
- Utilisez une liste de révocation de certificats (CRL) et assurez-vous que les clients et les serveurs qui communiquent peuvent toujours y accéder.

  Ces certificats sont requis pour les clients des appareils mobiles et pour les connexions d'ordinateurs clients sur Internet et, à l'exception des points de distribution, ils sont recommandés pour toutes les connexions client sur l'Intranet.

  Pour plus d'informations sur les spécifications requises des certificats PKI et comment ils sont utilisés pour protéger Configuration Manager, voir Configuration requise des certificats PKI pour System Center Configuration Manager.

  **Approuver automatiquement les ordinateurs clients à partir de domaines approuvés et vérifier et approuver manuellement d'autres ordinateurs**

  Vous pouvez configurer l'approbation pour la hiérarchie comme manuelle, automatique pour les ordinateurs de domaines approuvés ou automatique pour tous les ordinateurs. La méthode d'approbation la plus sûre consiste à approuver automatiquement les clients qui sont membres de domaines approuvés, puis à vérifier et approuver manuellement tous les autres ordinateurs. Il n'est pas recommandé d'approuver automatiquement tous les clients, sauf si vous disposez d'autres contrôles d'accès pour empêcher l'accès des ordinateurs non approuvés à votre réseau.

  L'approbation identifie un ordinateur dont vous approuvez la gestion par Configuration Manager lorsque vous ne pouvez pas utiliser l'authentification PKI.

  Pour plus d'informations sur l'approbation manuelle des ordinateurs, voir Gérer les clients à partir du nœud Appareils.

  **Ne vous fiez pas au blocage pour empêcher certains clients d'accéder à la hiérarchie Configuration Manager**

L'infrastructure Configuration Manager rejette les clients bloqués afin qu'ils ne puissent pas communiquer avec les systèmes de site pour télécharger la stratégie, charger les données d'inventaire ou envoyer des messages d'état. Toutefois, ne vous fiez pas au blocage pour protéger la hiérarchie Configuration Manager des ordinateurs non approuvés lorsque des systèmes de site acceptent les connexions client HTTP. Dans ce scénario, un client bloqué peut se reconnecter au site avec un nouveau certificat auto-signé et un nouvel ID de matériel. Ce blocage vise à bloquer le support de démarrage perdu ou compromis pendant le déploiement d'un système d'exploitation sur des clients et quand tous les systèmes de site acceptent des connexions client HTTPS. Si vous utilisez une infrastructure à clés publiques (PKI) et si elle prend en charge une liste de révocation de certificats, envisagez toujours de définir la révocation de certificats comme première ligne de défense contre les certificats potentiellement compromis. Le blocage des clients dans Configuration Manager fournit une seconde ligne de défense pour protéger votre hiérarchie.

Pour plus d'informations, voir Déterminer si des clients doivent être bloqués dans System Center Configuration Manager.

**Utilisez les méthodes d'installation de client plus sécurisées qui sont pratiques pour votre environnement :**

- Pour les ordinateurs du domaine, les méthodes d'installation du client de la stratégie de groupe et les méthodes d'installation du client basé sur des mises à jour sont plus sûres que l'installation poussée du client.
- L'acquisition d'images et l'installation manuelle peuvent être très sûres si vous appliquez des contrôles d'accès et modifiez des contrôles.

  Parmi toutes les méthodes d'installation des clients, l'installation poussée du client est la moins sûre en raison des nombreuses dépendances qu'elle possède, notamment les autorisations d'administrateur local, le partage Admin$ et de nombreuses exceptions de pare-feu. Ces dépendances augmentent votre surface d'attaque.

  Pour plus d'informations sur les différentes méthodes d'installation de clients, voir Méthodes d'installation du client dans System Center Configuration Manager.

  De plus, dans la mesure du possible, sélectionnez une méthode d'installation du client qui nécessite le moins d'autorisations de sécurité dans Configuration Manager et limitez les utilisateurs administratifs auxquels sont affectés des rôles de sécurité qui incluent des autorisations pouvant être utilisées à d'autres fins que le déploiement du client. Par exemple, la mise à niveau automatique du client nécessite le rôle de sécurité **Administrateur complet** , qui accorde à un utilisateur administratif toutes les autorisations de sécurité.

  Pour plus d'informations sur les dépendances et les autorisations de sécurité requises pour chaque méthode d'installation du client, voir « Dépendances liées aux méthodes d'installation » dans Configuration requise pour les clients d'ordinateurs.

  **Si vous devez utiliser l'installation Push du client, prenez des mesures supplémentaires pour sécuriser le compte d'installation Push du client**

  Bien que ce compte doive être membre du groupe **Administrateurs** local sur chaque ordinateur qui installera le logiciel client Configuration Manager, n'ajoutez jamais le compte d'installation Push du client au groupe **Administrateurs de domaine**. Créez plutôt un groupe global, puis ajoutez ce groupe global au groupe **Administrateurs** local sur vos ordinateurs clients. Vous pouvez également créer un objet de stratégie de groupe pour ajouter un paramètre de groupe restreint afin d'ajouter le compte d'installation poussée du client au groupe **Administrateurs** local.

  Pour renforcer la sécurité, créez plusieurs comptes d'installation poussée du client, disposant chacun d'un accès administratif à un nombre limité d'ordinateurs, de sorte que si un compte est compromis, seuls les ordinateurs clients auxquels ce compte a accès sont compromis.

**Supprimez les certificats avant l'acquisition d'images de l'ordinateur client**

Si vous prévoyez de déployer des clients en utilisant la technologie d'acquisition d'images, supprimez toujours les certificats tels que les certificats PKI qui incluent l'authentification du client et les certificats auto-signés avant de capturer l'image. Si vous ne supprimez pas ces certificats, les clients pourront emprunter l'identité l'un de l'autre et vous ne serez pas en mesure de vérifier les données pour chaque client.

Pour plus d'informations sur l'utilisation de Sysprep pour préparer un ordinateur à l'acquisition d'images, voir la documentation de votre déploiement Windows.

**Assurez-vous que les clients d'ordinateur Configuration Manager obtiennent une copie autorisée de ces certificats :**

- La clé racine approuvée de Configuration Manager

  Si vous n'avez pas développé le schéma Active Directory pour Configuration Manager et si les clients n'utilisent pas de certificats PKI lorsqu'ils communiquent avec des points de gestion, les clients font appel à la clé racine approuvée de Configuration Manager pour authentifier les points de gestion valides. Dans ce scénario, les clients n'ont aucun moyen de vérifier que le point de gestion est un point de gestion approuvé pour la hiérarchie, sauf s'ils utilisent la clé racine approuvée. Sans la clé racine approuvée, un attaquant doué pourrait diriger les clients vers un point de gestion non autorisé.

  Lorsque les clients ne peuvent pas télécharger la clé racine approuvée de Configuration Manager à partir du catalogue global ou en utilisant des certificats PKI, mettez en service anticipé les clients qui possèdent la clé racine approuvée pour être sûr qu'ils ne peuvent pas être dirigés vers un point de gestion non autorisé. Pour plus d'informations, voir Planning for the Trusted Root Key.

- Le certificat de signature du serveur de site

  Les clients utilisent le certificat de signature du serveur de site pour vérifier que le serveur de site a signé la stratégie de clients qu'ils téléchargent à partir d'un point de gestion. Ce certificat est auto-signé par le serveur de site et publié dans les services de domaine Active Directory.

  Lorsque les clients ne peuvent pas télécharger le certificat de signature de serveur de site à partir du catalogue global, par défaut ils le téléchargent à partir du point de gestion. Lorsque le point de gestion est exposé à un réseau non approuvé (par exemple, Internet), installez manuellement le certificat de signature de serveur de site sur les clients pour vous assurer qu'ils ne peuvent pas exécuter de stratégies de clients qui ont été falsifiées à partir d'un point de gestion compromis.

  Pour installer manuellement le certificat de signature de serveur de site, utilisez la propriété client.msi CCMSetup **SMSSIGNCERT**. Pour plus d'informations, voir À propos des propriétés d'installation du client dans System Center Configuration Manager.

  **Ne pas utiliser l'attribution automatique de site si le client envisage de télécharger la clé racine approuvée à partir du premier point de gestion qu'il contacte**

  Cette pratique recommandée en termes de sécurité est liée à l'entrée précédente. Pour éviter le risque qu'un nouveau client télécharge la clé racine approuvée à partir d'un point de gestion factice, utilisez l'attribution automatique de site dans les scénarios suivants uniquement :

- Le client peut accéder aux informations de site Configuration Manager publiées dans les services de domaine Active Directory.
- Vous préconfigurez un client avec la clé racine approuvée.
- Vous utilisez des certificats PKI depuis une autorité de certification d'entreprise pour établir l'approbation entre le client et le point de gestion.

Pour plus d'informations sur la clé racine approuvée, voir Planification de la clé racine approuvée.

**Installer des ordinateurs clients avec l'option Client.msi CCMSetup SMSDIRECTORYLOOKUP=NoWINS**

La méthode d'emplacement des services la plus sûre pour les clients afin de trouver des sites et des points de gestion consiste à utiliser des services de domaine Active Directory. Si cela n'est pas possible, par exemple, parce que vous ne pouvez pas développer le schéma Active Directory pour Configuration Manager ou parce que les clients se trouvent dans une forêt ou un groupe de travail non approuvé, vous pouvez utiliser la publication DNS comme autre méthode d'emplacement des services. Si ces deux méthodes échouent, les clients peuvent recourir à l'utilisation de WINS lorsque le point de gestion n'est pas configuré pour les connexions client HTTPS.

Dans la mesure où la publication vers WINS est moins sûre que les autres méthodes de publication, configurez les ordinateurs clients de sorte qu'ils ne recourent pas à l'utilisation de WINS en spécifiant SMSDIRECTORYLOOKUP=NoWINS. Si vous devez utiliser WINS pour l'emplacement des services, utilisez SMSDIRECTORYLOOKUP=WINSSECURE (paramètre par défaut), qui utilise la clé racine approuvée de Configuration Manager pour valider le certificat auto-signé du point de gestion.

> **NOTE**
> Lorsque le client est configuré pour SMSDIRECTORYLOOKUP=WINSSECURE et trouve un point de gestion à partir de WINS, le client vérifie sa copie de la clé racine approuvée de Configuration Manager qui se trouve dans WMI. Si la signature du certificat du point de gestion correspond à la copie du client de la clé racine approuvée, le certificat est validé et le client communique avec le point de gestion trouvé à l'aide de WINS. Si la signature du certificat du point de gestion ne correspond pas à la copie du client de la clé racine approuvée, le certificat n'est pas validé et le client ne communique pas avec le point de gestion trouvé à l'aide de WINS.

**Assurez-vous que les fenêtres de maintenance sont assez grandes pour déployer des mises à jour logicielles critiques**

Vous pouvez configurer des fenêtres de maintenance pour les regroupements d'appareils afin de limiter les périodes où Configuration Manager peut installer des logiciels sur ces appareils. Si vous configurez une fenêtre de maintenance trop petite, le client peut ne pas installer les mises à jour logicielles critiques et se retrouver vulnérable à l'attaque qui aurait été contrée par la mise à jour logicielle.

**Dans le cas d'appareils Windows Embedded avec des filtres d'écriture, prendre des précautions de sécurité supplémentaires pour réduire la surface d'attaque si Configuration Manager désactive les filtres d'écriture dans le but de conserver les installations logicielles et les modifications**

Lorsque des filtres d'écriture sont activés sur des appareils Windows Embedded, les installations logicielles ou les modifications sont apportées dans le segment de recouvrement uniquement et ne sont pas conservées après le redémarrage de l'appareil. Si vous utilisez Configuration Manager pour désactiver temporairement les filtres d'écriture dans le but de conserver les installations logicielles et les modifications, pendant cette période, l'appareil intégré est vulnérable aux modifications apportées à tous les volumes, y compris les dossiers partagés.

Bien que Configuration Manager verrouille l'ordinateur pendant cette période afin que seuls les administrateurs locaux puissent se connecter, prenez des précautions de sécurité supplémentaires pour aider à protéger l'ordinateur lorsque cela est possible. Par exemple, activez des restrictions supplémentaires sur le pare-feu et déconnectez l'appareil du réseau.

Si vous utilisez des fenêtres de maintenance pour conserver les modifications, planifiez soigneusement la durée de ces fenêtres pour réduire le temps de désactivation des filtres d'écriture mais permettre les installations logicielles et les redémarrages.

**Si vous utilisez l'installation de client basée sur des mises à jour logicielles et installez une version**

**ultérieure du client sur le site, exécutez la mise à jour logicielle publiée sur le point de mise à jour logicielle afin que le client reçoive la version la plus récente**

Si vous installez une version ultérieure du client sur le site, par exemple, vous mettez le site à niveau, la mise à jour logicielle pour le déploiement de client qui est publiée sur le point de mise à jour logicielle n'est pas exécutée automatiquement. Vous devez republier le client Configuration Manager sur le point de mise à jour logicielle et cliquer sur **Oui** pour mettre à jour le numéro de version.

Pour plus d'informations, voir la procédure « Pour publier le client Configuration Manager dans le point de mise à jour logicielle » dans Comment installer des clients Configuration Manager à l'aide d'une installation basée sur les mises à jour logicielles.

**Configurez le paramètre de l'appareil client de l'Agent ordinateur Interrompre l'entrée du code confidentiel BitLocker au redémarrage sur Toujours uniquement pour les ordinateurs auxquels vous faites confiance et qui ont un accès physique limité**

Lorsque vous définissez ce paramètre client sur **Toujours**, Configuration Manager peut terminer l'installation du logiciel afin de s'assurer que les mises à jour logicielles critiques sont installées et que les services ont repris. Toutefois, si un attaquant intercepte le processus de redémarrage, il peut prendre le contrôle de l'ordinateur. Utilisez ce paramètre uniquement lorsque vous faites confiance à l'ordinateur et lorsque l'accès physique à l'ordinateur est limité. Par exemple, ce paramètre peut convenir aux serveurs d'un centre de données.

**Ne configurez pas le paramètre de l'appareil client de l'Agent ordinateur Stratégie d'exécution de PowerShell sur Ignorer.**

Ce paramètre client permet au client Configuration Manager d'exécuter des scripts PowerShell non signés, ce qui peut autoriser l'exécution de programmes malveillants sur des ordinateurs clients. Si vous devez sélectionner cette option, utilisez un paramètre client personnalisé et affectez-le uniquement aux ordinateurs clients qui doivent exécuter des scripts PowerShell non signés.

## Bonnes pratiques de sécurité pour les appareils mobiles

**Pour les appareils mobiles que vous inscrivez à Configuration Manager et qui seront pris en charge sur Internet : Installer le point proxy d'inscription dans un réseau de périmètre et le point d'inscription dans l'Intranet**

Cette séparation des rôles permet de protéger le point d'inscription contre une attaque. Si le point d'inscription est compromis, un attaquant peut obtenir des certificats pour authentification et voler les informations d'identification des utilisateurs qui inscrivent leurs appareils mobiles.

**Pour les appareils mobiles : Configurez les paramètres de mot de passe pour protéger les appareils mobiles contre les accès non autorisés**

Pour les appareils mobiles qui sont inscrits par Configuration Manager: Utilisez un élément de configuration d'appareil mobile pour configurer la complexité du mot de passe comme étant le code confidentiel et au moins la longueur par défaut pour la longueur minimale du mot de passe.

Pour les appareils mobiles sur lesquels le client Configuration Manager n'est pas installé mais qui sont gérés par le connecteur Exchange Server : Configurez les **Paramètres de mot de passe** pour le connecteur Exchange Server, de sorte que la complexité du mot de passe soit le code confidentiel et spécifier au moins la longueur par défaut pour la longueur minimale du mot de passe.

**Pour les appareils mobiles : Empêchez la falsification des informations d'inventaire et des informations d'état en autorisant l'exécution des applications uniquement lorsqu'elles sont signées par des entreprises approuvées et ne pas autoriser l'installation de fichiers non signés**

Pour d'autres appareils mobiles qui sont inscrits par Configuration Manager : Utilisez un élément de configuration

d'appareil mobile pour configurer le paramètre de sécurité **Applications non signée**s comme **Interdites** et configurez les **Installations de fichiers non signés** comme une source approuvée.

Pour les appareils mobiles sur lesquels le client Configuration Manager n'est pas installé mais qui sont gérés par le connecteur Exchange Server : Configurez les **Paramètres d'application** pour le connecteur Exchange Server, de sorte que l'**Installation de fichiers non signés** et les **Applications non signées** soient configurées comme **Interdites**.

**Pour les appareils mobiles : Empêchez l'élévation des attaques de privilège en verrouillant l'appareil mobile lorsqu'il n'est pas autorisé**

Pour d'autres appareils mobiles qui sont inscrits par Configuration Manager : Utiliser un élément de configuration d'appareil mobile pour configurer le paramètre de mot de passe **Durée d'inactivité en minutes avant le verrouillage du périphérique mobile**.

Pour les appareils mobiles sur lesquels le client Gestionnaire de configuration n'est pas installé mais qui sont gérés par le connecteur Exchange Server : Configurez les **Paramètres de mot de passe** pour le connecteur Exchange Server afin de configurer la **Durée d'inactivité en minutes avant le verrouillage du périphérique mobile** .

**Pour les appareils mobiles : Empêchez l'élévation de privilèges en limitant les utilisateurs qui peuvent inscrire leurs appareils mobiles**

Utilisez un paramètre client personnalisé plutôt que les paramètres clients par défaut, pour que seuls les utilisateurs autorisés puissent inscrire leurs appareils mobiles.

**Pour les appareils mobiles : Ne déployez pas d'applications pour les utilisateurs qui possèdent des appareils mobiles inscrits par Configuration Manager ou Microsoft Intune dans les cas suivants :**

- Lorsque l'appareil mobile est utilisé par plusieurs personnes.
- Lorsque l'appareil est inscrit par un administrateur pour le compte d'un utilisateur.
- Lorsque l'appareil est transféré à une autre personne sans retirer puis réinscrire l'appareil.

  Une relation d'affinité entre appareil et utilisateur est créée lors de l'inscription, qui mappe l'utilisateur effectuant l'inscription à l'appareil mobile. Si un autre utilisateur utilise l'appareil mobile, il pourra exécuter les applications que vous déployez sur l'utilisateur d'origine, ce qui peut entraîner une élévation de privilèges. De même, si un autre administrateur inscrit l'appareil mobile pour un utilisateur, les applications déployées sur l'utilisateur ne sont pas installées sur l'appareil mobile, mais les applications déployées sur l'administrateur peuvent être installées.

  Contrairement à l'affinité entre appareil et utilisateur pour les ordinateurs Windows, vous ne pouvez pas définir manuellement les informations d'affinité entre appareil et utilisateur pour les appareils mobiles qui sont inscrits par Microsoft Intune.

  Si vous transférez la propriété d'un appareil mobile inscrit par Intune, retirez l'appareil mobile de Intune pour supprimer l'affinité entre appareil et utilisateur, puis demandez à l'utilisateur actuel de réinscrire l'appareil.

  **Pour les appareils mobiles : Assurez-vous que les utilisateurs inscrivent leurs appareils mobiles pour Microsoft Intune**

  Dans la mesure où une relation d'affinité entre appareil et utilisateur est créée lors de l'inscription qui mappe l'utilisateur effectuant l'inscription sur l'appareil mobile, si un administrateur inscrit l'appareil mobile pour un utilisateur, les applications déployées sur l'utilisateur ne sont pas installées sur l'appareil mobile, mais les applications déployées sur l'administrateur peuvent être installées.

  **Pour le connecteur Exchange Server : Assurez-vous que la connexion entre le serveur de site Configuration Manager et l'ordinateur Exchange Server est protégée**

Utiliser IPsec si le serveur Exchange Server est sur le site ; Exchange hébergé sécurise automatiquement la connexion par SSL.

**Pour le connecteur Exchange Server : Utilisez le principe des privilèges minimum pour le connecteur**

Pour obtenir la liste des applets de commande dont le connecteur Exchange Server a besoin au minimum, voir Gérer des appareils mobiles à l'aide de System Center Configuration Manager et d'Exchange.

## Bonnes pratiques de sécurité pour les ordinateurs Mac

**Pour les ordinateurs Mac : Stockez et accédez aux fichiers sources du client à partir d'un emplacement sécurisé.**

Configuration Manager ne vérifie pas si ces fichiers source du client ont été falsifiés avant d'installer ou d'inscrire le client sur un ordinateur Mac. Téléchargez ces fichiers à partir d'une source digne de confiance, enregistrez-les et accédez-y en toute sécurité.

**Pour les ordinateurs Mac : Indépendamment de Configuration Manager, surveillez et effectuez le suivi de la période de validité du certificat d'inscription des utilisateurs.**

Pour garantir la pérennité des activités, surveillez et effectuez le suivi de la période de validité des certificats que vous utilisez pour les ordinateurs Mac. Configuration Manager ne prend pas en charge le renouvellement automatique de ce certificat et ne vous avertit pas que le certificat est sur le point d'expirer. La période de validité type est de 1 an.

Pour plus d'informations sur le renouvellement du certificat, voir Renouvellement manuel du certificat client Mac.

**Pour les ordinateurs Mac : Envisagez de configurer le certificat d'Autorité de certification racine approuvé de manière à ce qu'il soit approuvé pour le protocole SSL uniquement afin d'empêcher une élévation des privilèges.**

Lorsque vous inscrivez des ordinateurs Mac, un certificat utilisateur destiné à gérer le client Configuration Manager est automatiquement installé, ainsi que le certificat racine approuvé auquel est lié le certificat utilisateur. Si vous voulez limiter l'approbation de ce certificat racine au protocole SSL uniquement, vous pouvez procéder comme suit.

Une fois cette procédure exécutée, le certificat racine n'est pas approuvé pour valider les protocoles autres que SSL : par exemple, Courrier sécurisé (S/MIME), Protocole EAP (Extensible Authentication), ou la signature de code.

> **NOTE**
> Vous pouvez également utiliser cette procédure si vous avez installé le certificat client indépendamment de Configuration Manager.

Pour limiter le certificat d'autorité de certification racine pour le protocole SSL uniquement :

1. Sur l'ordinateur Mac, ouvrez une fenêtre de terminal.
2. Entrez la commande **sudo /Applications/Utilities/Keychain\ Access.app/Contents/MacOS/Keychain\ Access**
3. Dans la boîte de dialogue **Trousseau d'accès** , dans la zone **Trousseau** , cliquez sur **Système**, puis dans la zone **Catégorie** , cliquez sur **Certificats**.
4. Recherchez et double-cliquez sur le certificat d'autorité de certification racine pour le certificat client Mac.
5. Dans la boîte de dialogue du certificat d'autorité de certification racine, développez la zone **Confiance** , puis

apportez les modifications suivantes :

a. Pour le paramètre **Lors de l'utilisation de ce certificat** , remplacez le paramètre par défaut **Toujours faire confiance** par **Utiliser les valeurs système par défaut**.

b. Pour le paramètre **Secure Sockets Layer (SSL)** , remplacez le paramètre **aucune valeur spécifiée** par **Toujours faire confiance**.

6. Fermez la boîte de dialogue et lorsque vous y êtes invité, entrez le mot de passe de l'administrateur, puis cliquez sur **Mettre à jour les paramètres**.

## Problèmes de sécurité pour les clients Configuration Manager

Les problèmes de sécurité suivants ne peuvent pas être atténués :

- Les messages de statut ne sont pas authentifiés

  Aucune authentification n'est effectuée sur les messages de statut. Lorsqu'un point de gestion accepte les connexions client HTTP, n'importe quel appareil peut envoyer des messages de statut au point de gestion. Si le point de gestion n'accepte que les connexions client HTTPS, un appareil doit obtenir un certificat d'authentification client valide provenant d'une autorité de certification racine de confiance, mais peut également envoyer des messages de statut par la suite. Si un client envoie un message de statut non valide, il est supprimé.

  Il existe donc peu d'attaques potentielles contre cette vulnérabilité. Un attaquant pourrait envoyer un message de statut erroné pour adhérer à un regroupement basé sur des requêtes de messages de statut. Un client pourrait déclencher un refus de service contre le point de gestion en l'inondant de messages de statut. Si les messages de statut déclenchent des actions dans les règles de filtrage des messages de statut, un attaquant pourrait déclencher la règle de filtrage des messages de statut. Un attaquant pourrait également envoyer un message de statut qui rendrait les informations de rapport incorrectes.

- Des stratégies peuvent être reciblées vers des clients non ciblés

  Un attaquant pourrait utiliser plusieurs méthodes pour faire en sorte qu'une stratégie ciblée sur un seul client soit appliquée à un client totalement différent. Par exemple, un attaquant au niveau d'un client approuvé pourrait envoyer de fausses informations de découverte ou d'inventaire pour que l'ordinateur soit ajouté à un regroupement auquel il ne devrait pas appartenir, puis recevoir tous les déploiements de celui-ci. Bien que des contrôles existent pour aider à empêcher les attaquants de modifier la stratégie directement, des attaquants pourraient prendre une stratégie existante pour reformater ou redéployer un système d'exploitation et l'envoyer à un autre ordinateur, créant ainsi un refus de service. Ces types d'attaques demanderaient un minutage précis et des connaissances approfondies de l'infrastructure de Configuration Manager.

- Les journaux du client permettent l'accès utilisateur

  Tous les fichiers journaux des clients accordent un accès en lecture aux utilisateurs et un accès en écriture aux utilisateurs interactifs. Si vous activez la journalisation détaillée, des attaquants peuvent lire les fichiers journaux pour y rechercher des informations sur la compatibilité ou les vulnérabilités du système. Les processus tels que l'installation de logiciels, effectués dans un contexte de l'utilisateur, doivent être capables d'écrire vers les journaux avec un compte d'utilisateur doté de droits limités. Cela signifie qu'un attaquant pourrait également écrire vers les journaux avec un compte doté de droits limités.

  Le risque le plus sérieux est qu'un attaquant puisse supprimer des informations des fichiers journaux, dont un administrateur pourrait avoir besoin pour l'audit et la détection d'intrus.

- Un ordinateur peut être utilisé pour obtenir un certificat conçu pour l'inscription d'appareils mobiles

  Lorsque Configuration Manager traite une demande d'inscription, il ne peut pas vérifier qu'elle émane d'un

appareil mobile plutôt que d'un ordinateur. Si la demande provient d'un ordinateur, il peut installer un certificat PKI qui lui permet ensuite de s'inscrire avec Configuration Manager. Pour prévenir une attaque par élévation de privilèges dans ce scénario, n'autorisez que les utilisateurs approuvés à inscrire leurs appareils mobiles et surveillez attentivement les activités d'inscription.

- La connexion d'un client au point de gestion n'est pas abandonnée si vous bloquez un client, et celui-ci peut continuer à envoyer des paquets de notification client au point de gestion, par exemple, des messages de conservation d'activité

  Lorsque vous bloquez un client auquel vous ne faites plus confiance, et qui a établi une communication de notification client, Configuration Manager ne déconnecte pas la session. Le client bloqué peut continuer à envoyer des paquets à son point de gestion jusqu'à ce que le client se déconnecte du réseau. Ces paquets sont seulement des paquets de petite taille, des paquets de conservation d'activité, et ces clients ne peuvent pas être gérés par Configuration Manager jusqu'à ce qu'ils soient débloqués.

- Lorsque vous utilisez la mise à niveau automatique des clients et que le client est dirigé vers un point de gestion pour télécharger les fichiers source du client, le point de gestion n'est pas vérifié comme une source fiable

- Lorsque les utilisateurs inscrivent des ordinateurs Mac pour la première fois, ils sont exposés à l'usurpation DNS

  Lorsque l'ordinateur Mac se connecte au point proxy d'inscription lors de l'inscription, il est peu probable que l'ordinateur Mac possède déjà le certificat d'autorité de certification racine. À ce stade, le serveur est non approuvé par l'ordinateur Mac et il invite l'utilisateur à continuer. Si le nom de domaine complet du point proxy d'inscription est résolu par un serveur DNS non autorisé, il peut diriger l'ordinateur Mac vers un point proxy d'inscription non autorisé et installer des certificats à partir d'une source non approuvée. Pour réduire ce risque, suivez les meilleures pratiques afin d'éviter l'usurpation DNS dans votre environnement.

- L'inscription d'ordinateurs Mac ne limite pas les demandes de certificat

  Les utilisateurs peuvent réinscrire leurs ordinateurs Mac, en demandant chaque fois un certificat client. Configuration Manager ne vérifie pas s'il existe plusieurs demandes ni limite le nombre de certificats demandés à partir d'un seul ordinateur. Un utilisateur non autorisé pourrait exécuter un script qui répète la demande d'inscription de ligne de commande, provoquant un déni de service sur le réseau ou sur l'autorité de certification (CA) émettrice. Pour réduire ce risque, surveillez attentivement l'autorité de certification émettrice pour ce type de comportement suspect. Un ordinateur qui présente ce modèle de comportement doit immédiatement être bloqué de la hiérarchie Configuration Manager.

- Un accusé de réception de réinitialisation ne vérifie pas que l'appareil a bien été réinitialisé

  Lorsque vous lancez une action de réinitialisation pour un appareil mobile et Configuration Manager affiche l'état de la réinitialisation pour laquelle un accusé de réception est attendu, la vérification indique que Configuration Manager a bien envoyé le message et non que l'appareil a effectué une action sur celui-ci. En outre, pour les appareils mobiles qui sont gérés par le connecteur Exchange Server, un accusé de réception de réinitialisation vérifie que la commande a été reçue par Exchange, et non par l'appareil.

- Si vous utilisez les options de validation des modifications sur des appareils Windows Embedded, les comptes peuvent être verrouillés plus tôt que prévu

  Si l'appareil Windows Embedded exécute un système d'exploitation antérieur à Windows 7, et qu'un utilisateur tente de se connecter alors que les filtres d'écriture sont désactivés pour valider des modifications apportées par Configuration Manager, le nombre de tentatives de connexion incorrectes permis avant le verrouillage du compte est réduit de moitié. Par exemple, si le **Seuil de verrouillage de compte** est configuré sur 6, et que l'utilisateur entre son mot de passe incorrectement 3 fois, le compte est bloqué, ce qui crée une situation de déni de service. Si les utilisateurs doivent se connecter aux appareils intégrés dans

ce scénario, avertissez-les du risque d'un seuil de verrouillage réduit.

# Informations de confidentialité pour les clients Configuration Manager

Lorsque vous déployez le client Configuration Manager, vous activez des paramètres clients afin de pouvoir utiliser les fonctionnalités de gestion de Configuration Manager. Les paramètres que vous utilisez pour configurer les fonctionnalités peuvent s'appliquer à tous les clients de la hiérarchie Configuration Manager, qu'ils soient directement connectés au réseau d'entreprise, connectés via une session distante ou connectés à Internet mais pris en charge par Configuration Manager.

Les informations sur le client sont stockées dans la base de données Configuration Manager et ne sont pas envoyées à Microsoft. Les informations sont conservées dans la base de données jusqu'à leur suppression par les tâches de maintenance du site **Supprimer les données de découverte anciennes** , tous les 90 jours. Vous pouvez configurer l'intervalle de suppression.

Avant de configurer le client Configuration Manager, réfléchissez à vos besoins en matière de confidentialité.

**Informations sur la confidentialité des appareils mobiles qui sont inscrits par Configuration Manager**

Pour des informations sur la confidentialité quand vous inscrivez un appareil mobile par Configuration Manager, voir Déclaration de confidentialité de System Center Configuration Manager - Addendum relatif aux appareils mobiles.

**État du client**

Configuration Manager surveille l'activité des clients et l'évalue périodiquement, et peut corriger le client Configuration Manager et ses dépendances. L'état du client est activé par défaut et il utilise les mesures côté serveur pour vérifier l'activité du client, ainsi que les actions côté client pour les auto-contrôles, la correction et pour l'envoi d'informations sur l'état du client au site Configuration Manager. Le client exécute les auto-contrôles en fonction d'un calendrier que vous pouvez configurer. Le client envoie les résultats des contrôles au site Configuration Manager. Ces informations sont chiffrées lors du transfert.

Les informations sur l'état du client sont stockées dans la base de données Configuration Manager et ne sont pas envoyées à Microsoft. Les informations ne sont pas stockées sous forme chiffrée dans la base de données du site. Ces informations sont conservées dans la base de données jusqu'à ce qu'elles en soient supprimées en fonction de la valeur configurée pour le paramètre de l'état du client **Conserver l'historique de l'état du client pendant le nombre de jours suivant** . La valeur par défaut pour ce paramètre est 31 jours.

Avant d'installer le client Configuration Manager avec vérification de l'état du client, pensez à vos besoins en matière de confidentialité.

# Informations de confidentialité pour les appareils mobiles qui sont gérés à l'aide du connecteur Exchange Server

Le connecteur Exchange Server détecte et gère les appareils qui se connectent à Exchange Server (hébergés ou sur site) en utilisant le protocole ActiveSync. Les enregistrements trouvés par le connecteur Exchange Server sont stockés dans la base de données Configuration Manager. Les informations sont collectées à partir d'Exchange Server. Elles ne contiennent pas d'informations supplémentaires par rapport à ce que les appareils mobiles envoient à Exchange Server.

Les informations de l'appareil mobile ne sont pas envoyées à Microsoft. Ensuite, les informations de compatibilité sont stockées dans la base de données de Configuration Manager. Les informations sont conservées dans la base de données jusqu'à leur suppression par les tâches de maintenance du site **Supprimer les données de découverte anciennes** , tous les 90 jours. Vous pouvez configurer l'intervalle de suppression.

Avant d'installer et de configurer le connecteur Exchange Server, pensez à vos besoins en matière de confidentialité.

# Bonnes pratiques pour le déploiement de clients dans System Center Configuration Manager

22/06/2018 • 10 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

## Utilisation de l'installation de client basée sur des mises à jour logicielles sur les ordinateurs Active Directory

Cette méthode de déploiement du client utilise les technologies Windows existantes, s'intègre avec votre infrastructure Active Directory et ne nécessite qu'une configuration minimale dans Configuration Manager. Elle est la plus facile pour configurer le pare-feu et elle est aussi la plus sûre. À l'aide de groupes de sécurité et du filtrage WMI pour la configuration de stratégie de groupe, vous disposez d'une grande flexibilité pour contrôler quels ordinateurs installent le client Configuration Manager.

Pour plus d'informations, voir Comment installer des clients Configuration Manager à l'aide d'une installation basée sur les mises à jour logicielles.

## Développement du schéma Active Directory et publication du site afin de pouvoir exécuter CCMSetup sans options de ligne de commande

Lorsque vous étendez le schéma Active Directory pour Configuration Manager et que le site est publié dans les services de domaine Active Directory, de nombreuses propriétés d'installation du client sont publiées dans les services de domaine Active Directory. Si un ordinateur peut localiser ces propriétés d'installation du client, il peut les utiliser au cours du déploiement du client Configuration Manager. Ces informations étant générées automatiquement, le risque d'erreur humaine propre à la saisie manuelle des propriétés d'installation est éliminé.

Pour plus d'informations, consultez À propos de la publication des propriétés d'installation du client sur les services de domaine Active Directory dans System Center Configuration Manager.

## Utiliser un déploiement échelonné pour gérer l'utilisation de l'UC

Minimisez les besoins de traitement par le processeur sur le serveur de site en utilisant un déploiement échelonné des clients. Déployez les clients en dehors des heures de travail pour que les autres services disposent de plus de bande passante pendant la journée et pour éviter de perturber le travail des utilisateurs si leur ordinateur ralentit ou nécessite un redémarrage.

## Activation de la mise à niveau automatique après le déploiement client principal

Les mises à niveau automatiques du client sont utiles quand vous voulez mettre à niveau un petit nombre d'ordinateurs clients qui peuvent avoir été ignorés par votre méthode d'installation principale du client, par exemple car ils étaient hors connexion.

**NOTE**

Les améliorations des performances dans Configuration Manager vous permettent d'utiliser les mises à niveau automatiques comme méthode principale de mise à niveau des clients. Toutefois, les performances dépendent de l'infrastructure de votre hiérarchie, par exemple, le nombre de clients.

## Utilisation de SMSMP et FSP pour l'installation du client avec les propriétés client.msi

La propriété SMSMP définit le point de gestion initial avec lequel le client communique et supprime la dépendance sur les solutions d'emplacement de service telles que les services de domaine Active Directory, DNS et WINS.

Utilisez la propriété FSP et installez un point d'état de secours afin de pouvoir surveiller l'installation et l'affectation du client, et identifier les problèmes de communication.

Pour plus d'informations sur ces options, consultez À propos des propriétés d'installation du client dans System Center Configuration Manager.

## Installer des modules linguistiques client avant d'installer les clients

Nous vous recommandons d'installer les modules linguistiques client avant de déployer le client. Si vous installez des modules linguistiques client (pour activer des langues supplémentaires) sur un site après avoir installé des clients, vous devez réinstaller ces derniers avant qu'ils puissent utiliser ces langues. Pour les clients d'appareils mobiles, vous devez réinitialiser les appareils mobiles et les réinscrire.

## Préparer les certificats PKI nécessaires à l'avance

Pour gérer des appareils sur Internet, des appareils mobiles inscrits et des ordinateurs Mac, vous devez disposer de certificats PKI sur les systèmes de site (points de gestion et points de distribution) et les appareils clients. Sur les réseaux de production, l'approbation de la gestion des modifications peut être requise pour utiliser de nouveaux certificats et redémarrer les serveurs de système de site. Sinon, les utilisateurs devront devront fermer la session et la rouvrir pour appliquer l'appartenance au nouveau groupe. En outre, vous devrez laisser suffisamment de temps pour la réplication des autorisations de sécurité et pour les nouveaux modèles de certificat.

Pour plus d'informations sur les certificats PKI nécessaires, consultez Configuration requise des certificats PKI pour System Center Configuration Manager.

## Configuration des paramètres client et des fenêtres de maintenance requis avant l'installation de clients

Même si vous pouvez configurer les paramètres client et les fenêtres de maintenance avant ou après l'installation des clients, il est préférable de configurer les paramètres nécessaires avant d'installer les clients pour pouvoir utiliser ces paramètres dès que le client est installé.

Configurez des fenêtres de maintenance pour les serveurs et les appareils Windows Embedded, afin de garantir un fonctionnement ininterrompu des appareils critiques. Les fenêtres de maintenance garantissent que les mises à jour logicielles et les logiciels anti-programme malveillant nécessaires ne redémarrent pas l'ordinateur pendant les heures de bureau.

**IMPORTANT**

Pour les ordinateurs Windows 10 que vous souhaitez protéger avec le Filtre d'écriture unifié (UWF), vous devez configurer le périphérique pour UWF avant d'installer le client. Ceci permet à Configuration Manager d'installer le client avec un fournisseur d'informations d'identification personnalisées qui empêche des utilisateurs aux droits restreints de se connecter à l'appareil pendant qu'il est en mode maintenance.

## Planifier l'expérience d'inscription de vos utilisateurs pour les ordinateurs Mac et les appareils mobiles

Si des utilisateurs doivent inscrire leurs ordinateurs Mac et leurs appareils mobiles avec Configuration Manager, planifiez l'expérience utilisateur. Par exemple, vous pouvez créer un script pour le processus d'installation et d'inscription en utilisant une page web sur laquelle les utilisateurs indiquent seulement les informations strictement nécessaires, et leur envoyer les instructions avec un lien par e-mail.

## Utiliser des filtres d'écriture basés sur des fichiers pour les appareils Windows Embedded

Les appareils embarqués qui utilisent des filtres d'écriture améliorés (EWF) peuvent rencontrer des resynchronisations de messages d'état. Si vous n'avez que quelques appareils embarqués qui utilisent des filtres d'écriture améliorés, il est possible que vous ne vous en rendiez pas compte. Par contre, si vous en avez beaucoup qui resynchronisent leurs informations, par exemple qui envoient un inventaire complet plutôt qu'un inventaire différentiel, cela risque de générer une augmentation détectable des paquets réseau et un traitement par le processeur plus élevé sur le serveur de site.

Si vous avez le choix du type de filtre d'écriture à activer, choisissez des filtres d'écriture basés sur des fichiers et configurez des exceptions pour conserver l'état du client et les données d'inventaire entre redémarrages d'appareil et préserver l'efficacité du réseau et du processeur sur le client Configuration Manager. Pour plus d'informations sur les filtres d'écriture, consultez Planification du déploiement de clients sur des appareils Windows Embedded dans System Center Configuration Manager.

Pour plus d'informations sur le nombre maximal de clients Windows Embedded pris en charge par un site principal, consultez Systèmes d'exploitation pris en charge pour les clients et les appareils.

# Déterminer si des clients doivent être bloqués dans System Center Configuration Manager

22/06/2018 • 5 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Si un ordinateur client ou un appareil mobile client n'est plus approuvé, vous pouvez bloquer ce client dans la console System Center 2012 Configuration Manager. L'infrastructure Configuration Manager rejette les clients bloqués afin qu'ils ne puissent pas communiquer avec les systèmes de site pour télécharger la stratégie, charger les données d'inventaire ou envoyer des messages d'état.

Vous devez bloquer et débloquer les clients depuis leur site attribué plutôt que depuis un site secondaire ou un site d'administration centrale.

> **IMPORTANT**
> Le blocage dans Configuration Manager aide à sécuriser le site Configuration Manager, mais ne vous fiez pas à cette fonctionnalité pour protéger le site contre les ordinateurs ou les appareils mobiles non approuvés si vous autorisez les clients à communiquer avec les systèmes du site à l'aide de HTTP, car un client bloqué peut de nouveau joindre le site avec un nouveau certificat auto-signé et un nouvel ID matériel. À la place, utilisez la fonctionnalité de blocage pour bloquer les supports de démarrage perdus ou non fiables, que vous utilisez pour déployer les systèmes d'exploitation, et lorsque les systèmes de site acceptent les connexions client HTTPS.

Les clients accédant au site à l'aide du certificat proxy ISV ne peuvent pas être bloqués. Pour plus d'informations sur le certificat de proxy ISV, consultez le kit SDK de System Center Configuration Manager.

Si vos systèmes de site acceptent les connexions client HTTPS et que votre infrastructure de clé publique (PKI) prend en charge une liste de révocation de certificats, envisagez toujours de définir la révocation de certificat comme première ligne de défense contre les certificats potentiellement compromis. Le blocage des clients dans Configuration Manager fournit une seconde ligne de défense pour protéger votre hiérarchie.

## Éléments à prendre en considération pour le blocage des clients

- Cette option est disponible pour les connexions client HTTP et HTTPS, mais sa sécurité est limitée lorsque les clients se connectent à des systèmes de site en utilisant le protocole HTTP.
- Les utilisateurs administratifs de Configuration Manager ont l'autorité nécessaire pour bloquer un client et cette action est entreprise dans la console Configuration Manager.
- La communication client est rejetée uniquement à partir de la hiérarchie Configuration Manager.

  > **NOTE**
  > Le même client peut s'inscrire auprès d'une autre hiérarchie Configuration Manager.

- Le client est immédiatement bloqué hors du site Configuration Manager.
- Permet de protéger les systèmes de site des ordinateurs et des appareils mobiles potentiellement compromis.

# Éléments à prendre en considération pour l'utilisation de la révocation de certificats

- Cette option est disponible pour les connexions HTTPS des clients Windows si l'infrastructure à clé publique prend en charge une liste de révocation de certificats (CRL).

  Les clients Mac contrôlent systématiquement la liste de révocation de certificats, et cette fonctionnalité ne peut pas être désactivée.

  Même si les clients d'appareils mobiles n'utilisent pas de listes de révocation de certificats pour vérifier les certificats des systèmes de site, leurs certificats peuvent être révoqués et vérifiés par Configuration Manager.

- Les administrateurs de l'infrastructure de clé publique ont l'autorité nécessaire pour révoquer un certificat et cette action est entreprise hors de la console Configuration Manager.

- Les communications client peuvent être rejetées à partir de tout ordinateur ou appareil mobile nécessitant ce certificat de client.

- Il y aura probablement un délai entre la révocation d'un certificat et le téléchargement par les systèmes de site de la liste de révocation de certificats (CRL) modifiée.

- Pour de nombreux déploiements PKI, ce délai peut être d'un ou de plusieurs jours. Par exemple, dans les services de certificats Active Directory, la période d'expiration par défaut est d'une semaine pour une liste de révocation de certificats complète et d'un jour pour une liste de révocation de certificats delta.

- Permet de protéger les systèmes de site et les clients contre des ordinateurs et des appareils mobiles potentiellement compromis.

  > **NOTE**
  > Il est possible d'améliorer la protection des systèmes de site qui exécutent IIS contre des clients inconnus en configurant une liste de certificats de confiance (CTL) dans IIS.

# Planification du déploiement de clients sur des ordinateurs Linux et UNIX dans System Center Configuration Manager

22/06/2018 • 22 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez installer le client System Center Configuration Manager sur des ordinateurs exécutant Linux ou UNIX. Ce client est conçu pour les serveurs qui fonctionnent en tant qu'ordinateur de groupe de travail, et le client ne prend pas en charge l'interaction avec les utilisateurs connectés. Une fois que le logiciel client est installé et que le client a établi la communication avec le site Configuration Manager, vous gérez le client à l'aide de la console et des rapports Configuration Manager.

**NOTE**

Le client Configuration Manager pour les ordinateurs Linux et UNIX ne prend pas en charge les fonctionnalités de gestion suivantes :

- Installation poussée du client
  - Déploiement du système d'exploitation
  - Déploiement d'application ; à la place, déployez des logiciels à l'aide de packages et programmes.
  - Inventaire logiciel
  - Mises à jour logicielles
  - Paramètres de conformité
  - Contrôle à distance
  - Gestion de l'alimentation
  - Vérification et correction de l'état du client
  - Gestion des clients basés sur Internet

Pour plus d'informations sur les distributions Linux et UNIX prises en charge et le matériel requis pour prendre en charge le client pour Linux et UNIX, consultez Matériel recommandé pour System Center Configuration Manager.

Aidez-vous des informations de cet article pour planifier le déploiement du client Configuration Manager pour Linux et UNIX.

## Conditions préalables pour le déploiement du client sur des serveurs Linux et UNIX

Utilisez les informations suivantes pour déterminer les conditions préalables pour que doivent avoir mis en place installer le client pour Linux et UNIX.

**Dépendances externes à Configuration Manager :**

Les tableaux suivants décrivent les systèmes d'exploitation UNIX et Linux requis et les dépendances des packages.

**Red Hat Enterprise Linux Server 5.1 (Tikanga)**

| PACKAGE REQUIS | DESCRIPTION | VERSION MINIMALE |
|---|---|---|
| glibc | Bibliothèques standards C | 2.5-12 |
| Openssl | Bibliothèque OpenSSL, protocole de communication réseau sécurisé | 0.9.8b-8.3.el5 |
| PAM | Modules d'authentification enfichables | 0.99.6.2-3.14.el5 |

### Red Hat Enterprise Linux Server 6

| PACKAGE REQUIS | DESCRIPTION | VERSION MINIMALE |
|---|---|---|
| glibc | Bibliothèques standards C | 2.12-1.7 |
| Openssl | Bibliothèque OpenSSL, protocole de communication réseau sécurisé | 1.0.0-4 |
| PAM | Modules d'authentification enfichables | 1.1.1-4 |

### Red Hat Enterprise Linux Server version 7

| PACKAGE REQUIS | DESCRIPTION | VERSION MINIMALE |
|---|---|---|
| glibc | Bibliothèques standards C | 2.17 |
| Openssl | Bibliothèque OpenSSL, protocole de communication réseau sécurisé | 1.0.1 |
| PAM | Modules d'authentification enfichables | 1.1.1-4 |

### Solaris 10 SPARC

| PACKAGE REQUIS | DESCRIPTION | VERSION MINIMALE |
|---|---|---|
| Correctifs du système d'exploitation requis | Fuites de mémoire PAM | 117463-05 |
| SUNWlibC | Compilateurs Sun Workshop fournis en standard libC (sparc) | 5.10, REV=2004.12.22 |
| SUNWlibms | Bibliothèques Math & Microtasking (Usr) (sparc) | 5.10, REV=2004.11.23 |
| SUNWlibmsr | Bibliothèques Math & Microtasking (Root) (sparc) | 5.10, REV=2004.11.23 |
| SUNWcslr | Bibliothèques Core Solaris (Root) (sparc) | 11.10.0, REV=2005.01.21.15.53 |
| SUNWcsl | Bibliothèques Core Solaris (Root) (sparc) | 11.10.0, REV=2005.01.21.15.53 |

| PACKAGE REQUIS | DESCRIPTION | VERSION MINIMALE |
|---|---|---|
| Openssl | SUNopenssl-libraries (Usr)<br><br>Sun fournit les bibliothèques OpenSSL pour Solaris 10 SPARC. Elles sont fournies avec le système d'exploitation. | 11.10.0,REV=2005.01.21.15.53 |
| PAM | Modules d'authentification enfichables<br><br>SUNWcsr, Core Solaris, (Root) (sparc) | 11.10.0, REV=2005.01.21.15.53 |

### Solaris 10 x86

| PACKAGE REQUIS | DESCRIPTION | VERSION MINIMALE |
|---|---|---|
| Correctifs du système d'exploitation requis | Fuites de mémoire PAM | 117464-04 |
| SUNWlibC | LibC regroupés de compilateurs Sun atelier (i386) | 5.10,REV=2004.12.20 |
| SUNWlibmsr | Bibliothèques Math & Microtasking (Root) (i386) | 5.10, REV=2004.12.18 |
| SUNWcsl | Solaris, (et les bibliothèques partagées) de base (i386) | 11.10.0,REV=2005.01.21.16.34 |
| SUNWcslr | Bibliothèques de Solaris principales (racine) (i386) | 11.10.0, REV=2005.01.21.16.34 |
| Openssl | Bibliothèques SUNWopenssl ; Bibliothèques OpenSSL (Usr) (i386) | 11.10.0, REV=2005.01.21.16.34 |
| PAM | Modules d'authentification enfichables<br><br>Installation principale, Solaris, (Root) (i386) | 11.10.0,REV=2005.01.21.16.34 |

### Solaris 11 SPARC

| PACKAGE REQUIS | DESCRIPTION | VERSION MINIMALE |
|---|---|---|
| SUNWlibC | Sun Workshop Compilers Bundled libC | 5.11, REV=2011.04.11 |
| SUNWlibmsr | Bibliothèques Math & Microtasking (Root) | 5.11, REV=2011.04.11 |
| SUNWcslr | Core Solaris Libraries (Root) | 11.11, REV=2009.11.11 |
| SUNWcsl | Core Solaris, (Shared Libs) | 11.11, REV=2009.11.11 |
| SUNWcsr | Core Solaris, (Root) | 11.11, REV=2009.11.11 |
| SUNWopenssl-libraries | Bibliothèques OpenSSL (Usr) | 11.11.0,REV=2010.05.25.01.00 |

### Solaris 11 x86

| PACKAGE REQUIS | DESCRIPTION | VERSION MINIMALE |
|---|---|---|
| SUNWlibC | Sun Workshop Compilers Bundled libC | 5.11, REV=2011.04.11 |
| SUNWlibmsr | Bibliothèques Math & Microtasking (Root) | 5.11, REV=2011.04.11 |
| SUNWcslr | Core Solaris Libraries (Root) | 11.11, REV=2009.11.11 |
| SUNWcsl | Core Solaris, (Shared Libs) | 11.11, REV=2009.11.11 |
| SUNWcsr | Core Solaris, (Root) | 11.11, REV=2009.11.11 |
| SUNWopenssl-libraries | Bibliothèques OpenSSL (Usr) | 11.11.0,REV=2010.05.25.01.00 |

### SUSE Linux Enterprise Server 10 SP1 (i586)

| PACKAGE REQUIS | DESCRIPTION | VERSION MINIMALE |
|---|---|---|
| glibc-2,4-31,30 | Bibliothèque standard partagée C | 2.4-31.30 |
| OpenSSL | Bibliothèque OpenSSL, protocole de communication réseau sécurisé | 0.9.8a-18.15 |
| PAM | Modules d'authentification enfichables | 0.99.6.3-28.8 |

### SUSE Linux Enterprise Server 11 (i586)

| PACKAGE REQUIS | DESCRIPTION | VERSION MINIMALE |
|---|---|---|
| glibc-2.9-13.2 | Bibliothèque standard partagée C | 2.9-13.2 |
| PAM | Modules d'authentification enfichables | pam-1.0.2-20.1 |

### Universal Linux (Debian package) Debian, Ubuntu Server

| PACKAGE REQUIS | DESCRIPTION | VERSION MINIMALE |
|---|---|---|
| libc6 | Bibliothèque standard partagée C | 2.3.6 |
| Openssl | Bibliothèque OpenSSL, protocole de communication réseau sécurisé | 0.9.8 ou 1.0 |
| PAM | Modules d'authentification enfichables | 0.79-3 |

### Universal Linux (RPM package) CentOS, Oracle Linux

| PACKAGE REQUIS | DESCRIPTION | VERSION MINIMALE |
|---|---|---|
| glibc | Bibliothèque standard partagée C | 2.5-12 |

| PACKAGE REQUIS | DESCRIPTION | VERSION MINIMALE |
|---|---|---|
| Openssl | Bibliothèque OpenSSL, protocole de communication réseau sécurisé | 0.9.8 ou 1.0 |
| PAM | Modules d'authentification enfichables | 0.99.6.2-3.14 |

### IBM AIX 6.1

| PACKAGE REQUIS | DESCRIPTION | VERSION MINIMALE |
|---|---|---|
| Version du système d'exploitation | Version du système d'exploitation | AIX 6.1, technologie de tout niveau et tout Service Pack |
| xlC.rte | XL C/C++ Runtime | 9.0.0.5 |
| OpenSSL/openssl.base | Bibliothèque OpenSSL, protocole de communication réseau sécurisé | 0.9.8.4 |

### IBM AIX 7.1 (Power)

| PACKAGE REQUIS | DESCRIPTION | VERSION MINIMALE |
|---|---|---|
| Version du système d'exploitation | Version du système d'exploitation | AIX 7.1, technologie de tout niveau et tout Service Pack |
| xlC.rte | XL C/C++ Runtime | |
| OpenSSL/openssl.base | Bibliothèque OpenSSL, protocole de communication réseau sécurisé | |

### HP-UX 11i v3 IA64

| PACKAGE REQUIS | DESCRIPTION | VERSION MINIMALE |
|---|---|---|
| HPUX11i-OE | HP-UX Foundation Operating Environment | B.11.31.0709 |
| OS-Core.MinimumRuntime.CORE-SHLIBS | Bibliothèques spécifiques de développement IA | B.11.31 |
| SysMgmtMin | Outils minimum de déploiement logiciel | B.11.31.0709 |
| SysMgmtMin.openssl | Bibliothèque OpenSSL, protocole de communication réseau sécurisé | A.00.09.08d.002 |
| PAM | Modules d'authentification enfichables | Sous HP-UX, PAM fait partie des composants centraux du système d'exploitation. Il n'y a pas d'autre dépendance. |

**Dépendances de Configuration Manager :** le tableau suivant répertorie les rôles de système de site qui prennent en charge des clients Linux et UNIX. Pour plus d'informations sur ces rôles de système de site, consultez Déterminer les rôles de système de site pour les clients System Center Configuration Manager.

| SYSTÈME DE SITE CONFIGURATION MANAGER | PLUS D'INFORMATIONS |
| --- | --- |
| Point de gestion | Bien qu'un point de gestion ne soit pas nécessaire pour installer un client Configuration Manager pour Linux et UNIX, vous devez disposer d'un point de gestion pour transférer les informations entre les ordinateurs clients et les serveurs Configuration Manager. Sans point de gestion, vous ne pouvez pas gérer les ordinateurs clients. |
| Point de distribution | Le point de distribution n'est pas nécessaire pour installer un client Configuration Manager pour Linux et UNIX. Toutefois, le rôle de système de site est requis si vous déployez des logiciels sur des serveurs Linux et UNIX.<br><br>Dans la mesure où le client Configuration Manager pour Linux et UNIX ne prend pas en charge le protocole SMB, les points de distribution que vous utilisez avec le client doivent prendre en charge la communication HTTP ou HTTPS. |
| Point d'état de secours | Le point d'état de secours n'est pas nécessaire pour installer un client Configuration Manager pour Linux et UNIX. Toutefois, le point d'état de secours permet aux ordinateurs du site Configuration Manager d'envoyer des messages d'état quand ils ne peuvent pas communiquer avec un point de gestion. Client peut également envoyer leur état d'installation pour le point d'état de secours. |

**Pare-feu exigences**: Assurez-vous que les pare-feu ne bloquent pas les communications sur les ports que vous spécifiez en tant que ports de demande client. Le client pour Linux et UNIX communique directement avec les points de gestion, les points de distribution et les points d'état de secours.

Pour plus d'informations sur les ports de demande et de communication client, consultez Configurer le client pour Linux et UNIX pour qu'il localise des points de gestion.

## Planification des communications entre les approbations de forêts pour les serveurs Linux et UNIX

Les serveurs Linux et UNIX que vous gérez avec Configuration Manager fonctionnent comme des clients de groupe de travail et nécessitent des configurations similaires à celles des clients Windows situés dans un groupe de travail. Pour plus d'informations sur les communications à partir d'ordinateurs qui se trouvent dans des groupes de travail, consultez la section Communications dans les forêts Active Directory dans la rubrique Communications entre points de terminaison dans System Center Configuration Manager.

**Emplacement du service par le client pour Linux et UNIX**

La tâche de recherche d'un serveur de système de site qui fournit le service aux clients est appelée emplacement de service. Contrairement à un client fonctionnant sous Windows, le client pour Linux et UNIX n'utilise pas Active Directory pour l'emplacement de service. De plus, le client Configuration Manager pour Linux et UNIX ne prend pas en charge une propriété cliente qui spécifie le suffixe de domaine d'un point de gestion. Au lieu de cela, le client a eu connaissance des serveurs de système de site supplémentaires qui fournissent des services aux clients à partir d'un point de gestion connu que vous affectez lorsque vous installez le logiciel client.

Pour plus d'informations sur l'emplacement de service, consultez la section Emplacement du service et façon dont les clients déterminent leur point de gestion attribué dans la rubrique Comprendre comment les clients recherchent des services et des ressources de site pour System Center Configuration Manager.

## Planification de la sécurité et des certificats pour les serveurs Linux et

# UNIX

Pour des communications sécurisées et authentifiées avec les sites Configuration Manager, le client Configuration Manager pour Linux et UNIX utilise le même modèle de communication que le client Configuration Manager pour Windows.

Quand vous installez le client pour Linux et UNIX, vous pouvez lui affecter un certificat PKI qui lui permet d'utiliser le protocole HTTPS pour communiquer avec les sites Configuration Manager. Si vous n'affectez pas un certificat PKI, le client crée un certificat auto-signé et communique uniquement par HTTP.

Les clients qui sont fournis un certificat PKI lorsqu'ils installent utilisent HTTPS pour communiquer avec les points de gestion. Lorsqu'un client est impossible de trouver un point de gestion qui prend en charge le protocole HTTPS, il revient pour utiliser HTTP avec le certificat PKI fourni.

Lorsqu'un client Linux ou UNIX utilise un certificat PKI vous n'êtes pas obligé de les approuver. Quand un client utilise un certificat auto-signé, passez en revue les paramètres de hiérarchie pour l'approbation du client dans la console Configuration Manager. Si la méthode d'approbation du client n'est pas **Approuver automatiquement tous les ordinateurs (non recommandés)**, vous devez approuver manuellement le client.

Pour plus d'informations sur l'approbation manuelle du client, consultez la section Gérer les clients à partir du nœud Appareils dans la rubrique Comment gérer les clients dans System Center Configuration Manager.

Pour plus d'informations sur l'utilisation des certificats dans Configuration Manager, consultez Configuration requise des certificats PKI pour System Center Configuration Manager.

**À propos des certificats pour les serveurs Linux et UNIX**

Le client Configuration Manager pour Linux et UNIX utilise un certificat auto-signé ou un certificat PKI X.509, comme les clients Windows. Aucune modification des exigences PKI pour les systèmes de site Configuration Manager n'est nécessaire quand vous gérez des clients Linux et UNIX.

Les certificats utilisés pour les clients Linux et UNIX qui communiquent avec les systèmes de site Configuration Manager doivent être au format PKCS#12 (Public Key Certificate Standard). De plus, vous devez connaître le mot de passe pour pouvoir l'indiquer au client quand vous spécifiez le certificat PKI.

Le client Configuration Manager pour Linux et UNIX ne prend en charge qu'un seul certificat PKI. Il ne prend pas en charge plusieurs certificats. Ainsi, les critères de sélection de certificat que vous configurez pour un site Configuration Manager ne s'appliquent pas.

**Configuration de certificats pour les serveurs Linux et UNIX**

Pour configurer l'utilisation des communications HTTPS par un client Configuration Manager pour les serveurs Linux et UNIX, vous devez configurer le client pour qu'il utilise un certificat PKI au moment de son installation. Vous ne pouvez pas configurer un certificat avant l'installation du logiciel client.

Lorsque vous installez un client qui utilise un certificat PKI, vous utilisez le paramètre de ligne de commande **-/usepkicert** pour spécifier l'emplacement et le nom d'un fichier PKCS #12 qui contient le certificat PKI. En outre, vous devez utiliser le paramètre de ligne de commande **- certpw** pour spécifier le mot de passe du certificat.

Si vous ne spécifiez pas **- /usepkicert**, le client génère un certificat auto-signé et tente de communiquer avec les serveurs de système de site via le protocole HTTP uniquement.

# À propos des systèmes d'exploitation Linux et UNIX qui ne prennent pas en charge SHA-256

Les systèmes d'exploitation Linux et UNIX suivants, pris en charge en tant que clients pour Configuration Manager, ont été publiés avec des versions d'OpenSSL qui ne prennent pas en charge SHA-256 :

- Solaris Version 10 (SPARC/x86)

Pour gérer ces systèmes d'exploitation avec Configuration Manager, vous devez installer le client Configuration Manager pour Linux et UNIX avec un commutateur de ligne de commande qui indique au client d'ignorer la validation de SHA-256. Les clients Configuration Manager qui s'exécutent sur ces versions de système d'exploitation fonctionnent dans un mode moins sécurisé que les clients qui prennent en charge SHA-256. Ce mode de fonctionnement moins sécurisé a le comportement suivant :

- Les clients ne valident pas la signature de serveur de site associée qu'ils demandent à partir d'un point de gestion de stratégie.
- Les clients ne valident pas le hachage des packages qu'ils téléchargent à partir d'un point de distribution.

> **IMPORTANT**
> Le **ignoreSHA256validation** option permet d'exécuter le client pour les ordinateurs Linux et UNIX en mode moins sécurisé. Cela est voulu pour une utilisation sur des plates-formes plus anciennes qui n'inclut pas de prise en charge de l'algorithme SHA-256. Ceci est un remplacement de la sécurité et n'est pas recommandé par Microsoft, mais est pris en charge pour une utilisation dans un environnement de centre de données sécurisé et fiable.

Durant l'installation du client Configuration Manager pour Linux et UNIX, le script d'installation vérifie la version du système d'exploitation. Par défaut, si la version du système d'exploitation est identifiée comme ayant été publiée sans une version d'OpenSSL prenant en charge SHA-256, l'installation du client Configuration Manager se solde par un échec.

Pour installer le client Configuration Manager sur les systèmes d'exploitation Linux et UNIX qui n'ont pas été publiés avec une version d'OpenSSL prenant en SHA-256, vous devez utiliser le commutateur de ligne de commande **ignoreSHA256validation**. Quand vous utilisez cette option de ligne de commande sur un système d'exploitation Linux ou UNIX applicable, le client Configuration Manager ignore la validation de SHA-256. Une fois l'installation effectuée, le client n'utilise pas SHA-256 pour signer les données qu'il envoie aux systèmes de site via HTTP. Pour plus d'informations sur la configuration des clients Linux et UNIX pour utiliser des certificats, consultez Planning for Security and Certificates for Linux and UNIX Servers dans cette rubrique. Pour plus d'informations sur l'utilisation de SHA-256, consultez la section Configurer la signature et le chiffrement dans la rubrique Configurer la sécurité dans System Center Configuration Manager.

> **NOTE**
> L'option de ligne de commande **ignoreSHA256validation** est ignorée sur les ordinateurs qui exécutent une version de Linux et UNIX publié avec les versions d'OpenSSL qui prennent en charge SHA-256.

# Planification du déploiement du client pour les ordinateurs Mac dans System Center Configuration Manager

22/06/2018 • 3 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez installer le client Configuration Manager sur des ordinateurs Mac qui exécutent le système d'exploitation Mac OS X et utilisent les fonctionnalités de gestion suivantes :

- **Inventaire matériel**

  Vous pouvez utiliser l'inventaire matériel de Configuration Manager pour collecter des informations sur le matériel et les applications installées sur des ordinateurs Mac. Consultez ensuite ces informations dans l'Explorateur de ressources dans la console Configuration Manager et utilisez-les pour créer des regroupements, des requêtes et des rapports. Pour plus d'informations, consultez Guide pratique pour utiliser l'Explorateur de ressources pour afficher l'inventaire matériel dans System Center Configuration Manager.

  Configuration Manager collecte les informations matérielles suivantes auprès des ordinateurs Mac :

  - Processeur
  - Système informatique
  - Lecteur de disque
  - Partition de disque
  - Carte réseau
  - Système d'exploitation
  - Service
  - Processus
  - Logiciel installé
  - Produit système informatique
  - Contrôleur USB
  - Périphérique USB
  - Lecteur de CD-ROM
  - Contrôleur vidéo
  - Moniteur du Bureau
  - Batterie portable
  - Mémoire physique
  - Imprimante

> **IMPORTANT**
> Vous ne pouvez pas étendre les informations matérielles collectées à partir d'ordinateurs Mac pendant un inventaire matériel.

- **Paramètres de compatibilité**

  Vous pouvez utiliser les paramètres de compatibilité de Configuration Manager pour afficher la compatibilité des paramètres de préférence (.plist) Mac OS X et les corriger. Par exemple, vous pouvez appliquer des paramètres pour la page d'accueil du navigateur web Safari ou veiller à ce que le pare-feu Apple soit activé. Vous pouvez également utiliser des scripts Shell pour surveiller et corriger des paramètres dans MAC OS X.

- **Gestion des applications**

  Configuration Manager peut déployer des logiciels sur les ordinateurs Mac. Vous pouvez déployer les formats logiciels suivants sur les ordinateurs Mac :

  - Image disque Apple (.DMG)
  - Fichier métapaquet (.MPKG)
  - Paquet d'installation Mac OS X (.PKG)
  - Application Mac OS X (.APP)

  Quand vous installez le client Configuration Manager sur des ordinateurs Mac, vous ne pouvez pas utiliser les fonctionnalités de gestion suivantes prises en charge par le client Configuration Manager sur les ordinateurs Windows :

- Installation poussée du client
- Déploiement du système d'exploitation
- Mises à jour logicielles

  > **NOTE**
  > Vous pouvez utiliser la gestion des applications Configuration Manager pour déployer des mises à jour logicielles Mac OS X requises sur les ordinateurs Mac. En outre, vous pouvez utiliser des paramètres de conformité pour vous assurer que les ordinateurs disposent des mises à jour logicielles requises.

- Fenêtres de maintenance
- Contrôle à distance
- Gestion de l'alimentation
- Vérification et correction de l'état du client

  Pour plus d'informations sur la manière d'installer et de configurer le client Mac Configuration Manager, consultez Guide pratique pour déployer des clients sur des Mac dans System Center Configuration Manager.

# Planification du déploiement de clients sur des appareils Windows Embedded dans System Center Configuration Manager

04/06/2018 • 10 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Si votre appareil Windows Embedded n'inclut pas le client System Center Configuration Manager, vous pouvez utiliser l'une des méthodes d'installation de ce client si l'appareil respecte les dépendances requises. Si l'appareil intégré prend en charge les filtres d'écriture, vous devez désactiver ces filtres avant d'installer le client, puis réactiver les filtres une fois le client installé et attribué à un site.

Notez que quand vous désactivez les filtres, vous ne devez pas désactiver les pilotes de filtre. En général, ces pilotes démarrent automatiquement au démarrage de l'ordinateur. La désactivation de ces pilotes empêche l'installation du client ou interfère avec l'orchestration des filtres d'écriture, ce qui entraîne l'échec des opérations du client. Voici les services associés à chaque type de filtre d'écriture devant rester en cours d'exécution :

| TYPE DE FILTRE D'ÉCRITURE | PILOTE | TAPEZ | DESCRIPTION |
|---|---|---|---|
| EWF | EWF | Noyau | Met en œuvre la redirection des E/S au niveau du secteur sur les volumes protégés. |
| FBWF | FBWF | Système de fichiers | Met en œuvre la redirection des E/S au niveau du fichier sur les volumes protégés. |
| UWF | uwfreg | Noyau | Redirecteur de Registre UWF |
| UWF | uwfs | Système de fichiers | Redirecteur de fichier UWF |
| UWF | uwfvol | Noyau | Gestionnaire de volume UWF |

Les filtres d'écritures contrôlent la manière dont le système d'exploitation sur l'appareil intégré est mis à jour lorsque vous apportez des modifications, comme lorsque vous installez des logiciels. Lorsque les filtres d'écriture sont activés, au lieu d'apporter les modifications directement dans le système d'exploitation, celles-ci sont redirigées vers un segment de recouvrement temporaire. Si les modifications sont écrites uniquement dans le segment de recouvrement, elles sont perdues lorsque l'appareil intégré s'arrête. Toutefois, si les filtres d'écriture sont temporairement désactivés, les modifications peuvent être rendues définitives afin que vous n'ayez pas à les apporter de nouveau (ou à réinstaller le logiciel) à chaque redémarrage de l'appareil intégré. Cependant, la désactivation temporaire suivie de la réactivation de ces filtres d'écriture requiert un ou plusieurs redémarrages, si bien qu'il est souhaitable de les contrôler en configurant des fenêtres de maintenance permettant aux redémarrages de se produire en dehors des heures de bureau.

Vous pouvez configurer des options pour désactiver et réactiver automatiquement les filtres d'écriture quand vous déployez des logiciels tels que des applications, des séquences de tâches, des mises à jour logicielles et le client Endpoint Protection. Il existe une exception pour les lignes de base de configuration comportant des éléments de configuration qui utilisent une correction automatique. Dans ce scénario, la correction se produit toujours dans le segment de recouvrement afin d'être disponible uniquement jusqu'au redémarrage de l'appareil.

La correction est appliquée de nouveau lors du prochain cycle d'évaluation, mais uniquement au segment de recouvrement, lequel est effacé au redémarrage. Pour forcer Configuration Manager à valider les modifications de la correction, vous pouvez déployer la ligne de base de configuration, puis un autre déploiement logiciel qui prend en charge la validation de la modification dès que possible.

Si les filtres d'écriture sont désactivés, vous pouvez installer des logiciels sur les appareils Windows Embedded à l'aide du Centre logiciel. Toutefois, si les filtres d'écriture sont activés, l'installation échoue et Configuration Manager affiche un message d'erreur indiquant que vos autorisations ne sont pas suffisantes pour installer l'application.

> **WARNING**
> Même si vous ne sélectionnez pas les options Configuration Manager permettant de valider les modifications, celles-ci peuvent l'être si une autre installation logicielle ou modification est effectuée en ce sens. Dans ce scénario, les modifications d'origine sont validées en plus des nouvelles modifications.

Quand Configuration Manager désactive les filtres d'écriture pour rendre les modifications définitives, seuls les utilisateurs qui possèdent des droits administratifs locaux peuvent se connecter et utiliser l'appareil intégré. Pendant cette période, les utilisateurs dont les droits sont peu élevés sont verrouillés et ils voient un message indiquant que l'ordinateur n'est pas disponible car il est en cours de maintenance. Cette indisponibilité protège l'appareil pendant que son état permet l'application de modifications définitives et ce comportement de verrouillage du mode de maintenance constitue une autre raison pour configurer une fenêtre de maintenance pendant laquelle les utilisateurs ne se connectent pas à ces appareils.

Configuration Manager prend en charge la gestion des types de filtres d'écriture suivants :

- Filtre d'écriture basé sur des fichiers (FBWF) : pour plus d'informations, consultez Filtre d'écriture basé sur des fichiers.
- RAM de filtre d'écriture amélioré (EWF) : pour plus d'informations, consultez Filtre d'écriture amélioré.
- Filtre d'écriture unifié (UWF) : pour plus d'informations, consultez Filtre d'écriture unifié.

  Configuration Manager ne prend pas en charge les opérations de filtre d'écriture quand l'appareil Windows Embedded est en mode de registre RAM EWF.

**IMPORTANT**

Si vous avez le choix, utilisez des filtres d'écriture basés sur des fichiers avec Configuration Manager pour une efficacité accrue et une meilleure évolutivité.

**Pour les appareils qui utilisent des filtres d'écriture basés sur des fichiers uniquement :** configurez les exceptions suivantes pour rendre permanents l'état du client et les données d'inventaire entre les redémarrages de l'appareil :

- CCMINSTALLDIR*.sdf
  - CCMINSTALLDIR\ServiceData
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CCM\StateSystem

  Les appareils qui exécutent Windows Embedded 8.0 et ses versions ultérieures ne prennent pas en charge les exclusions qui contiennent des caractères génériques. Sur ces appareils, vous devez configurer individuellement les exclusions suivantes :

- Tous les fichiers dans CCMINSTALLDIR portant l'extension .sdf, généralement :
  - UserAffinityStore.sdf
  - InventoryStore.sdf
  - CcmStore.sdf
  - StateMessageStore.sdf
  - CertEnrollmentStore.sdf
  - CCMINSTALLDIR\ServiceData
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CCM\StateSystem

**Pour les appareils qui utilisent des filtres d'écriture basés sur des fichiers et des filtres d'écriture unifiés :** quand les clients d'un groupe de travail utilisent des certificats à des fins d'authentification auprès de points de gestion, vous devez également exclure la clé privée pour que les clients puissent continuer à communiquer avec les points de gestion. Sur ces appareils, configurez les exceptions suivantes :

- c:\Windows\System32\Microsoft\Protect
  - c:\ProgramData\Microsoft\Crypto
  - HKEY_LOCAL_MACHINE\Software\Microsoft\SystemCertificates\SMS\Certificates

Pour obtenir un exemple de scénario de déploiement et de gestion d'appareils Windows Embedded avec des filtres d'écriture activés dans Configuration Manager, consultez Exemple de scénario de déploiement et de gestion de clients System Center Configuration Manager sur des appareils Windows Embedded.

Pour plus d'informations sur la façon de créer des images pour les appareils Windows Embedded et de configurer des filtres d'écriture, reportez-vous à votre documentation Windows Embedded ou contactez votre fabricant d'ordinateurs OEM.

**NOTE**

Lorsque vous sélectionnez les plates-formes applicables aux déploiements logiciels et aux éléments de configuration, celles-ci affichent les familles Windows Embedded, plutôt que des versions spécifiques. Utilisez la liste suivante pour faire correspondre la version spécifique de Windows Embedded aux options figurant dans la zone de liste :

- L'option**Systèmes d'exploitation intégrés basés sur Windows XP (32 bits)** inclut les éléments suivants :
  - Windows XP Embedded
  - Windows Embedded for Point of Service
  - Windows Embedded Standard 2009
  - Windows Embedded POSReady 2009
  - L'option**Systèmes d'exploitation intégrés basés sur Windows 7 (32 bits)** inclut les éléments suivants :
  - Windows Embedded Standard 7 (32 bits)
  - Windows Embedded POSReady 7 (32 bits)
  - Windows ThinPC
  - L'option**Systèmes d'exploitation intégrés basés sur Windows 7 (64 bits)** inclut les éléments suivants :
  - Windows Embedded Standard 7 (64 bits)
  - Windows Embedded POSReady 7 (64 bits)

# Exemple de scénario de déploiement et de gestion de clients System Center Configuration Manager sur des appareils Windows Embedded

22/06/2018 • 23 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Ce scénario montre comment vous pouvez gérer des appareils Windows Embedded activés pour les filtres d'écriture avec Configuration Manager. Si vos appareils incorporés ne prennent pas en charge les filtres d'écriture, ils se comportent comme des clients Configuration Manager standard et ces procédures ne s'appliquent pas.

Coho Vineyard & Winery ouvre un centre d'accueil et a besoin de bornes qui utilisent Windows Embedded pour exécuter des présentations interactives. Le bâtiment du nouveau centre d'accueil n'étant pas proche du service informatique, les bornes doivent être gérées à distance. Outre le logiciel qui exécute les présentations, ces appareils doivent exécuter des logiciels anti-programmes malveillants actualisés pour se conformer aux stratégies de sécurité de l'entreprise. Les bornes doivent fonctionner 7 jours par semaine, sans interruption pendant les heures d'ouverture du centre d'accueil.

Coho utilise déjà Configuration Manager pour gérer les appareils de son réseau. Configuration Manager est configuré pour exécuter Endpoint Protection et pour installer les mises à jour logicielles et les applications. Toutefois, sachant que l'équipe informatique n'a jamais géré d'appareils Windows Embedded auparavant, Jane, administratrice de Configuration Manager, a mis en place un pilote pour gérer deux bornes situées dans le hall de réception.

Pour gérer ces appareils Windows Embedded à filtre d'écriture, Jane effectue les étapes suivantes pour installer le client Configuration Manager, le protéger à l'aide d'Endpoint Protection et installer le logiciel de présentation interactive.

1. Jane s'informe de la manière dont les appareils Windows Embedded utilisent les filtres d'écriture, puis de la manière dont Configuration Manager peut simplifier cette utilisation en désactivant, puis en réactivant automatiquement ces filtres d'écriture, dans le but de conserver une installation logicielle.

   Pour plus d'informations, consultez Planification du déploiement de clients sur des appareils Windows Embedded dans System Center Configuration Manager.

2. Avant d'installer le client Configuration Manager, Jane crée un regroupement d'appareils basé sur une requête pour les appareils Windows Embedded. Comme l'entreprise utilise des formats d'attribution de noms standard pour identifier ses ordinateurs, Jane peut identifier les appareils Windows Embedded de façon univoque par les six premières lettres du nom de l'ordinateur : **WEMDVC**. Elle utilise la requête WQL suivante pour créer ce regroupement : **select SMS_R_System.NetbiosName from SMS_R_System where SMS_R_System.NetbiosName like "WEMDVC%"**

   Ce regroupement lui permet de gérer les appareils Windows Embedded avec des options de configuration différentes des autres appareils. Elle utilise ce regroupement pour contrôler les redémarrages, déployer Endpoint Protection avec les paramètres du client et déployer l'application de présentation interactive.

   Voir Comment créer des regroupements dans System Center Configuration Manager.

3. Jane configure le regroupement pendant une fenêtre de maintenance pour veiller à ce que les redémarrages nécessaires pour installer l'application de présentation et toutes les éventuelles mises à jour ne se produisent pas pendant les heures d'ouverture du centre d'accueil. Le centre est ouvert de 9h00 à

18h00, du lundi au dimanche. Elle configure la fenêtre de maintenance de sorte à ce qu'elle se produise tous les jours, de 18h30 à 6h00.

4. Pour plus d'informations, consultez Guide pratique pour utiliser les fenêtres de maintenance dans System Center Configuration Manager.

5. Jane configure ensuite un paramètre client personnalisé pour les appareils en vue d'installer le client Endpoint Protection en sélectionnant **Oui** pour les paramètres suivants, puis elle déploie ce paramètre client personnalisé sur le regroupement d'appareils Windows Embedded :

   - **Installer le client Endpoint Protection sur les ordinateurs clients**
   - **Pour les appareils Windows Embedded munis de filtres d'écriture, valider l'installation du client Endpoint Protection (nécessite un redémarrage)**
   - **Autoriser l'installation et le redémarrage du client Endpoint Protection en dehors des fenêtres de maintenance**

     Quand le client Configuration Manager est installé, ces paramètres permettent d'installer le client Endpoint Protection et de garantir qu'il est maintenu dans le système d'exploitation pendant l'installation, au lieu d'être seulement écrit dans le segment de recouvrement. Les stratégies de sécurité de l'entreprise exigent une installation permanente du logiciel anti-programme malveillant et Jane ne veut pas prendre le risque de laisser les bornes sans protection même pendant un court instant alors qu'ils redémarrent.

   > **NOTE**
   > Les redémarrages requis pour installer le client Endpoint Protection ne se produisent qu'une seule fois, pendant la période d'installation des appareils et avant que le centre d'accueil ne soit opérationnel. À la différence du déploiement périodique d'applications ou de mises à jour de définitions logicielles, la prochaine installation du client Endpoint Protection sur le même appareil aura probablement lieu quand l'entreprise procédera à la mise à niveau vers la prochaine version de Configuration Manager.

   Pour plus d'informations, consultez Configuration d'Endpoint Protection dans System Center Configuration Manager.

6. Maintenant que les paramètres de configuration du client sont en place, Jane prépare l'installation des clients Configuration Manager. Avant de pouvoir installer les clients, elle doit désactiver manuellement le filtre d'écriture sur les appareils Windows Embedded. Elle lit la documentation du fabricant qui accompagne les bornes et suit les instructions pour désactiver les filtres d'écriture.

   Jane renomme l'appareil pour qu'il utilise le format d'attribution de noms standard de l'entreprise, puis elle installe le client manuellement en exécutant CCMSetup à l'aide de la commande suivante, à partir d'un lecteur mappé qui contient les fichiers sources du client : **CCMSetup.exe /MP:mpserver.cohovineyardandwinery.com SMSSITECODE=CO1**

   Cette commande permet d'installer le client, d'affecter le client au point de gestion dont le nom de domaine complet de l'intranet est **mpserver.cohovineyardandwinery.com**, puis d'affecter le client au site principal nommé **CO1**.

   Jane sait qu'il faut toujours un certain temps pour que les clients s'installent et renvoient leur état au site. Par conséquent, elle patiente avant de confirmer l'installation correcte des clients, leur affectation au site et leur affichage en tant que clients dans le regroupement qu'elle a créé pour les appareils Windows Embedded.

   Comme contrôle supplémentaire, elle vérifie les propriétés de Configuration Manager dans le Panneau de configuration sur les appareils et les compare aux ordinateurs Windows standard gérés par le site. Par

exemple, sous l'onglet **Composants** , l'élément **Agent de l'inventaire matériel** affiche **Activé**et sous l'onglet **Actions** figurent 11 actions disponibles, notamment **Cycle d'évaluation du déploiement de l'application** et **Cycle de collecte de données de découverte**.

Certaine que les clients sont correctement installés et affectés, et que le point de gestion leur envoie la stratégie client, Jane active ensuite manuellement les filtres d'écriture en suivant les instructions du fabricant.

Pour plus d'informations, voir :

- Guide pratique pour déployer des clients sur des ordinateurs Windows dans System Center Configuration Manager
- Guide pratique pour affecter des clients à un site dans System Center Configuration Manager

7. Maintenant que le client Configuration Manager est installé sur les appareils Windows Embedded, Jane vérifie qu'elle peut les gérer de la même manière que les clients Windows standard. Par exemple, à partir de la console Configuration Manager, elle peut les gérer à distance à l'aide du contrôle à distance, leur appliquer la stratégie et afficher les propriétés du client, ainsi que l'inventaire matériel.

   Comme ces appareils sont joints à un domaine Active Directory, elle n'a pas besoin de les confirmer manuellement en tant que clients approuvés ; pour cela, elle utilise la console Configuration Manager.

   Pour plus d'informations, voir Comment gérer des clients dans Configuration Manager.

8. Pour installer le logiciel de présentation interactive, Jane exécute l' **Assistant Déploiement logiciel** et configure une application requise. Sur la page **Expérience utilisateur** de l'Assistant, dans la section **Traitement des filtres d'écriture pour les appareils Windows Embedded** , elle accepte l'option par défaut qui sélectionne **Valider les changements à l'échéance ou pendant une fenêtre de maintenance (redémarrage requis)**.

   Jane garde cette option par défaut pour les filtres d'écriture pour garantir la conservation de l'application après un redémarrage, afin qu'elle soit toujours disponible pour les visiteurs qui utilisent les bornes. La fenêtre de maintenance quotidienne offre une période sans risque au cours de laquelle les redémarrages d'installation et les mises à jour peuvent se produire.

   Jane déploie l'application sur le regroupement d'appareils Windows Embedded.

   Pour plus d'informations, consultez Comment déployer des applications avec System Center Configuration Manager.

9. Pour configurer les mises à jour de définitions pour Endpoint Protection, Jane utilise des mises à jour logicielles et exécute l'Assistant Création d'une règle de déploiement automatique. Elle sélectionne le modèle **Mises à jour de définitions** pour préremplir l'Assistant avec les paramètres appropriés à Endpoint Protection.

   Ces paramètres incluent les éléments suivants sur la page **Expérience utilisateur** de l'Assistant :

   - **Comportement à l'échéance**: la case **Installation du logiciel** n'est pas cochée.
   - **Traitement des filtres d'écriture pour les appareils Windows Embedded**: la case **Valider les changements à l'échéance ou pendant une fenêtre de maintenance (redémarrage requis)** n'est pas cochée.

     Jane conserve ces paramètres par défaut. Associées à cette configuration, ces deux options permettent d'installer toutes les définitions de mises à jour logicielles pour Endpoint Protection dans le segment de recouvrement pendant la journée, sans attendre leur installation et leur validation au cours de la fenêtre de maintenance. Cette configuration respecte mieux la stratégie de sécurité de l'entreprise en ce qui concerne l'exécution par les ordinateurs d'une protection actualisée contre les

programmes malveillants.

> **NOTE**
> Contrairement aux installations logicielles des applications, les définitions de mises à jour logicielles pour Endpoint Protection peuvent se produire très fréquemment, voire même plusieurs fois par jour. Il s'agit souvent de petits fichiers. Pour ces types de déploiements liés à la sécurité, il s'avère souvent bénéfique de toujours procéder à l'installation dans le segment de recouvrement plutôt que d'attendre la fenêtre de maintenance. Le client Configuration Manager réinstalle rapidement les mises à jour de définitions logicielles si le l'appareil redémarre, car cette action lance un contrôle d'évaluation sans attendre la prochaine évaluation planifiée.

Jane sélectionne le regroupement d'appareils Windows Embedded pour la règle de déploiement automatique.

Pour plus d'informations, voir
Étape 3 : configurer les mises à jour logicielles de Configuration Manager pour fournir des mises à jour de définitions aux ordinateurs clients dans Configuration d'Endpoint Protection dans System Center Configuration Manager

10. Jane décide de configurer une tâche de maintenance qui valide régulièrement toutes les modifications apportées au segment de recouvrement. Cette tâche consiste à prendre en charge le déploiement des définitions de mises à jour logicielles, afin de réduire le nombre de mises à jour qui s'accumulent et doivent être à nouveau installées, chaque fois que l'appareil redémarre. Elle sait, par expérience, que cela permet aux logiciels anti-programmes malveillants de s'exécuter plus efficacement.

> **NOTE**
> Ces définitions de mises à jour logicielles seraient automatiquement validées dans l'image si les appareils embarqués exécutaient une autre tâche de gestion prenant en charge la validation des modifications. Par exemple, l'installation d'une nouvelle version du logiciel de présentation interactive permettrait également de valider les modifications pour les définitions de mises à jour logicielles. Ou bien, l'installation mensuelle de mises à jour logicielles standard au cours de la fenêtre de maintenance permettrait également de valider les modifications pour les définitions de mises à jour logicielles. En revanche, dans ce scénario, où les mises à jour logicielles standard ne s'exécutent pas et le logiciel de présentation interactive a peu de chances d'être souvent mis à jour, des mois peuvent passer avant que les mises à jour de définitions logicielles ne soient automatiquement validées dans l'image.

Jane crée d'abord une séquence de tâches personnalisée sans autre paramètre que le nom. Elle exécute l'Assistant Création d'une séquence de tâches :

a. Sur la page **Créer une séquence de tâches** , sélectionnez **Créez une séquence de tâches personnalisée**, puis cliquez sur **Suivant**.

b. Sur la page **Informations sur la séquence de tâches** , elle entre **Maintenance task to commit changes on embedded devices** pour le nom de la séquence de tâches, puis clique sur **Suivant**.

c. Sur la page **Résumé** , elle sélectionne **Suivant**et termine l'Assistant.

Jane déploie ensuite cette séquence de tâches personnalisée sur le regroupement d'appareils Windows Embedded, puis elle configure la planification pour une exécution mensuelle. Dans le cadre des paramètres de déploiement, elle active la case à cocher **Valider les changements à l'échéance ou pendant une fenêtre de maintenance (redémarrage requis)** pour conserver les modifications après un redémarrage. Pour configurer ce déploiement, elle sélectionne la séquence de tâches personnalisée qu'elle vient de créer, puis sous l'onglet **Accueil** , dans le groupe **Déploiement** , elle clique sur **Déployer** pour démarrer l'Assistant Déploiement logiciel :

d. Sur la page **Général** , elle sélectionne le regroupement d'appareils Windows Embedded, puis elle clique sur **Suivant**.

e. Sur la page **Paramètres de déploiement** , elle sélectionne **Obligatoire** pour l'option **Objet**, puis elle clique sur **Suivant**.

f. Sur la page **Planification** , elle clique sur **Nouveau** pour spécifier une planification hebdomadaire au cours de la fenêtre de maintenance, puis elle clique sur **Suivant**.

g. Elle termine l'Assistant sans apporter d'autres modifications.

Pour plus d'informations, voir
Gérer les séquences de tâches pour automatiser des tâches dans System Center Configuration Manager.

11. Pour que les bornes fonctionnent automatiquement, Jane écrit un script permettant de configurer les appareils comme suit :

- Ouverture de session automatique via un compte invité sans mot de passe.
- Exécution automatique du logiciel de présentation interactive au démarrage.

Jane utilise des packages et des programmes pour déployer ce script sur le regroupement d'appareils Windows Embedded. Lors de l'exécution de l'Assistant Déploiement logiciel, elle active là encore la case à cocher **Valider les changements à l'échéance ou pendant une fenêtre de maintenance (redémarrage requis)** pour conserver les modifications après un redémarrage.

Pour plus d'informations, consultez Packages et programmes dans System Center Configuration Manager.

12. Le matin suivant, Jane contrôle les appareils Windows Embedded. Elle vérifie les éléments suivants :

- La borne a ouvert automatiquement une session en utilisant le compte invité.
- Le logiciel de présentation interactive est en cours d'exécution.
- Le client Endpoint Protection est installé et dispose des dernières définitions de mises à jour logicielles.
- L'appareil a bien redémarré au cours de la fenêtre de maintenance.

Pour plus d'informations, voir :

- Guide pratique pour surveiller Endpoint Protection dans System Center Configuration Manager
- Surveiller des applications avec System Center Configuration Manager

13. Jane surveille les bornes et indique à son responsable que ces bornes sont correctement gérées. Ainsi, le centre d'accueil passe une commande de 20 bornes.

Pour éviter de devoir installer manuellement le client Configuration Manager, ce qui nécessiterait de désactiver et d'activer manuellement les filtres d'écriture, Jane s'assure que la commande comprend une image personnalisée qui intègre déjà l'installation et l'affectation de site du client Configuration Manager. En outre, les noms des appareils sont attribués conformément au format choisi par la société.

Les bornes sont livrées au centre d'accueil une semaine après son ouverture. Pendant ce laps de temps, les bornes sont connectées au réseau. Toutes les opérations de gestion des appareils sont automatisées et aucun administrateur n'est requis localement. Jane vérifie que les bornes fonctionnent comme prévu :

- Les clients installés sur les bornes réalisent une attribution de site et téléchargent la clé racine approuvée auprès des services de domaine Active Directory.

- Les clients installés sur les bornes sont ajoutés automatiquement au regroupement d’appareils Windows Embedded et leur fenêtre de maintenance est configurée.
- Le client Endpoint Protection est installé et dispose des dernières définitions de mises à jour logicielles, pour la protection contre les programmes malveillants.
- Le logiciel de présentation interactive est installé et s'exécute automatiquement. Il est entièrement prêt à l'emploi pour les visiteurs.

14. Au terme de cette configuration initiale, les redémarrages éventuellement nécessaires pour l'installation des mises à jour ont lieu seulement lorsque le centre d'accueil est fermé au public.

# Planifier la sortie de veille des clients dans System Center Configuration Manager

26/06/2018 • 15 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Configuration Manager prend en charge les paquets de mise en éveil traditionnels permettant de réveiller les ordinateurs en mode veille lorsque vous souhaitez installer le logiciel requis, par exemple des mises à jour logicielles et des applications.

Vous pouvez compléter la méthode traditionnelle des paquets de mise en éveil par des paramètres de client de proxy de mise en éveil. Le proxy de mise en éveil utilise un protocole entre homologues et des ordinateurs sélectionnés pour vérifier si les autres ordinateurs du sous-réseau sont éveillés et les sortir de veille si nécessaire. Lorsque le site est configuré pour l'éveil par appel réseau (Wake On LAN) et les clients configurés pour le proxy de mise en éveil, le processus fonctionne comme suit :

1. Les ordinateurs dotés du client Configuration Manager qui ne sont pas en veille sur le sous-réseau vérifient si les autres ordinateurs du sous-réseau sont éveillés. Pour effectuer cette vérification, ils s'envoient une commande ping TCP/IP toutes les cinq secondes.

2. Si les autres ordinateurs ne répondent pas, ils sont considérés comme étant en veille. Les ordinateurs qui ne sont pas en veille deviennent *ordinateurs gestionnaires* du sous-réseau.

   Étant donné qu'un ordinateur risque ne pas répondre pour une raison autre que la veille (par exemple, s'il est éteint, supprimé du réseau ou si le paramètre client de mise en éveil du proxy n'est plus appliqué), les ordinateurs reçoivent un paquet de mise en éveil tous les jours à 14h00, heure locale. Les ordinateurs qui ne répondent pas ne sont plus considérés comme étant en veille et ne sont pas mis en éveil par le proxy de mise en éveil.

   Pour prendre en charge un proxy de mise en éveil, au moins trois ordinateurs doivent être sortis de veille pour chaque sous-réseau. Pour remplir cette condition, trois ordinateurs sont choisis sans déterminisme en tant que *gardiens* du sous-réseau. Cet état signifie qu'ils restent éveillés, malgré toute stratégie d'alimentation configurée pour la mise en veille ou la mise en veille prolongée à l'issue d'une période d'inactivité. Les gardiens respectent les commandes d'arrêt ou de redémarrage, par exemple, consécutivement à des tâches de maintenance. Dans ce cas, les gardiens restants mettent en éveil un autre ordinateur du sous-réseau afin que le sous-réseau continue à disposer de trois gardiens.

3. Les ordinateurs gestionnaires demandent au commutateur réseau de rediriger le trafic réseau des ordinateurs en veille vers eux-mêmes.

   La redirection est accomplie par l'ordinateur gestionnaire qui émet une trame Ethernet qui utilise l'adresse MAC de l'ordinateur en veille comme adresse source. Ce comportement permet au commutateur réseau de se comporter comme si l'ordinateur en veille avait été déplacé vers le même port que celui sur lequel se trouve l'ordinateur gestionnaire. L'ordinateur gestionnaire envoie également des paquets ARP pour que les ordinateurs en veille conservent l'entrée actualisée dans le cache ARP. L'ordinateur gestionnaire répond également aux requêtes ARP au nom de l'ordinateur en veille en utilisant l'adresse MAC de cet ordinateur en veille.

> **WARNING**
> Pendant ce processus, le mappage IP vers MAC de l'ordinateur en veille reste le même. Le proxy de mise en éveil fonctionne en informant le commutateur réseau qu'une autre carte réseau utilise le port qui a été enregistré par une autre carte réseau. Toutefois, ce comportement est connu sous le nom de bagottement MAC et il est inhabituel dans le cadre d'un fonctionnement normal du réseau. Certains outils d'analyse réseau recherchent ce comportement et peuvent supposer que quelque chose ne va pas. Par conséquent, ces outils d'analyse peuvent générer des alertes ou arrêter des ports lorsque vous utilisez le proxy de mise en éveil.
>
> N'utilisez pas de proxy de mise en éveil si vos outils et services d'analyse réseau n'autorisent pas les bagottements MAC.

4. Lorsqu'un ordinateur gestionnaire voit une nouvelle demande de connexion TCP pour un ordinateur en veille et que la demande cible un port que l'ordinateur en veille écoutait avant sa mise en veille, l'ordinateur gestionnaire envoie un paquet de mise en éveil à l'ordinateur en veille, puis arrête la redirection du trafic pour cet ordinateur.
5. L'ordinateur en veille reçoit le paquet de mise en éveil et sort de veille. L'ordinateur expéditeur procède automatiquement à une nouvelle tentative de connexion et cette fois, l'ordinateur est mis en éveil et peut répondre.

Le proxy de mise en éveil est soumis aux conditions préalables et limitations suivantes :

> **IMPORTANT**
> Si vous disposez d'une équipe distincte responsable de l'infrastructure réseau et des services réseau, avertissez-la et intégrez-la lors de votre évaluation et votre période de test. Par exemple, sur un réseau qui utilise le contrôle d'accès réseau 802.1X, le proxy de mise en éveil ne fonctionne pas et peut perturber le service réseau. En outre, le proxy de mise en éveil peut amener certains outils d'analyse réseau à générer des alertes en cas de détection de trafic destiné à mettre en éveil d'autres ordinateurs.

- Tous les systèmes d'exploitation Windows répertoriés comme clients pris en charge dans Systèmes d'exploitation pris en charge pour les clients et appareils sont pris en charge pour l'éveil par appel réseau (Wake On LAN).
- Les systèmes d'exploitation invités qui s'exécutent sur une machine virtuelle ne sont pas pris en charge.
- Les clients doivent être activés pour le proxy de mise en éveil via des paramètres client. Bien que le fonctionnement du proxy de mise en éveil ne dépende pas de l'inventaire matériel, les clients ne signalent pas l'installation du service du proxy de mise en éveil sauf s'ils sont activés pour l'inventaire matériel et qu'ils ont soumis au moins un inventaire matériel.
- Les cartes réseau (et éventuellement le BIOS) doivent être activées et configurées pour les paquets de mise en éveil. Si la carte réseau n'est pas configurée pour les paquets de mise en éveil ou que ce paramètre est désactivé, Configuration Manager le configure et l'active automatiquement pour un ordinateur à réception du paramètre client permettant d'activer le proxy de mise en éveil.
- Si un ordinateur possède plusieurs cartes réseau, vous ne pouvez pas configurer la carte à utiliser pour le proxy de mise en éveil ; ce choix s'effectue sans déterminisme. Cependant, la carte choisie est enregistrée dans le fichier SleepAgent<*DOMAINE*>*@SYSTEM_0.log*.
- Le réseau doit autoriser les requêtes d'écho ICMP (au moins au sein du sous-réseau). Vous ne pouvez pas configurer l'intervalle de cinq secondes qui est utilisé pour envoyer les commandes ping ICMP.
- La communication est décryptée et non authentifiée, et le protocole IPsec n'est pas pris en charge.

- Les configurations réseau suivantes ne sont pas prises en charge :
  - 802.1X avec authentification de port
  - Réseaux sans fil
  - Commutateurs réseau permettant de lier des adresses MAC à des ports spécifiques
  - Réseaux IPv6 uniquement
  - Durées de bail DHCP inférieures à 24 heures

Si vous voulez sortir de veille des ordinateurs pour l'installation planifiée d'un logiciel, vous devez configurer chaque site principal de sorte que ce dernier utilise des paquets de mise en éveil.

Pour utiliser le proxy de mise en éveil, vous devez déployer les paramètres client correspondants de gestion de l'alimentation en plus de configurer le site principal.

Décidez d'utiliser ou non des paquets de diffusions dirigées vers le sous-réseau, ou des paquets monodiffusion, ainsi que le numéro de port UDP à utiliser. Par défaut, les paquets de mise en éveil traditionnels sont transmis via le port UDP 9, mais pour une plus grande sécurité, vous pouvez sélectionner un autre port pour le site si cet autre port est pris en charge par les routeurs et pare-feu qui interviennent.

**Choisir entre une diffusion monodiffusion et une diffusion dirigée vers le sous-réseau pour Wake on LAN**

Si vous avez choisi de réveiller des ordinateurs en envoyant des paquets de mise en éveil traditionnels, vous devez décider de transmettre les paquets monodiffusion ou les paquets de diffusion dirigée vers le sous-réseau. Si vous utilisez le proxy de mise en éveil, vous devez utiliser des paquets monodiffusion. Sinon, utilisez le tableau suivant pour déterminer la méthode de transmission à choisir.

| MÉTHODE DE TRANSMISSION | AVANTAGES | INCONVÉNIENTS |
|---|---|---|
| Monodiffusion | Il s'agit d'une solution plus sécurisée que les diffusions dirigées vers le sous-réseau car le paquet est envoyé directement à un seul ordinateur, et non à tous les ordinateurs d'un sous-réseau.<br><br>Ne nécessite pas de reconfiguration des routeurs (vous devrez peut-être configurer le cache ARP).<br><br>Elle consomme moins de bande passante réseau que les transmissions par diffusion dirigées vers le sous-réseau.<br><br>Prise en charge avec IPv4 et IPv6. | Les paquets de mise en éveil ne trouvent pas les ordinateurs de destination qui ont modifié leur adresse de sous-réseau depuis le dernier calendrier d'inventaire matériel.<br><br>La configuration des commutateurs sera peut-être nécessaire pour transmettre les paquets UDP.<br><br>Il est possible que certaines cartes réseau ne répondent pas aux paquets de mise en éveil dans tous les états de veille lorsque la monodiffusion est utilisée comme méthode de transmission. |

| MÉTHODE DE TRANSMISSION | AVANTAGES | INCONVÉNIENTS |
| --- | --- | --- |
| Diffusion dirigée vers le sous-réseau | Elle génère un taux de réussite supérieur à celui de la monodiffusion si vous possédez des ordinateurs qui modifient souvent leur adresse IP dans le même sous-réseau.<br><br>Aucune configuration de commutateur n'est requise.<br><br>Le taux de compatibilité avec les cartes d'ordinateurs pour tous les états de veille est élevé. En effet, les diffusions dirigées vers le sous-réseau correspondaient à la méthode de transmission d'origine pour l'envoi des paquets de mise en éveil. | Solution moins sûre que l'utilisation de la monodiffusion, car une personne malveillante pourrait envoyer des flux continus de demandes d'écho ICMP à partir d'une adresse source falsifiée à l'adresse de diffusion dirigée. En conséquence, tous les hôtes répondent à cette adresse source. Si les routeurs sont configurés pour autoriser les diffusions dirigées vers le sous-réseau, la configuration supplémentaire est recommandée pour des raisons de sécurité :<br><br>- Configurez les routeurs pour autoriser uniquement les diffusions dirigées vers IP depuis le serveur de site Configuration Manager, à l'aide d'un numéro de port UDP spécifique.<br>- Configurez Configuration Manager pour utiliser le numéro de port autre que celui par défaut spécifié.<br><br>Il peut être nécessaire de reconfigurer tous les routeurs intervenants pour permettre des diffusions dirigées vers le sous-réseau.<br><br>Elle consomme plus de bande passante réseau que les transmissions par monodiffusion.<br><br>Prise en charge avec IPv4 uniquement. IPv6 n'est pas pris en charge. |

**WARNING**

Il existe des risques de sécurité associés aux diffusions dirigées vers le sous-réseau : Une personne malveillante pourrait envoyer des flux continus de demandes d'écho ICMP (Internet Control Message Protocol) à partir d'une adresse source falsifiée vers l'adresse de diffusion dirigée, obligeant tous les hôtes à répondre à cette adresse source. Ce type d'attaque par déni de service est généralement appelé attaque de réflexion et est traité en rejetant les diffusions dirigées vers le sous-réseau.

# Considérations sur la gestion des clients System Center Configuration Manager dans une infrastructure VDI

22/06/2018 • 4 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

System Center Configuration Manager prend en charge l'installation du client Configuration Manager dans les scénarios VDI suivants :

- **Machines virtuelles personnelles** : les machines virtuelles personnelles sont généralement utilisées quand vous voulez vous assurer que les données et les paramètres utilisateur sont conservés sur les machines virtuelles entre les sessions.
- **Sessions de services Bureau à distance** : les services Bureau à distance permettent à un serveur d'héberger plusieurs sessions clientes simultanées. Les utilisateurs peuvent se connecter à une session, puis exécuter des applications sur ce serveur.
- **Machines virtuelles regroupées** : les machines virtuelles regroupées ne sont pas conservées entre les sessions. Lorsqu'une session est fermée, toutes les données et tous les paramètres sont supprimés. Les machines virtuelles regroupées sont utiles lorsqu'il est impossible d'utiliser les services Bureau à distance, car une application métier requise ne peut pas s'exécuter sur le serveur Windows hébergeant les sessions clientes.

  Le tableau suivant recense les éléments à prendre en considération pour la gestion du client Configuration Manager dans une infrastructure VDI.

| TYPE DE MACHINE VIRTUELLE | ÉLÉMENTS À PRENDRE EN CONSIDÉRATION |
|---|---|
| Machines virtuelles personnelles | Configuration Manager traite les machines virtuelles personnelles comme un ordinateur physique. Le client Configuration Manager peut être préinstallé sur l'image de machine virtuelle ou déployé après avoir approvisionné la machine virtuelle. |
| Services Bureau à distance | Le client Configuration Manager n'est pas installé pour les sessions Bureau à distance individuelles. Ce client est plutôt installé une seule fois sur le serveur des services Bureau à distance. Toutes les fonctionnalités de Configuration Manager peuvent être utilisées sur le serveur des services Bureau à distance. |
| Machines virtuelles regroupées | Quand une machine virtuelle regroupée est mise hors service, les modifications que vous apportez à l'aide de Configuration Manager sont perdues.<br><br>Les données renvoyées par les fonctionnalités de Configuration Manager, telles que l'inventaire logiciel, l'inventaire matériel et le contrôle de logiciel peuvent ne pas répondre à vos besoins, car la machine virtuelle risque de ne fonctionner que sur une courte période. Envisagez d'exclure les ordinateurs virtuels regroupés des tâches d'inventaire. |

Sachant que la virtualisation prend en charge l'exécution de plusieurs clients Configuration Manager sur un même ordinateur physique, de nombreuses opérations du client possèdent un délai randomisé prédéfini pour les actions planifiées telles que l'inventaire matériel et logiciel, les analyses anti-programmes malveillants, les installations logicielles et les analyses de mises à jour logicielles. Ce délai permet de distribuer le traitement processeur et le transfert de données pour un ordinateur doté de plusieurs machines virtuelles qui exécutent le client Configuration Manager.

**NOTE**

À l'exception des clients Windows Embedded en mode maintenance, les clients Configuration Manager qui ne s'exécutent pas dans des environnements virtualisés utilisent aussi ce délai randomisé. Quand le nombre de clients déployés est important, ce comportement permet d'éviter des pics d'utilisation de la bande passante réseau et de réduire les besoins de traitement processeur sur les systèmes de site Configuration Manager, tels que le point de gestion et le serveur de site. L'intervalle du délai varie en fonction de la fonctionnalité de Configuration Manager.

Le délai de randomisation est désactivé par défaut pour les mises à jour logicielles requises et les déploiements d'applications requis à l'aide du paramètre client suivant : **Agent ordinateur**: **Désactiver la randomisation des échéances**.

# Comment configurer les ports de communication des clients dans System Center Configuration Manager

22/06/2018 • 9 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez modifier les numéros des ports de demande utilisés par les clients System Center Configuration Manager pour communiquer avec les systèmes de site qui utilisent des protocoles HTTP et HTTPS pour les communications. Même si les protocoles HTTP ou HTTPS sont sans doute déjà configurés pour les pare-feu, une notification de client utilisant le protocole HTTP ou HTTPS consomme plus de ressources processeur et de mémoire sur l'ordinateur du point de gestion qu'en utilisant un numéro de port personnalisé. Vous pouvez également spécifier le numéro de port de site à utiliser si vous réveillez les clients à l'aide de paquets de réveil traditionnels.

Lorsque vous spécifiez les ports de demande HTTP et HTTPS, vous pouvez spécifier un numéro de port par défaut et un autre numéro de port. Les clients essaient automatiquement le port alternatif après un échec de communication avec le port par défaut. Vous pouvez spécifier des paramètres pour la communication de données HTTP et HTTPS.

Les valeurs par défaut des ports de demande client sont **80** pour le trafic HTTP et **443** pour le trafic HTTPS. Modifiez-les uniquement si vous ne souhaitez pas utiliser ces valeurs par défaut. Un exemple typique d'utilisation des ports personnalisés est lorsque vous utilisez un site Web personnalisé dans IIS, plutôt que le site Web par défaut. Si vous modifiez les numéros de port par défaut pour le site Web par défaut dans IIS et que d'autres applications utilisent également le site Web par défaut, ils sont susceptibles d'échouer.

**IMPORTANT**

Avant de modifier des numéros de port dans Configuration Manager, pensez aux conséquences. Exemples :

- Si vous changez les numéros de port des services de demande client en tant que configuration du site et que des clients existants ne sont pas reconfigurés de façon à utiliser les nouveaux numéros de port, ceux-ci ne seront pas gérés.
  - Avant de configurer un numéro de port non défini par défaut, assurez-vous que les pare-feu et tous les périphériques réseau intermédiaires peuvent prendre en charge cette configuration, puis effectuez la reconfiguration en conséquence. Si vous allez gérer des clients sur Internet et modifier le numéro de port HTTPS par défaut 443, les routeurs et les pare-feu d'Internet pourraient bloquer cette communication.

Pour vous assurer que les clients ne sont pas non gérés après la modification des numéros de port de demande, les clients doivent être configurés pour utiliser les nouveaux numéros de port de demande. Lorsque vous modifiez les ports de requêtes sur un site principal, tout site secondaire associé héritera automatiquement de la même configuration de port. Utilisez la procédure décrite dans cette rubrique pour configurer les ports de requêtes sur le site principal.

**NOTE**

Pour plus d'informations sur la façon de configurer les ports de demande pour les clients sur les ordinateurs qui exécutent Linux et UNIX, consultez Configurer des ports de demande pour le client pour Linux et UNIX.

Lorsque le site Configuration Manager est publié dans les services de domaine Active Directory, les nouveaux clients et les clients existants qui peuvent accéder à ces informations seront automatiquement configurés avec leurs paramètres de port du site. Vous ne devez effectuer aucune opération ultérieure. Les clients qui ne peuvent pas accéder à ces informations publiées dans les services de domaine Active Directory incluent les clients des groupes de travail, les clients d'une autre forêt Active Directory, les clients configurés pour la gestion Internet uniquement et les clients qui se trouvent actuellement sur Internet. Si vous modifiez les numéros de ports par défaut après l'installation de ces clients, réinstallez-les et installez tout nouveau client à l'aide de l'une des méthodes suivantes :

- Réinstallez les clients en utilisant l'Assistant Installation poussée du client. L'Installation poussée du client configure automatiquement les clients avec la configuration de port de site en cours. Pour plus d'informations sur l'utilisation de l'Assistant Installation Push du client, consultez Guide pratique pour installer des clients Configuration Manager à l'aide d'une installation Push.
- Réinstallez les clients à l'aide du programme CCMSetup.exe ainsi que les propriétés d'installation du client.msi de CCMHTTPPORT et CCMHTTPSPORT. Pour plus d'informations sur ces propriétés, consultez À propos des propriétés d'installation du client dans System Center Configuration Manager.
- Réinstallez les clients à l'aide d'une méthode qui permet de rechercher les propriétés d'installation du client Configuration Manager dans les Services de domaine Active Directory. Pour plus d'informations, consultez À propos de la publication des propriétés d'installation du client sur les services de domaine Active Directory dans System Center Configuration Manager.

  Pour reconfigurer les numéros de port de clients existants, vous pouvez également utiliser le script PORTSWITCH.VBS fourni avec le support d'installation dans le dossier SMSSETUP\Tools\PortConfiguration .

> **IMPORTANT**
> Pour les clients existants et les nouveaux clients sur Internet, vous devez configurer les numéros de port par défaut en utilisant les propriétés CCMSetup.exe client.msi de CCMHTTPPORT et CCMHTTPSPORT.

Après avoir modifié les ports de demande sur le site, les nouveaux clients installés à l'aide de la méthode d'installation poussée du client à l'échelle du site seront automatiquement configurés avec les numéros de port du site en cours.

**Pour configurer les numéros de port de communication client pour un site**

1. Dans la console Configuration Manager, cliquez sur **Administration**.
2. Dans l'espace de travail **Administration** développez **Configuration du site**, cliquez sur **Sites**et sélectionnez le site principal à configurer.
3. Dans l'onglet **Accueil** , cliquez sur **Propriétés**, puis sur l'onglet **Ports** .
4. Sélectionnez l'un des éléments et cliquez sur l'icône Propriétés pour ouvrir la boîte de dialogue **Détails du port** .
5. Dans la boîte de dialogue **Détails du port** , spécifiez le numéro de port et la description de l'élément et cliquez sur **OK**.
6. Sélectionnez **Utiliser un site Web personnalisé** si vous souhaitez utiliser le nom du site Web personnalisé de **SMSWeb** pour les systèmes de site qui exécutent IIS.
7. Cliquez sur **OK** pour fermer la boîte de dialogue des propriétés du site.

   Répétez cette procédure pour tous les sites principaux de la hiérarchie.

# Comment configurer des ordinateurs clients pour trouver des points de gestion à l'aide de la publication DNS dans System Center Configuration Manager

22/06/2018 • 5 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les clients de System Center Configuration Manager doivent localiser un point de gestion pour terminer l'affectation de site et, dans le cadre d'un processus continu, pour continuer d'être gérés. Les services de domaine Active Directory offrent la méthode la plus sûre pour que les clients sur l'intranet trouvent leurs points de gestion. Toutefois, si les clients ne peuvent pas utiliser cette méthode d'emplacement des services (par exemple, parce que vous n'avez pas étendu le schéma Active Directory ou que les clients font partie d'un groupe de travail), utilisez la publication DNS comme alternative principale à cette méthode.

> **NOTE**
> Lorsque vous installez le client pour Linux et UNIX, vous devez indiquer le point de gestion à utiliser comme point de contact initial. Pour plus d'informations sur l'installation du client pour Linux et UNIX, consultez Guide pratique pour déployer des clients sur des serveurs UNIX et Linux dans System Center Configuration Manager.

Avant d'utiliser la publication DNS pour les points de gestion, assurez-vous que les serveurs DNS sur l'intranet disposent d'enregistrements de ressource d'emplacement de service (SRV RR) et d'enregistrements de ressource d'hôte correspondant (A ou AAA) pour les points de gestion du site. Les enregistrements de ressource d'emplacement de service peuvent être créés automatiquement par Configuration Manager ou manuellement par l'administrateur DNS qui crée les enregistrements dans DNS.

Pour plus d'informations sur la publication DNS comme méthode d'emplacement de service pour les clients Configuration Manager, consultez Comprendre comment les clients recherchent des services et ressources de site pour System Center Configuration Manager.

Par défaut, les clients recherchent DNS pour les points de gestion dans leur domaine DNS. Toutefois, si aucun point de gestion n'est publié dans le domaine des clients, vous devez configurer manuellement les clients avec un suffixe DNS de point de gestion. Vous pouvez configurer ce suffixe DNS sur les clients, soit pendant l'installation du client, soit après :

- Pour configurer les clients pour un suffixe de point de gestion pendant l'installation du client, configurez les propriétés CCMSetup Client.msi.
- Pour configurer les clients pour un suffixe de point de gestion après l'installation du client, dans le panneau de configuration, configurez les **Propriétés du Configuration Manager**.

#### Pour configurer les clients pour un suffixe de point de gestion pendant l'installation du client

- Installez le client avec la propriété CCMSetup Client.msi suivante :
  - **DNSSUFFIX=** *<domaine du point de gestion>*

    Si le site dispose de plusieurs points de gestion et que ceux-ci se trouvent dans plusieurs domaines, ne spécifiez qu'un seul domaine. Lorsque les clients se connectent à un point de gestion dans ce domaine, ils téléchargent une liste de points de gestion disponibles, qui inclura les points de gestion

des autres domaines.

Pour plus d'informations sur les propriétés de ligne de commande CCMSetup, consultez À propos des propriétés d'installation du client dans System Center Configuration Manager.

**Pour configurer les clients pour un suffixe de point de gestion après l'installation du client**

1. Dans le Panneau de configuration de l'ordinateur client, accédez à **Configuration Manager**, puis double-cliquez sur **Propriétés**.
2. Dans l'onglet **Site** , spécifiez le suffixe DNS d'un point de gestion, puis cliquez sur **OK**.

   Si le site dispose de plusieurs points de gestion et que ceux-ci se trouvent dans plusieurs domaines, ne spécifiez qu'un seul domaine. Lorsque les clients se connectent à un point de gestion dans ce domaine, ils téléchargent une liste de points de gestion disponibles, qui inclura les points de gestion des autres domaines.

# Guide pratique pour configurer les paramètres client dans System Center Configuration Manager

22/06/2018 • 5 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous gérez tous les paramètres client dans System Center Configuration Manager depuis **Administration** > **Paramètres client**. Modifiez les paramètres par défaut lorsque vous souhaitez configurer des paramètres pour tous les utilisateurs et appareils de la hiérarchie ne disposant pas de paramètres personnalisés. Si vous souhaitez appliquer différents paramètres à certains utilisateurs ou appareils, créez des paramètres personnalisés et déployez-les vers les regroupements.

Pour plus d'informations sur chaque paramètre client, consultez À propos des paramètres client dans System Center Configuration Manager.

> **NOTE**
> Vous pouvez également utiliser des éléments de configuration pour gérer des clients afin d'évaluer, de suivre et de corriger la conformité de la configuration des appareils. Pour plus d'informations, consultez Garantir la conformité des appareils avec System Center Configuration Manager.

## Configurer les paramètres client par défaut

1. Dans la console Configuration Manager, choisissez **Administration** > **Paramètres client** > **Paramètres client par défaut**.
2. Sous l'onglet **Accueil**, choisissez **Propriétés**.
3. Consultez et configurez les paramètres client pour chaque groupe de paramètres dans le volet de navigation.

   Les ordinateurs clients sont configurés avec ces paramètres lorsqu'ils téléchargent la stratégie client. Pour lancer une récupération de stratégie pour un seul client, consultez Lancer une récupération de stratégie pour un client Configuration Manager dans Comment gérer les clients dans System Center Configuration Manager.

## Créer et déployer des paramètres client personnalisés

Lorsque vous déployez ces paramètres personnalisés, ceux-ci remplacent les paramètres client par défaut. Avant de débuter cette procédure, assurez-vous que vous disposez d'un regroupement qui contient les utilisateurs ou les appareils qui nécessitent ces paramètres client personnalisés.

1. Dans la console Configuration Manager, cliquez sur **Administration** > **Paramètres client**.
2. Sous l'onglet **Accueil**, dans le groupe **Créer**, choisissez **Créer des paramètres client personnalisés**, puis choisissez une des deux options suivantes :
   - **Créer des paramètres d'appareil client personnalisés**
   - **Créer des paramètres utilisateur client personnalisés**
3. Spécifiez un nom et une description de l'option.

4. Cochez une ou plusieurs des cases qui affichent un groupe de paramètres.
5. Choisissez chaque groupe de paramètres dans le volet de navigation et configurez les paramètres disponibles, puis cliquez sur **OK**.
6. Sélectionnez le paramètre client personnalisé que vous avez créé. Sous l'onglet **Accueil**, dans le groupe **Paramètres client**, choisissez **Déployer**.
7. Dans la boîte de dialogue **Sélectionner un regroupement**, sélectionnez le regroupement approprié, puis choisissez **OK**. Vous pouvez vérifier le regroupement sélectionné en cliquant sur l'onglet **Déploiements** du volet d'informations.
8. Consultez l'ordre du paramètre client personnalisé que vous avez créé. Lorsque vous disposez de plusieurs paramètres client personnalisés, ceux-ci sont appliqués en fonction de leur numéro. En cas de conflit, le paramètre dont le numéro d'ordre est le plus petit remplace les autres paramètres. Pour changer le numéro d'ordre, sous l'onglet **Accueil**, dans le groupe **Paramètres client**, cliquez sur **Déplacer l'élément vers le haut** ou **Déplacer l'élément vers le bas**.

   Les ordinateurs clients sont configurés avec ces paramètres lorsqu'ils téléchargent la stratégie client. Pour lancer une récupération de stratégie pour un seul client, consultez Lancer une récupération de stratégie pour un client Configuration Manager dans Comment gérer les clients dans System Center Configuration Manager.

## Afficher les paramètres client

Quand vous déployez plusieurs paramètres client sur le même appareil, utilisateur ou groupe d'utilisateurs, la définition des priorités et la combinaison des paramètres sont complexes. Pour afficher les paramètres client :

1. Dans la console Configuration Manager, choisissez **Ressources et Conformité** > **Appareils** > **Utilisateurs** ou **Regroupements d'utilisateurs**.
2. Sélectionnez un appareil, un utilisateur ou un groupe d'utilisateurs, puis dans le groupe **Paramètres client** , sélectionnez **Paramètres résultants du client**.
3. Sélectionnez un paramètre client dans le volet gauche pour afficher les paramètres. Dans cette vue, les paramètres sont en lecture seule.

> **NOTE**
> Pour afficher les paramètres client, vous devez disposer d'un accès en lecture aux paramètres client.

# À propos des paramètres client dans System Center Configuration Manager

22/06/2018 • 82 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez gérer tous les paramètres client dans la console Configuration Manager à partir du nœud **Paramètres client** de l'espace de travail **Administration**. Configuration Manager est fourni avec un ensemble de paramètres par défaut. Quand vous modifiez les paramètres client par défaut, ces paramètres sont appliqués à tous les clients de la hiérarchie. Vous pouvez également configurer des paramètres client personnalisés, qui remplacent les paramètres client par défaut lorsque vous les affectez à des regroupements. Pour plus d'informations, consultez Guide pratique pour configurer les paramètres client.

Les sections suivantes décrivent en détail les paramètres et les options.

## service de transfert intelligent en arrière-plan (BITS)

**Limiter la bande passante réseau maximale pour les transferts BITS en arrière-plan**

Quand cette option est **Oui**, les clients utilisent la limitation de bande passante BITS. Pour configurer les autres paramètres de ce groupe, vous devez activer ce paramètre.

**Heure de début de la fenêtre de limitation**

Spécifiez l'heure locale de début de la fenêtre de limitation BITS.

**Heure de fin de la fenêtre de limitation**

Spécifiez l'heure locale de fin de la fenêtre de limitation BITS. Si l'heure de fin est égale à l'**heure de début de la fenêtre de limitation**, la limitation BITS est toujours activée.

**Taux de transfert maximal dans la fenêtre de limitation (Kbit/s)**

Spécifie le taux de transfert maximal que les clients peuvent utiliser pendant la fenêtre.

**Autoriser les téléchargements BITS en dehors de la fenêtre de limitation**

Permet aux clients d'utiliser des paramètres BITS distincts en dehors de la fenêtre spécifiée.

**Taux de transfert maximal en dehors de la fenêtre de limitation (Kbit/s)**

Spécifiez le taux de transfert maximal que les clients peuvent utiliser en dehors de la fenêtre de limitation BITS.

## Paramètres du cache du client

**Configurer BranchCache**

Configurez l'ordinateur client pour Windows BranchCache. Pour autoriser la mise en cache BranchCache sur le client, définissez **Activer BranchCache** sur **Oui**.

- **Activer BranchCache**
  Active BranchCache sur les ordinateurs clients.
- **Taille maximale du cache BranchCache (pourcentage du disque)**
  Pourcentage du disque que vous autorisez BranchCache à utiliser.

**Configurer la taille du cache des clients**

Le cache du client Configuration Manager sur les ordinateurs Windows stocke les fichiers temporaires utilisés

pour installer des applications et des programmes. Si cette option est définie sur **Non**, la taille par défaut est de 5 120 Mo.

Si choisissez **Oui**, spécifiez :

- **Taille maximale du cache (Mo)**
- **Taille maximale du cache (pourcentage du disque)**
  La taille du cache du client augmente jusqu'à la taille maximale en mégaoctets (Mo) ou au pourcentage du disque, selon la valeur la moins élevée des deux.

**Permettre au client Configuration Manager exécutant le système d'exploitation complet de partager du contenu**

Active le cache d'homologue pour les clients Configuration Manager. Choisissez **Oui**, puis spécifiez le port par lequel le client communique avec l'ordinateur homologue.

- **Port pour la diffusion réseau initiale** (par défaut : 8004)
- **Port pour le téléchargement de contenu à partir d'un pair** (par défaut : 8003)
  Configuration Manager configure automatiquement les règles de Pare-feu Windows pour autoriser ce trafic. Si vous utilisez un autre pare-feu, vous devez configurer manuellement des règles pour autoriser ce trafic.

## Stratégie du client

**Intervalle d'interrogation de stratégie client (minutes)**

Spécifie la fréquence à laquelle les clients Configuration Manager suivants téléchargent la stratégie client :

- Ordinateurs Windows (par exemple, ordinateurs de bureau, serveurs, ordinateurs portables)
- Appareils mobiles inscrits par Configuration Manager
- Ordinateurs Mac
- Ordinateurs qui exécutent Linux ou UNIX

**Activer la stratégie utilisateur sur les clients**

Quand vous affectez la valeur **Oui** à cette option et que vous utilisez la découverte d'utilisateurs, les clients reçoivent les applications et programmes destinés à l'utilisateur connecté.

Le catalogue d'applications reçoit la liste des logiciels disponibles pour les utilisateurs à partir du serveur de site. Ainsi, ce paramètre ne doit pas obligatoirement être **Oui** pour que les utilisateurs voient et demandent des applications au catalogue d'applications. Si ce paramètre a la valeur **Non**, les comportements suivants ne fonctionnent pas quand les utilisateurs utilisent le catalogue d'applications :

- Les utilisateurs ne peuvent pas installer les applications qu'ils voient dans le catalogue des applications.
- Les utilisateurs ne voient pas les notifications concernant leurs demandes d'approbation d'application. Au lieu de cela, ils doivent actualiser le catalogue d'applications et vérifier l'état d'approbation.
- Les utilisateurs ne reçoivent pas de révisions et de mises à jour pour les applications qui sont publiées dans le catalogue d'applications. Les utilisateurs voient les modifications apportées aux informations de l'application dans le catalogue d'applications.
- Si vous supprimez le déploiement d'une application après que le client a installé l'application en question à partir du catalogue d'applications, les clients continuent à vérifier que l'application est installée pendant une durée qui peut atteindre deux jours.

En outre, si ce paramètre est défini sur **Non**, les utilisateurs ne reçoivent pas les applications requises que vous déployez sur les utilisateurs. Ils ne reçoivent pas non plus d'autres tâches de gestion dans les stratégies utilisateur.

Ce paramètre s'applique aux utilisateurs si leur ordinateur se trouve sur l'intranet ou Internet. Il doit avoir la valeur **Oui** si vous souhaitez également activer les stratégies utilisateur sur Internet.

**Autoriser les demandes de stratégie utilisateur depuis des clients Internet**

Définissez ce paramètre sur **Oui** pour que les utilisateurs reçoivent la stratégie utilisateur sur les ordinateurs basés sur Internet. Les conditions suivantes s'appliquent également :

- Le client et le site sont configurés pour la gestion des clients Internet ou pour une passerelle de gestion cloud.
- Le paramètre **Activer la stratégie utilisateur sur les clients** est défini sur **Oui**.
- Le point de gestion basé sur Internet authentifie correctement l'utilisateur à l'aide de l'authentification Windows (Kerberos ou NTLM). Pour plus d'informations, consultez Éléments à prendre en considération pour les communications clients à partir d'Internet.
- À compter de la version 1710, la passerelle de gestion cloud peut authentifier l'utilisateur avec Azure Active Directory. Pour plus d'informations, consultez Déployer des applications disponibles pour l'utilisateur sur des appareils joints à Azure AD.

Si vous affectez la valeur **Non** à cette option, ou si l'une des conditions ci-dessus n'est pas remplie, un ordinateur sur Internet reçoit uniquement les stratégies ordinateur. Dans ce cas, les utilisateurs peuvent toujours voir, demander et installer des applications à partir d'un catalogue d'applications basé sur Internet. Si ce paramètre est **Non**, mais que **Activer la stratégie utilisateur sur les clients** est **Oui**, les utilisateurs ne reçoivent les stratégies utilisateur qu'une fois l'ordinateur connecté à intranet.

> **NOTE**
> Pour la gestion des clients Internet, les demandes d'approbation d'applications des utilisateurs ne nécessitent pas de stratégies utilisateur ou d'authentification utilisateur. La passerelle de gestion cloud ne prend pas en charge les demandes d'approbation d'applications.

## Services cloud

**Autoriser l'accès au point de distribution cloud**

Définissez ce paramètre sur **Oui** pour que les clients obtiennent le contenu à partir d'un point de distribution cloud. Ce paramètre ne nécessite pas que l'appareil soit basé sur Internet.

**Inscrire automatiquement les nouveaux appareils joints au domaine Windows 10 auprès d'Azure Active Directory**

Quand vous configurez Azure Active Directory pour prendre en charge la jointure hybride, Configuration Manager configure les appareils Windows 10 pour cette fonctionnalité. Pour plus d'informations, consultez Guide pratique pour configurer des appareils hybrides joints à Azure Active Directory.

**Autoriser les clients à utiliser une passerelle de gestion cloud**

Par défaut, tous les clients Internet itinérants utilisent n'importe quelle passerelle de gestion cloud disponible. Vous pouvez affecter la valeur **Non** à ce paramètre par exemple quand vous souhaitez limiter l'étendue du service, comme lors d'un projet pilote, ou pour réduire les coûts.

## Paramètres de conformité

**Activer l'évaluation de compatibilité sur les clients**

Définissez ce paramètre sur **Oui** pour configurer les autres paramètres de ce groupe.

**Planifier l'évaluation de compatibilité**

Sélectionnez **Planifier** pour créer le calendrier par défaut pour les déploiements de la base de référence de configuration. Cette valeur est configurable pour chaque ligne de base dans la boîte de dialogue **Déployer la**

**ligne de base de la configuration**.

**Activer les données et profils utilisateurs**

Choisissez **Oui** si vous souhaitez déployer des éléments de configuration de données et de profils utilisateur.

## Agent ordinateur

**Notifications à l'utilisateur pour les déploiements obligatoires**

Pour plus d'informations sur les trois paramètres suivants, consultez Notifications à l'utilisateur pour les déploiements obligatoires :

- **Échéance du déploiement supérieure à 24 heures, effectuer un rappel à l'utilisateur toutes les (heures)**
- **Échéance du déploiement inférieure à 24 heures, effectuer un rappel à l'utilisateur toutes les (heures)**
- **Échéance du déploiement inférieure à 1 heure, effectuer un rappel à l'utilisateur toutes les (minutes)**

**Point de site Web du catalogue d'applications par défaut**

Configuration Manager utilise ce paramètre pour connecter les utilisateurs au catalogue d'applications du Centre logiciel. Sélectionnez **Définir un site Web** pour spécifier un serveur qui héberge le point du site web du catalogue d'applications. Entrez son nom NetBIOS ou son nom de domaine complet, spécifiez la détection automatique, ou spécifiez une URL pour les déploiements personnalisés. Dans la plupart des cas, la détection automatique est le meilleur choix car elle offre les avantages suivants :

- Si le site a un point du site web du catalogue d'applications, les clients reçoivent automatiquement un point du site web du catalogue d'applications à partir de leur site.
- Le client préfère les points de site web du catalogue d'applications activés HTTPS sur l'intranet aux serveurs HTTP-uniquement. Cette fonctionnalité offre une protection contre les serveurs non autorisés.
- Le point de gestion donne aux clients Internet un point de site web du catalogue d'applications basé sur Internet. Le point de gestion donne aux clients intranet un point du site web du catalogue d'applications basé sur intranet.

La détection automatique ne garantit pas que les clients recevront le point du site web du catalogue d'applications le plus proche. Vous pouvez décider de ne pas utiliser **Détecter automatiquement** pour les raisons suivantes :

- Vous voulez configurer manuellement le serveur le plus proche pour les clients ou vous assurer qu'ils ne connectent pas à un serveur via une connexion réseau lente.
- Vous souhaitez contrôler quels clients se connectent à quel serveur. Cette configuration convient pour des raisons professionnelles ou de performances ou à des fins de tests.
- Vous ne souhaitez pas patienter jusqu'à 25 heures ou attendre une modification du réseau pour que les clients utilisent un autre point du site web du catalogue d'applications.

Si vous spécifiez le point de site web du catalogue d'applications au lieu d'utiliser la détection automatique, spécifiez le nom NetBIOS plutôt que le nom de domaine complet de l'intranet. Cette configuration réduit la probabilité que le navigateur web invite l'utilisateur à fournir des informations d'identification quand il accède à un catalogue d'applications basé sur intranet. Pour utiliser le nom NetBIOS, les conditions suivantes doivent s'appliquer :

- Le nom NetBIOS est spécifié dans les propriétés du point du site Web du catalogue d'applications.
- Vous utilisez WINS ou tous les clients sont dans le même domaine que le point du site web du catalogue

des applications.

- Vous configurez le point du site web du catalogue d'applications pour les connexions clientes HTTP, ou vous configurez le serveur pour HTTPS et le certificat du serveur web a le nom NetBIOS.

En règle générale, les utilisateurs sont invités à entrer leurs informations d'identification quand l'URL contient un nom de domaine complet, mais pas quand l'URL est un nom NetBIOS. Les utilisateurs doivent s'attendre à être toujours invités à saisir leurs informations d'identification lorsqu'ils se connectent à partir d'Internet, car cette connexion doit utiliser le nom de domaine complet Internet. Pour un client basé sur Internet, quand le navigateur web invite l'utilisateur à fournir des informations d'identification, vérifiez que le point du site web du catalogue d'applications peut se connecter à un contrôleur de domaine pour le compte de l'utilisateur. Cette configuration permet à l'utilisateur de s'authentifier à l'aide de Kerberos.

> **NOTE**
>
> Voici comment fonctionne la détection automatique :
>
> le client effectue une demande d'emplacement de service à un point de gestion. S'il existe un point de site Web du catalogue d'applications dans le même site que le client, ce serveur est donné au client en tant que le serveur du catalogue d'applications à utiliser. Si plusieurs point du site web du catalogue des applications sont disponibles dans le site, un serveur HTTPS est prioritaire sur un serveur qui n'est pas activé pour le protocole HTTPS. Après ce filtrage, tous les clients reçoivent l'un des serveurs à utiliser comme le catalogue d'applications. Configuration Manager n'équilibre pas la charge entre plusieurs serveurs. Quand le site du client ne contient pas de point du site web du catalogue des applications, le point de gestion retourne de manière non déterministique un point du site web du catalogue des applications à partir de la hiérarchie.
>
> Pour les clients basés sur intranet, si vous configurez le point du site web du catalogue d'applications avec un nom NetBIOS pour l'URL du catalogue d'applications, le point de gestion donne aux clients ce nom NetBIOS, plutôt que le nom de domaine complet de l'intranet. Pour les clients basés sur Internet, le point de gestion donne uniquement le nom de domaine complet Internet au client.
>
> Le client effectue cette demande d'emplacement de service toutes les 25 heures ou chaque fois qu'il détecte un changement de réseau. Par exemple, si le client passe de l'intranet à Internet, il s'agit d'une modification de réseau. Si le client peut alors localiser un point de gestion basé sur Internet, celui-ci fournit aux clients des serveurs de points du site web du catalogue d'applications basés sur Internet.

**Ajoute un site Web du catalogue d'applications par défaut à la zone des sites de confiance d'Internet Explorer**

Si cette option a la valeur **Oui**, le client ajoute automatiquement l'URL actuelle du site web du catalogue d'applications par défaut à la zone des sites de confiance dans Internet Explorer.

Ce paramètre garantit que le paramètre Internet Explorer en mode protégé n'est pas activé. Si le mode protégé est activé, le client Configuration Manager peut ne pas être en mesure d'installer des applications à partir du catalogue d'applications. Par défaut, la zone des sites de confiance prend également en charge l'ouverture de session utilisateur pour le catalogue d'applications, ce qui requiert l'authentification Windows.

Si vous conservez la valeur **Non** pour cette option, les clients Configuration Manager risquent de ne pas pouvoir installer des applications à partir du catalogue d'applications. Une autre méthode consiste à configurer ces paramètres Internet Explorer dans une autre zone pour l'URL du catalogue d'applications utilisée par les clients.

> **NOTE**
>
> Chaque fois que Configuration Manager ajoute l'URL du catalogue d'applications par défaut à la zone de sites de confiance, Configuration Manager supprime toute URL du catalogue d'applications ajoutée précédemment.
>
> Si l'URL est déjà spécifiée dans l'une des zones de sécurité, Configuration Manager ne peut pas l'ajouter. Dans ce cas, vous devez supprimer l'URL de l'autre zone ou configurer manuellement les paramètres Internet Explorer requis.

**Autoriser les applications Silverlight à s'exécuter en mode de confiance élevé**

Ce paramètre doit être **Oui** pour que les utilisateurs utilisent le catalogue d'applications.

Si vous modifiez ce paramètre, il prend effet au prochain chargement du navigateur par les utilisateurs ou lorsqu'ils actualisent la fenêtre du navigateur actuellement ouverte.

Pour plus d'informations sur ce paramètre, consultez Certificats pour Microsoft Silverlight 5 et mode de confiance élevée obligatoires pour le catalogue des applications.

**Nom d'organisation affiché dans le Centre logiciel**

Tapez le nom que les utilisateurs voient dans le Centre logiciel. Ces informations personnalisées aident les utilisateurs à identifier cette application comme une source approuvée.

**Utiliser le nouveau Centre logiciel**

Si vous sélectionnez **Oui**, tous les ordinateurs clients utilisent le Centre logiciel. Le Centre logiciel répertorie les applications accessibles à l'utilisateur qui étaient auparavant uniquement disponibles dans le catalogue d'applications. Le catalogue d'applications nécessite Silverlight, qui n'est pas un prérequis pour le Centre logiciel. À compter de Configuration Manager 1802, la valeur par défaut est **Oui**.

Les rôles de système de site Point du site web du catalogue des applications et Point de service web du catalogue des applications sont toujours exigés pour que les applications accessibles à l'utilisateur apparaissent dans le Centre logiciel.

Pour plus d'informations, consultez Planifier et configurer la gestion des applications.

**Activer la communication avec le service d'attestation d'intégrité**

Définissez ce paramètre sur **Oui** pour que les appareils Windows 10 utilisent l'attestation d'intégrité. Quand vous activez ce paramètre, le paramètre suivant est également disponible pour la configuration.

**Utiliser le service d'attestation d'intégrité local**

Définissez ce paramètre sur **Oui** pour que les appareils utilisent un service local. Définissez ce paramètre sur **non** pour que les appareils utilisent le service cloud de Microsoft.

**Autorisations d'installation**

> **IMPORTANT**
> Ce paramètre s'applique au catalogue des applications et au Centre logiciel. Ce paramètre n'a aucun effet quand les utilisateurs utilisent le portail d'entreprise.

Configurez la manière dont les utilisateurs peuvent lancer l'installation des logiciels, des mises à jour logicielles et des séquences de tâches :

- **Tous les utilisateurs** : les utilisateurs disposant de toutes les autorisations, sauf Invité.
- **Administrateurs uniquement** : les utilisateurs doivent être membres du groupe Administrateurs local.
- **Administrateurs et utilisateurs principaux uniquement**: les utilisateurs doivent être membres du groupe Administrateurs local ou des utilisateurs principaux de l'ordinateur.
- **Aucun utilisateur**: aucun utilisateur connecté à un ordinateur client ne peut lancer l'installation des logiciels, mises à jour logicielles et séquences de tâches. Les déploiements requis pour l'ordinateur sont toujours installés à la date d'échéance. Les utilisateurs ne peuvent pas lancer l'installation du logiciel à partir du catalogue d'applications ou du Centre logiciel.

**Interrompre l'entrée du code confidentiel BitLocker au redémarrage**

Si les ordinateurs exigent une entrée de code PIN BitLocker, cette option contourne la nécessité d'entrer un code

PIN quand l'ordinateur redémarre après l'installation d'un logiciel.

- **Toujours**: Configuration Manager suspend temporairement BitLocker après l'installation d'un logiciel nécessitant un redémarrage de l'ordinateur et qu'un redémarrage a été effectué. Ce paramètre s'applique uniquement à un redémarrage de l'ordinateur lancé par Configuration Manager. Il ne suspend pas l'obligation d'entrer le code PIN BitLocker quand l'utilisateur redémarre l'ordinateur. L'obligation d'entrer un code PIN BitLocker reprend après le démarrage de Windows.
- **Jamais**: Configuration Manager ne suspend pas BitLocker après avoir installé un logiciel qui nécessite un redémarrage. Dans ce cas, l'installation du logiciel ne peut être finalisée que lorsque l'utilisateur entre le code confidentiel pour terminer le processus de démarrage standard et charger Windows.

**D'autres logiciels gèrent le déploiement d'applications et de mises à jour logicielles**

Activez cette option uniquement si l'une des conditions suivantes s'applique :

- Vous utilisez une solution de fabricant qui nécessite l'activation de ce paramètre.
- Vous utilisez le kit de développement logiciel (SDK) Configuration Manager pour gérer les notifications d'agent client et l'installation d'applications et de mises à jour logicielles.

> **WARNING**
> Si vous choisissez cette option quand aucune de ces conditions ne s'applique, le client n'installe pas les mises à jour logicielles et les applications exigées. Ce paramètre n'empêche pas les utilisateurs d'installer des applications à partir du catalogue d'applications, et n'empêche pas l'installation des packages, programmes et séquences de tâches.

**Stratégie d'exécution de PowerShell**

Configurez la façon dont les clients Configuration Manager peuvent exécuter des scripts Windows PowerShell. Vous pouvez utiliser ces scripts pour la détection dans les éléments de configuration de paramètres de conformité. Vous pouvez également envoyer les scripts dans un déploiement sous la forme d'un script standard.

- **Ignorer** : le client Configuration Manager ignore la configuration Windows PowerShell sur l'ordinateur client afin que les scripts non signés puissent s'exécuter.
- **Restreint** : le client Configuration Manager utilise la configuration PowerShell actuelle sur l'ordinateur client. Cette configuration détermine si les scripts non signés peuvent s'exécuter.
- **Toutes signées** : le client Configuration Manager exécute les scripts uniquement s'ils sont signés par un éditeur approuvé. Cette restriction s'applique indépendamment de la configuration PowerShell actuelle sur l'ordinateur client.

Cette option nécessite au minimum la version 2.0 de Windows PowerShell. La valeur par défaut est **Toutes signées**.

> **TIP**
> Si les scripts non signés ne parviennent pas à s'exécuter en raison de ce paramètre client, Configuration Manager signale cette erreur ainsi :
>
> - L'espace de travail **Surveillance** dans la console affiche l'ID d'erreur d'état de déploiement **0x87D00327**. Il affiche également la description **Le script n'est pas signé**.
> - Les rapports affichent le type d'erreur **Erreur de découverte**. Les rapports affichent ensuite le code d'erreur **0x87D00327** et la description **Le script n'est pas signé**, ou le code d'erreur **0x87D00320** et la description **L'environnement d'exécution de scripts n'a pas encore été installé**. Exemple de rapport : **Détails des erreurs des éléments de configuration dans la base de référence de configuration d'un composant**.
> - Le fichier **DcmWmiProvider.log** affiche le message **Le script n'est pas signé (Erreur : 87D00327; Source : CCM)**.

**Afficher les notifications de nouveaux déploiements**

Choisissez **Oui** pour afficher une notification pour les déploiements disponibles moins d'une semaine. Ce message s'affiche à chaque démarrage de l'agent du client.

**Désactiver la randomisation des échéances**

Quand la date limite est atteinte, ce paramètre détermine si le client utilise un délai d'activation pouvant aller jusqu'à deux heures pour installer les mises à jour logicielles requises. Par défaut, le délai d'activation est désactivé.

Pour les scénarios d'infrastructure VDI (Virtual Desktop Infrastructure), ce délai aide à distribuer le traitement par le processeur et le transfert de données pour un ordinateur hôte doté de plusieurs machines virtuelles. Même si vous n'utilisez pas d'infrastructure VDI, si de nombreux clients installent les mêmes mises à jour en même temps, cela peut augmenter l'utilisation du processeur sur le serveur de site. Ce comportement peut également ralentir les points de distribution et réduire considérablement la bande passante réseau disponible.

Si les clients doivent installer des mises à jour logicielles requises à l'échéance du déploiement sans délai, configurez ce paramètre sur **Oui**.

**Période de grâce pour la mise en œuvre après l'échéance du déploiement (en heures)**

Si vous souhaitez accorder aux utilisateurs plus de temps pour installer les déploiements de mises à jour logicielles ou d'applications obligatoires au-delà de l'échéance, définissez ce paramètre sur **Oui**. Cette période de grâce est destinée au scénario dans lequel un ordinateur est hors tension pendant une durée prolongée et l'utilisateur doit installer de nombreux déploiements d'applications ou de mises à jour. Par exemple, ce paramètre est utile si un utilisateur rentre de congés et qu'il doit patienter longtemps pendant que le client installe les déploiements d'applications en retard.

Définissez une période de grâce comprise entre une et 120 heures. Utilisez ce paramètre conjointement avec la propriété de déploiement **Différer la mise en œuvre de ce déploiement selon les préférences de l'utilisateur**. Pour plus d'informations, consultez Déployer des applications.

## Redémarrage de l'ordinateur

Les paramètres suivants doivent être inférieurs à la durée de la fenêtre de maintenance la plus courte appliquée à l'ordinateur.

- **Afficher une notification temporaire à l'utilisateur indiquant l'intervalle avant la fermeture de la session de l'utilisateur ou le redémarrage de l'ordinateur (minutes)**
- **Afficher une boîte de dialogue que l'utilisateur ne peut pas fermer, indiquant l'intervalle de compte à rebours avant la fermeture de la session de l'utilisateur ou le redémarrage de l'ordinateur (minutes)**

Pour plus d'informations sur les fenêtres de maintenance, consultez Comment utiliser les fenêtres de maintenance dans System Center Configuration Manager.

## Optimisation de la distribution

Les groupes de limites Configuration Manager permettent de définir et de réguler la distribution de contenu sur le réseau de l'entreprise et dans les agences. L'Optimisation de la distribution de Windows est une technologie cloud pair à pair de partage de contenu entre appareils Windows 10. À compter de la version 1802, configurez-la de façon à ce qu'elle utilise vos groupes de limites pour partager du contenu entre homologues.

> **NOTE**
> L'Optimisation de la distribution n'est disponible que sur les clients Windows 10

**Utiliser les groupes de limites Configuration Manager pour l'ID de groupe d'Optimisation de la distribution**

Choisissez **Oui** pour appliquer l'identificateur de groupe de limites en tant qu'identificateur de groupe d'Optimisation de la distribution sur le client. Lorsque le client communique avec le service de cloud d'Optimisation de la distribution, il utilise cet identificateur pour localiser les pairs possédant le contenu souhaité.

# Endpoint Protection

> **TIP**
> En plus des informations suivantes, vous pouvez trouver des détails sur l'utilisation des paramètres du client Endpoint Protection dans Exemple de scénario : utilisation de System Center Endpoint Protection pour protéger des ordinateurs contre les programmes malveillants dans System Center Configuration Manager.

**Gérer le client Endpoint Protection sur les ordinateurs clients**

Choisissez **Oui** si vous souhaitez gérer les clients Endpoint Protection et Windows Defender existants sur des ordinateurs de la hiérarchie.

Choisissez cette option si vous avez déjà installé le client Endpoint Protection et que vous souhaitez le gérer avec Configuration Manager. Cette installation distincte inclut un processus sous forme de script utilisant un programme et un package ou une application Configuration Manager. À compter de Configuration Manager 1802, l'agent Endpoint Protection n'a pas besoin d'être installé sur les appareils Windows 10. L'option **Gérer le client Endpoint Protection sur les ordinateurs clients** doit néanmoins être activée sur ces ordinateurs.

**Installer le client Endpoint Protection sur les ordinateurs clients**

Choisissez **Oui** pour installer et activer le client Endpoint Protection sur les ordinateurs clients qui ne l'exécutent pas encore. À compter de Configuration Manager 1802, l'agent Endpoint Protection n'a pas besoin d'être installé sur les clients Windows 10.

> **NOTE**
> Si le client Endpoint Protection est déjà installé, le fait de choisir la valeur **Non** ne désinstalle pas le client Endpoint Protection. Pour désinstaller le client Endpoint Protection, affectez au paramètre client **Gérer le client Endpoint Protection sur les ordinateurs clients** la valeur **Non**. Ensuite, déployez un package et un programme pour désinstaller le client Endpoint Protection.

**Supprimer automatiquement le logiciel anti-programmes malveillants installé avant Endpoint Protection**

Définissez ce paramètre sur **Oui** pour que le client Endpoint Protection tente de désinstaller les autres applications anti-programmes malveillants. La présence de plusieurs clients anti-programmes malveillants sur le même appareil peut générer un conflit et affecter les performances du système.

**Autoriser l'installation du client Endpoint Protection et redémarrer en dehors des fenêtres de maintenance. Celles-ci doivent être d'une durée minimale de 30 minutes pour l'installation du client**

Définissez ce paramètre sur **Oui** pour remplacer les comportements d'installation par défaut avec des fenêtres de maintenance. Ce paramètre satisfait aux besoins de l'entreprise en ce qui concerne la priorité de la maintenance du système pour des raisons de sécurité.

**Pour les appareils Windows Embedded avec des filtres d'écriture, valider l'installation du client Endpoint Protection (nécessite un redémarrage)**

Choisissez **Oui** pour désactiver le filtre d'écriture sur l'appareil Windows Embedded et le redémarrer. Cette action valide l'installation sur l'appareil.

Si vous choisissez **Non**, le client est installé sur une superposition temporaire qui est effacée lors du redémarrage de l'appareil. Dans ce scénario, le client Endpoint Protection n'est entièrement installé que

lorsqu'une autre installation valide les modifications apportées à l'appareil. Il s'agit de la configuration par défaut.

**Supprimer tout redémarrage d'ordinateur requis après l'installation du client Endpoint Protection**

Choisissez **Oui** pour ignorer le redémarrage de l'ordinateur après l'installation du client Endpoint Protection.

> **IMPORTANT**
> Si le client Endpoint Protection nécessite un redémarrage de l'ordinateur et que ce paramètre est **Non**, l'ordinateur redémarre quelle que soit la fenêtre de maintenance configurée.

**Durée pendant laquelle les utilisateurs sont autorisés à différer un redémarrage nécessaire pour terminer l'installation de Endpoint Protection (heures)**

Si un redémarrage est nécessaire après l'installation du client Endpoint Protection, ce paramètre spécifie le nombre d'heures duquel les utilisateurs sont autorisés à différer le redémarrage. Ce paramètre exige que le paramètre **Supprimer tout redémarrage d'ordinateur requis après l'installation du client Endpoint Protection** soit **Non**.

**Désactiver les autres sources (telles que Microsoft Windows Update, Microsoft Windows Server Update Services ou les partages UNC) pour la mise à jour initiale des définitions sur les ordinateurs clients**

Choisissez **Oui** si vous souhaitez que Configuration Manager installe uniquement la mise à jour de définition initiale sur les ordinateurs clients. Ce paramètre peut s'avérer pratique pour éviter les connexions réseau inutiles et réduire la bande passante réseau pendant l'installation initiale de la mise à jour de définition.

## Inscription

**Intervalle d'interrogation pour clients hérités de périphériques mobiles**

Sélectionnez **Déf. un interv.** pour spécifier la durée, en minutes ou heures, d'interrogation de la stratégie par les appareils mobiles hérités. Ces appareils incluent des plateformes telles que Windows CE, Mac OS X et Unix ou Linux.

**Fréquence d'interrogation des appareils récents (minutes)**

Entrez l'intervalle d'interrogation (en minutes) de la stratégie par les appareils récents. Ce paramètre concerne les appareils Windows 10 gérés par le biais de la gestion des appareils mobiles locale.

**Autoriser les utilisateurs à inscrire des appareils mobiles et des ordinateurs Mac**

Pour activer l'inscription des appareils hérités par l'utilisateur, définissez ce paramètre sur **Oui**, puis configurez le paramètre suivant :

- **Profil d'inscription**
  Sélectionnez **Définir un profil** pour créer ou sélectionner un profil d'inscription. Pour plus d'informations, consultez Configurer les paramètres client pour l'inscription.

**Autoriser les utilisateurs à inscrire des appareils récents**

Pour activer l'inscription d'appareils modernes, définissez ce paramètre sur **Oui**, puis configurez le paramètre suivant :

- **Profil d'inscription des appareils récents**
  Sélectionnez **Définir un profil** pour créer ou sélectionner un profil d'inscription. Pour plus d'informations, consultez Créer un profil d'inscription qui permet aux utilisateurs d'inscrire des appareils récents.

## Inventaire matériel

**Activer l'inventaire matériel sur les clients**

Par défaut, ce paramètre est défini sur **Oui**. Pour plus d'informations, consultez Présentation de l'inventaire

matériel.

**Calendrier de l'inventaire matériel**

Sélectionnez **Planifier** pour régler la fréquence à laquelle les clients exécutent le cycle d'inventaire matériel. Par défaut, ce cycle se produit tous les sept jours.

**Délai aléatoire maximal (minutes)**

Spécifiez le nombre maximal de minutes pour la définition d'un délai aléatoire du cycle d'inventaire matériel par le client Configuration Manager, par rapport à la planification définie. Cette fonctionnalité de randomisation parmi tous les clients aide à équilibrer la charge d'inventaire sur le serveur de site. Vous pouvez spécifier une valeur comprise entre 0 et 480 minutes. Par défaut, cette valeur est définie sur 240 minutes (4 heures).

**Taille maximale du fichier MIF personnalisé (Ko)**

Spécifiez la taille maximale, en kilo-octets (Ko), autorisée pour chaque fichier Management Information Format (MIF) personnalisé recueilli par le client lors d'un cycle d'inventaire matériel. L'agent d'inventaire matériel Configuration Manager ne traite pas les fichiers MIF personnalisés qui dépassent cette taille. Vous pouvez spécifier une taille comprise entre 1 et 5 120 Ko. Par défaut, cette valeur est définie à 250 Ko. Ce paramètre n'affecte pas la taille du fichier de données d'inventaire matériel ordinaire.

> **NOTE**
> Ce paramètre est disponible uniquement dans les paramètres client par défaut.

**Classes d'inventaire matériel**

Sélectionnez **Déf. classes** pour étendre les informations matérielles que vous recueillez auprès des clients sans modifier manuellement le fichier sms_def.mof. Pour plus d'informations, consultez Guide pratique pour configurer l'inventaire matériel.

**Collecter des fichiers MIF**

Utilisez ce paramètre pour spécifier si vous souhaitez collecter des fichiers MIF à partir de clients Configuration Manager pendant l'inventaire matériel.

Pour qu'un fichier MIF soit collecté par un inventaire matériel, il doit se trouver à l'emplacement approprié sur l'ordinateur client. Par défaut, les fichiers se trouvent aux chemins suivants :

- Les **fichiers IDMIF** doivent être dans le dossier Windows\System32\CCM\Inventory\Idmif.
- Les **fichiers NOIDMIF** doivent être dans le dossier Windows\System32\CCM\Inventory\Noidmif.

> **NOTE**
> Ce paramètre est disponible uniquement dans les paramètres client par défaut.

## Connexions Internet facturées à l'usage

Gérez la façon dont les ordinateurs Windows 8 et versions ultérieures utilisent des connexions Internet facturées à l'usage pour communiquer avec Configuration Manager. Les fournisseurs Internet facturent parfois en fonction de la quantité de données que vous envoyez et recevez lorsque vous utilisez une connexion Internet facturée à l'usage.

> **NOTE**
>
> Le paramètre client configuré n'est pas appliqué dans les scénarios suivants :
>
> - Si l'ordinateur se trouve sur une connexion de données itinérante, le client Configuration Manager n'exécute aucune tâche nécessitant le transfert de données vers des sites Configuration Manager.
> - Si les propriétés de la connexion réseau Windows sont configurées pour une connexion non facturée à l'usage, le client Configuration Manager se comporte comme si la connexion n'était pas facturée à l'usage, et transfère donc les données vers le site.

**Communication des clients sur des connexions Internet facturées à l'usage**

Choisissez l'une des options suivantes pour ce paramètre :

- **Autoriser**: toutes les communications client sont autorisées via la connexion Internet facturée à l'usage, sauf si l'appareil client utilise une connexion de données itinérante.
- **Limite**: seules les communications client suivantes sont autorisées via la connexion Internet facturée à l'usage :
  - Récupération de stratégie client
  - Messages d'état du client à envoyer au site
  - Demandes d'installation de logiciels à l'aide du catalogue des applications
  - Déploiements requis (lorsque la date limite d'installation est atteinte)

  > **IMPORTANT**
  >
  > Le client autorise toujours les installations de logiciels à partir du Centre logiciel ou du catalogue des applications, quels que soient les paramètres de la connexion Internet facturée à l'usage.

  Si le client atteint la limite de transfert de données pour la connexion Internet facturée à l'usage, le client n'essaie plus de communiquer avec les sites Configuration Manager.
- **Bloc** : le client Configuration Manager n'essaie pas de communiquer avec les sites Configuration Manager quand il est sur une connexion Internet limitée. Il s'agit de l'option par défaut.

## Gestion de l'alimentation

**Autoriser la gestion de l'alimentation des périphériques**

Définissez ce paramètre sur **Oui** pour activer la gestion de l'alimentation sur les clients. Pour plus d'informations, consultez Présentation de la gestion de l'alimentation.

**Autoriser les utilisateurs à exclure leur appareil de la gestion de l'alimentation**

Choisissez **Oui** pour permettre aux utilisateurs du Centre logiciel d'exclure leur ordinateur des paramètres de gestion de l'alimentation configurés.

**Autoriser le proxy de mise en éveil**

Spécifiez **Oui** pour compléter le paramètre d'éveil par appel réseau du site lorsqu'il est configuré pour les paquets monodiffusion.

Pour plus d'informations sur le proxy de mise en éveil, consultez Planifier la sortie de veille des clients dans System Center Configuration Manager.

> **WARNING**
> N'activez pas le proxy de mise en éveil dans un réseau de production sans d'abord comprendre comment il fonctionne et l'évaluer dans un environnement de test.

Ensuite, configurez les paramètres supplémentaires suivants en fonction des besoins :

- **Numéro de port du proxy de mise en éveil (UDP)**
  Numéro du port utilisé par les clients pour envoyer des paquets de réveil aux ordinateurs en état de veille. Conservez le port par défaut 25536 ou remplacez-le par le numéro de votre choix.
- **Numéro de port Wake On LAN (UDP)**
  Conservez la valeur par défaut (9), sauf si vous avez modifié le numéro du port Wake On LAN (UDP) sous l'onglet **Ports**des **Propriétés** du site.

  > **IMPORTANT**
  > Ce numéro doit correspondre au numéro figurant dans les **Propriétés**du site. Si vous modifiez ce numéro dans un seul emplacement, sachez qu'il n'est pas actualisé automatiquement dans l'autre emplacement.

- **Exception du pare-feu Windows Defender pour le proxy de mise en éveil**
  Le client Configuration Manager configure automatiquement le numéro de port du proxy de mise en éveil sur les appareils qui exécutent le Pare-feu Windows Defender. Sélectionnez **Configurer** pour spécifier les profils de pare-feu souhaités.

  Si les clients exécutent un autre pare-feu, vous devez le configurer manuellement pour autoriser le **Numéro de port du proxy de mise en éveil (UDP)**.
- **Préfixes IPv6 si nécessaires pour DirectAccess ou d'autres périphériques réseau intervenants. Spécifiez plusieurs entrées en utilisant une virgule**
  Entrez les préfixes IPv6 nécessaires pour que le proxy de mise en éveil fonctionne sur votre réseau.

## outils de contrôle à distance.

**Activer le contrôle à distance sur des clients et Profils d'exception de pare-feu**

Sélectionnez **Configurer** pour activer la fonctionnalité de contrôle à distance de Configuration Manager. Vous pouvez éventuellement configurer les paramètres du pare-feu pour autoriser le contrôle à distance sur des ordinateurs clients.

Le contrôle à distance est désactivé par défaut.

> **IMPORTANT**
> Si les paramètres de pare-feu ne sont pas configurés, le contrôle à distance risque de ne pas fonctionner correctement.

**Les utilisateurs peuvent modifier les paramètres de stratégie ou de notification dans le Centre logiciel**

Indiquez si les utilisateurs peuvent modifier les options de contrôle à distance à partir du Centre logiciel.

**Autoriser le contrôle à distance d'un ordinateur autonome**

Indiquez si un administrateur peut utiliser le contrôle à distance pour accéder à un ordinateur client qui est déconnecté ou verrouillé. Seul un ordinateur connecté et déverrouillé peut être contrôlé à distance quand ce paramètre est désactivé.

**Inviter l'utilisateur à autoriser le contrôle à distance**

Choisissez si l'ordinateur client affiche un message demandant l'autorisation de l'utilisateur avant d'autoriser une session de contrôle à distance.

**Demander à l'utilisateur l'autorisation de transférer le contenu du Presse-papiers partagé**

Donnez à vos utilisateurs la possibilité d'accepter ou de refuser des transferts de fichiers avant de transférer le contenu du Presse-papiers partagé dans une session de contrôle à distance. Les utilisateurs n'ont besoin d'accorder l'autorisation qu'une seule fois par session tandis que l'observateur ne peut pas s'accorder l'autorisation d'effectuer le transfert de fichiers.

**Accorder l'autorisation de contrôle à distance au groupe Administrateurs local**

Indiquez si les administrateurs locaux sur le serveur qui lance la connexion de contrôle à distance peuvent établir des sessions de contrôle à distance vers des ordinateurs client.

**Niveau d'accès autorisé**

Spécifiez le niveau d'accès de contrôle à distance à accorder. Choisissez parmi les paramètres suivants :

- **Aucun accès**
- **Afficher uniquement**
- **Contrôle intégral**

**Observateurs autorisés des options de contrôle à distance et d'assistance à distance**

Sélectionnez **Définir des observateurs** pour spécifier les noms des utilisateurs Windows qui peuvent établir des sessions de contrôle à distance vers des ordinateurs clients.

**Afficher l'icône de notification de session sur la barre des tâches**

Configurez ce paramètre sur **Oui** pour afficher une icône dans la barre des tâches de Windows du client quand une session de contrôle à distance est en cours.

**Afficher la barre de connexion de session**

Définissez ce paramètre sur **Oui** pour afficher une barre de connexion de session de haute visibilité sur les clients quand une session de contrôle à distance est en cours.

**Émettre un signal sonore sur le client**

Définissez cette option afin d'utiliser le son pour indiquer qu'une session de contrôle à distance est active sur un ordinateur client. Sélectionnez l'une des options suivantes :

- **Aucun signal sonore**
- **Début et fin de session** (par défaut)
- **Fréquemment au cours d'une session**

**Gérer les paramètres de l'Assistance à distance non sollicités**

Configurez ce paramètre sur **Oui** pour autoriser Configuration Manager à gérer les sessions d'assistance à distance non sollicitées.

Dans une session d'assistance à distance non sollicitée, l'utilisateur de l'ordinateur client n'a pas demandé d'assistance pour lancer la session.

**Gérer les paramètres de l'Assistance à distance sollicités**

Définissez ce paramètre sur **Oui** pour autoriser Configuration Manager à gérer les sessions d'assistance à distance sollicitées.

Dans une session d'assistance à distance sollicitée, l'utilisateur de l'ordinateur client envoie une demande d'assistance à distance à l'administrateur.

**Niveau d'accès de l'Assistance à distance**

Choisissez le niveau d'accès à attribuer aux sessions d'assistance à distance lancées à partir de la console

Configuration Manager. Sélectionnez l'une des options suivantes :

- **Aucun** (par défaut)
- **Affichage à distance**
- **Contrôle intégral**

> **NOTE**
> L'utilisateur de l'ordinateur client doit toujours autoriser l'ouverture d'une session d'assistance à distance.

**Gérer les paramètres du Bureau à distance**

Définissez ce paramètre sur **Oui** pour autoriser Configuration Manager à gérer les sessions Bureau à distance des ordinateurs.

**Autoriser la connexion des observateurs autorisés à l'aide d'une connexion Bureau à distance**

Définissez ce paramètre sur **Oui** pour ajouter les utilisateurs spécifiés dans la liste des observateurs autorisés au groupe d'utilisateurs locaux Bureau à distance sur les clients.

**Exiger l'authentification au niveau du réseau sur les ordinateurs exécutant le système d'exploitation Windows Vista et versions ultérieures**

Définissez ce paramètre sur **Oui** pour utiliser l'authentification au niveau du réseau afin d'établir des connexions Bureau à distance aux ordinateurs clients. L'authentification au niveau du réseau nécessite moins de ressources d'ordinateur distant, car l'authentification des utilisateurs se termine avant l'établissement de la connexion Bureau à distance. L'authentification au niveau du réseau est une configuration plus sécurisée. Elle contribue à protéger l'ordinateur des utilisateurs ou logiciels malveillants, et réduit le risque d'attaque par déni de service.

## Centre logiciel

**Sélectionnez ces nouveaux paramètres pour spécifier des informations sur l'entreprise**

Définissez ce paramètre sur **Oui**, puis spécifiez les paramètres suivants pour personnaliser le Centre logiciel et l'adapter à votre organisation :

- **Nom de la société**
  Entrez le nom d'organisation visible par les utilisateurs dans le Centre logiciel.
- **Modèle de couleurs pour le Centre logiciel**
  Choisissez **Sélectionner une couleur** pour définir la couleur principale utilisée par le Centre logiciel.
- **Sélectionner un logo pour le Centre logiciel**
  Choisissez **Parcourir** pour sélectionner une image à afficher dans le Centre logiciel. Le logo doit être de type JPEG, PNG ou BMP et au format 400 x 100 pixels, avec une taille maximale de 750 Ko. Le nom de fichier du logo ne doit pas contenir d'espace.

**Masquer les applications non approuvées dans le Centre logiciel**

À compter de Configuration Manager version 1802, quand cette option est activée, les applications disponibles pour l'utilisateur qui nécessitent une approbation sont masquées dans le Centre logiciel.

**Masquer les applications installées dans le Centre logiciel**

À compter de Configuration Manager version 1802, les applications qui sont déjà installées ne s'affichent plus sous l'onglet Applications quand cette option est activée. Cette option est définie par défaut quand vous installez ou mettez à niveau vers Configuration Manager 1802. Les applications installées sont toujours disponibles pour examen sous l'onglet de l'état d'installation.

**Visibilité de l'onglet Centre logiciel**

Affectez la valeur **Oui** aux paramètres supplémentaires de ce groupe pour afficher les onglets suivants dans le

Centre logiciel :

- **Applications**
- **Mises à jour**
- **Systèmes d'exploitation**
- **État de l'installation**
- **Conformité de l'appareil**
- **Options**

Par exemple, si votre organisation n'utilise pas de stratégies de conformité et que vous souhaitez masquer l'onglet Conformité de l'appareil dans le Centre logiciel, définissez l'onglet **Activer l'onglet Conformité de l'appareil** sur **Non**.

# Déploiement logiciel

**Planifier la réévaluation des déploiements**

Configurez une planification pour la réévaluation des règles de spécifications par Configuration Manager pour tous les déploiements. La valeur par défaut est tous les sept jours.

> **IMPORTANT**
> Nous vous recommandons de ne pas choisir une valeur inférieure à la valeur par défaut, Un calendrier de réévaluation plus agressif affecte négativement les performances de votre réseau et des ordinateurs clients.

Lancez cette action à partir du client en procédant comme suit : dans le panneau de configuration de **Configuration Manager**, dans l'onglet **Actions**, sélectionnez **Cycle d'évaluation du déploiement de l'application**.

# Inventaire logiciel

**Activer l'inventaire logiciel sur les clients**

Ce paramètre est défini sur **Oui** par défaut. Pour plus d'informations, consultez Présentation de l'inventaire logiciel.

**Planifier l'inventaire logiciel et le regroupement de fichiers**

Sélectionnez **Planifier** pour régler la fréquence à laquelle les clients exécutent les cycles de regroupement de fichiers et d'inventaire logiciel. Par défaut, ce cycle se produit tous les sept jours.

**Détails sur le rapport d'inventaire**

Spécifiez l'un des niveaux d'informations de fichiers suivants à inventorier :

- **Fichier uniquement**
- **Produit uniquement**
- **Détails complets** (par défaut)

**Inventorier ces types de fichiers**

Si vous souhaitez spécifier les types de fichiers à inventorier, sélectionnez **Définir des types**, puis configurez les options suivantes :

> **NOTE**
> Si plusieurs paramètres clients personnalisés sont appliqués à un ordinateur, l'inventaire retourné par chaque paramètre est fusionné.

- Sélectionnez **Nouveau** pour ajouter un nouveau type de fichier à l'inventaire. Ensuite, spécifiez les informations suivantes dans la boîte de dialogue **Propriétés du fichier inventorié** :
  - **Nom** : définissez le nom du fichier à inventorier. Utilisez un astérisque (*****) comme caractère générique pour représenter une chaîne de texte et un point d'interrogation (**?**) pour représenter n'importe quel caractère. Par exemple, si vous souhaitez inventorier tous les fichiers portant l'extension .doc, spécifiez le nom de fichier ***.doc**.
  - **Emplacement** : sélectionnez **Définir** pour ouvrir la boîte de dialogue **Propriétés du chemin d'accès**. Configurez l'inventaire logiciel pour rechercher le fichier défini sur tous les disques durs des clients, effectuer une recherche à un emplacement donné (tel que **C:\Dossier**) ou rechercher une variable (telle que *%windir%*). Vous pouvez également exécuter une recherche dans tous les sous-dossiers du chemin indiqué.
  - **Exclure les fichiers chiffrés et compressés** : quand vous choisissez cette option, tous les fichiers compressés ou chiffrés ne sont pas inventoriés.
  - **Exclure des fichiers dans le dossier Windows** : quand vous choisissez cette option, tous les fichiers dans le dossier Windows et ses sous-répertoires ne sont pas inventoriés.

  Sélectionnez **OK** pour fermer la boîte de dialogue **Propriétés du fichier inventorié**. Ajoutez tous les fichiers à inventorier, puis sélectionnez **OK** pour fermer la boîte de dialogue **Configurer le paramètre client**.

**Collecter des fichiers**

Si vous souhaitez collecter des fichiers stockés à partir d'ordinateurs clients, sélectionnez **Définir des fichiers**, puis configurez les paramètres suivants :

> **NOTE**
> Si plusieurs paramètres clients personnalisés sont appliqués à un ordinateur, l'inventaire retourné par chaque paramètre est fusionné.

- Dans la boîte de dialogue **Configurer le paramètre client**, sélectionnez **Nouveau** pour ajouter un fichier à collecter.
- Dans la boîte de dialogue **Propriétés du fichier collecté** , fournissez les informations suivantes :
  - **Nom** : définissez le nom du fichier à collecter. Utilisez un astérisque (*****) comme caractère générique pour représenter une chaîne de texte et un point d'interrogation (**?**) pour représenter n'importe quel caractère.
  - **Emplacement** : sélectionnez **Définir** pour ouvrir la boîte de dialogue **Propriétés du chemin d'accès**. Configurez l'inventaire logiciel pour rechercher le fichier à collecter sur tous les disques durs des clients, effectuer une recherche à un emplacement donné (tel que **C:\Dossier**) ou rechercher une variable (telle que *%windir%*). Vous pouvez également exécuter une recherche dans tous les sous-dossiers du chemin indiqué.
  - **Exclure les fichiers chiffrés et compressés** : quand vous choisissez cette option, tous les fichiers compressés ou chiffrés ne sont pas collectés.

- **Arrêter le regroupement de fichiers lorsque la taille totale dépasse (Ko)** : spécifiez la taille de fichier, en Ko, au-delà de laquelle le client arrête la collecte des fichiers spécifiés.

> **NOTE**
>
> Le serveur de site collecte les cinq dernières versions modifiées des fichiers collectés et les enregistre dans le *<répertoire d'installation ConfigMgr>* \Inboxes\Sinv.box\Filecol. Si un fichier n'a pas changé depuis le dernier cycle d'inventaire logiciel, le fichier n'est pas recollecté.
>
> L'inventaire logiciel ne collecte pas les fichiers de plus de 20 Mo.
>
> La valeur **Taille maximale pour tous les fichiers regroupés (Ko)** dans la boîte de dialogue **Configurer le paramètre client** indique la taille maximale de tous les fichiers collectés. Quand cette taille est atteinte, la collecte de fichiers s'arrête. Tous les fichiers déjà regroupés sont conservés et envoyés au serveur de site.

> **IMPORTANT**
>
> Si vous configurez l'inventaire logiciel pour collecter un grand nombre de fichiers volumineux, vous risquez d'affecter négativement les performances du serveur de site et du réseau.

Pour plus d'informations sur l'affichage des fichiers collectés, consultez Guide pratique pour utiliser l'Explorateur de ressources pour afficher l'inventaire logiciel.

Sélectionnez **OK** pour fermer la boîte de dialogue **Propriétés du fichier collecté**. Ajoutez tous les fichiers à collecter, puis sélectionnez **OK** pour fermer la boîte de dialogue **Configurer le paramètre client**.

#### Définir des noms

L'agent d'inventaire logiciel récupère le nom du fabricant et du produit à partir des informations d'en-tête de fichier. Ces noms ne sont pas systématiquement normalisés dans les informations d'en-tête de fichier. Quand vous affichez l'inventaire logiciel dans l'Explorateur de ressources, des versions différentes du même nom de fabricant ou de produit peuvent apparaître. Pour normaliser ces noms complets, sélectionnez **Définir des noms**, puis configurez les paramètres suivants :

- **Type de nom** : l'inventaire logiciel collecte des informations sur les produits et les fabricants. Choisissez si vous souhaitez configurer des noms complets pour un **Fabricant** ou un **Produit**.
- **Nom complet** : spécifiez le nom complet que vous souhaitez utiliser à la place des noms dans la liste **Noms inventoriés**. Sélectionnez **Nouveau** pour spécifier un nouveau nom complet.
- **Noms inventoriés**: sélectionnez **Nouveau** pour ajouter un nom inventorié. Ce nom est remplacé dans l'inventaire logiciel par le nom choisi dans la liste **Nom complet**. Vous pouvez ajouter plusieurs noms à remplacer.

## Contrôle de logiciel

#### Activer le contrôle de logiciel sur les clients

Par défaut, ce paramètre est défini sur **Oui**. Pour plus d'informations, consultez Contrôle de logiciel.

#### Planifier le regroupement de données

Sélectionnez **Planifier** pour régler la fréquence à laquelle les clients exécutent le cycle de contrôle de logiciel. Par défaut, ce cycle se produit tous les sept jours.

## Mises à jour logicielles

**Activer les mises à jour logicielles sur les clients**

Utilisez ce paramètre pour activer les mises à jour logicielles sur les clients Configuration Manager. Quand vous désactivez ce paramètre, Configuration Manager supprime les stratégies de déploiement existantes du client. Lorsque vous réactivez ce paramètre, le client télécharge la stratégie de déploiement actuelle.

> **IMPORTANT**
> Quand vous désactivez ce paramètre, les stratégies de conformité qui reposent sur les mises à jour logicielles ne fonctionnent plus.

**Calendrier d'analyse des mises à jour logicielles**

Sélectionnez **Planifier** pour spécifier la fréquence à laquelle le client lance une analyse de la conformité. Cette analyse détermine l'état des mises à jour logicielles sur le client (par exemple, requise ou installée). Pour plus d'informations sur l'évaluation de la conformité, consultez Évaluation de la conformité des mises à jour logicielles.

Par défaut, cette analyse utilise un calendrier simple pour une exécution tous les sept jours. Vous pouvez créer une planification personnalisée. Vous pouvez spécifier une date et une heure exactes de début, utiliser le temps universel coordonné (UTC) ou l'heure locale, et configurer l'intervalle de récurrence pour un jour spécifique de la semaine.

> **NOTE**
> Si vous spécifiez un intervalle inférieur à une journée, Configuration Manager rétablit automatiquement la valeur par défaut (une journée).

> **WARNING**
> L'heure de début réelle sur les ordinateurs clients est l'heure de début plus une durée aléatoire de deux heures maximum. Cette fonctionnalité de randomisation empêche les ordinateurs clients de lancer l'analyse et de se connecter simultanément au point de mise à jour logicielle actif.

**Planifier la réévaluation du déploiement**

Sélectionnez **Planifier** pour configurer la fréquence à laquelle l'agent client des mises à jour logicielles réévalue les mises à jour logicielles pour en déterminer l'état de l'installation sur les ordinateurs clients Configuration Manager. Quand des mises à jour logicielles préalablement installées ne sont plus disponibles sur les clients, mais sont toujours requises, le client réinstalle les mises à jour logicielles.

Ajustez cette planification en fonction de la stratégie de l'entreprise relative à la conformité des mises à jour logicielles et du droit des utilisateurs à désinstaller des mises à jour logicielles. Chaque cycle de réévaluation du déploiement provoque une activité processeur sur l'ordinateur client et le réseau. Par défaut, ce paramètre utilise un calendrier simple pour lancer l'analyse de réévaluation du déploiement tous les sept jours.

> **NOTE**
> Si vous spécifiez un intervalle inférieur à une journée, Configuration Manager rétablit automatiquement la valeur par défaut (une journée).

**Dès que l'échéance d'un déploiement de mise à jour logicielle est atteinte, installer tous les autres déploiements de mise à jour logicielle avec une échéance pendant une période de temps spécifiée**

Définissez ce paramètre sur **Oui** pour installer toutes les mises à jour à partir des déploiements requis dont les échéances ont lieu pendant une période spécifiée. Quand un déploiement de mises à jour logicielles requis atteint

une échéance, le client lance l'installation des mises à jour logicielles du déploiement. Ce paramètre détermine s'il faut installer des mises à jour logicielles d'autres déploiements requis dont l'échéance tombe dans le délai spécifié.

Utilisez-le pour accélérer l'installation des mises à jour logicielles requises. Ce paramètre est également susceptible d'augmenter la sécurité du client, les notifications à l'utilisateur et réduire les redémarrages du client. Par défaut, ce paramètre est défini sur **Non**.

**Durée pendant laquelle tous les déploiements en attente avec une échéance dans cette période seront également installés**

Utilisez ce paramètre pour spécifier le laps de temps pour le paramètre précédent. Vous pouvez entrer une valeur comprise entre 1 et 23 heures et entre 1 et 365 jours. Par défaut, ce paramètre est configuré pour 7 jours.

**Activer l'installation de fichiers d'installation rapide sur les clients**

Définissez ce paramètre sur **Oui** pour permettre aux clients d'utiliser des fichiers d'installation rapide. Pour plus d'informations, consultez Gérer les fichiers d'installation rapide pour les mises à jour de Windows 10.

**Port utilisé pour télécharger du contenu pour les fichiers d'installation rapide**

Ce paramètre configure le port local permettant à l'écouteur HTTP de télécharger le contenu express. Par défaut, il s'agit du port 8005. Vous n'avez pas besoin d'ouvrir ce port dans le pare-feu du client.

**Activer la gestion de l'agent Office 365 Client**

Lorsque ce paramètre est défini sur **Oui**, il permet de configurer les paramètres d'installation d'Office 365. Il permet également de télécharger des fichiers à partir de réseaux de distribution de contenu (CDN) Office et déployer les fichiers en tant qu'application dans Configuration Manager. Pour plus d'informations, consultez Gérer Office 365 ProPlus.

**Activer les mises à jour de logiciels tiers**

Le fait d'affecter la valeur **Oui** à cette option définit la stratégie pour « Autoriser les mises à jour signées provenant d'un emplacement intranet du service de mise à jour Microsoft » et installe le certificat de signature dans la banque d'éditeurs approuvés sur le client. Ce paramètre client a été ajouté dans Configuration Manager version 1802.

## Messagerie d'état

**Cycle de diffusion des messages d'état (en minutes)**

Spécifie la fréquence à laquelle les clients signalent les messages d'état. La valeur par défaut est de 15 minutes.

## Affinité entre utilisateur et appareil

**Seuil d'utilisation de l'affinité entre utilisateur et appareil (minutes)**

Spécifiez le nombre de minutes avant que Configuration Manager ne crée un mappage d'affinité entre utilisateur et appareil. La valeur par défaut est de 2880 minutes (2 jours).

**Seuil d'utilisation de l'affinité entre utilisateur et appareil (jour)**

Spécifiez le nombre de jours durant lesquels le client mesure le seuil de l'affinité d'appareil basée sur l'utilisation. Par défaut, cette valeur est de 30 jours.

> **NOTE**
>
> Par exemple, si vous réglez **Seuil d'utilisation de l'affinité entre utilisateur et périphérique (minutes)** sur **60** minutes et **Seuil d'utilisation de l'affinité entre utilisateur et périphérique (jours)** sur **5** jours, l'utilisateur doit utiliser l'appareil pendant 60 minutes sur une période de 5 jours pour créer une affinité automatique avec l'appareil.

**Configurer automatiquement l'affinité entre utilisateur et appareil à partir des données d'utilisation**

Choisissez **Oui** pour créer une affinité automatique entre appareil et utilisateur en fonction des informations d'utilisation recueillies par Configuration Manager.

**Autoriser les utilisateurs à définir leurs appareils principaux**

Quand ce paramètre est défini sur **Oui**, les utilisateurs peuvent identifier leurs propres appareils principaux dans le Centre logiciel.

## Windows Analytics

Pour plus d'informations sur ces paramètres, consultez Configurer les clients pour envoyer des données à Windows Analytics.

# Guide pratique pour configurer Wake on LAN dans System Center Configuration Manager

22/06/2018 • 6 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Spécifiez les paramètres d'éveil par appel réseau (« Wake On LAN ») pour System Center Configuration Manager quand vous voulez sortir des ordinateurs d'un état de veille pour installer les logiciels requis, notamment des mises à jour logicielles, des applications, des séquences de tâches ou des programmes.

Vous pouvez compléter Wake On LAN en utilisant les paramètres client du proxy de mise en éveil. Cependant, pour pouvoir utiliser le proxy de mise en éveil, vous devez au préalable activer l'éveil par appel réseau sur le site et activer les options **Utiliser uniquement les paquets de mise en éveil** et **Monodiffusion** pour la méthode de transmission de l'éveil par appel réseau. Cette solution de mise en éveil prend également en charge les connexions ad hoc, notamment les connexions Bureau à distance.

Utilisez la première procédure pour configurer l'éveil par appel réseau sur un site principal. Ensuite, utilisez la deuxième procédure pour configurer les paramètres client du proxy de mise en éveil. Cette deuxième procédure configure les paramètres client par défaut, de façon à ce que les paramètres du proxy de mise en éveil soient appliqués à tous les ordinateurs de la hiérarchie. Si vous souhaitez appliquer ces paramètres à certains ordinateurs seulement, créez un paramètre d'appareil personnalisé et attribuez-le à un regroupement contenant les ordinateurs que vous souhaitez configurer pour le proxy de mise en éveil. Pour plus d'informations sur la création de paramètres client personnalisés, consultez Guide pratique pour configurer les paramètres client dans System Center Configuration Manager.

Un ordinateur qui reçoit les paramètres client du proxy de mise en éveil risque d'interrompre sa connexion réseau pendant 1 à 3 secondes. Cela est dû au fait que le client doit réinitialiser la carte d'interface réseau pour activer le pilote de proxy de mise en éveil.

> **WARNING**
> Pour éviter une interruption inattendue de vos services réseau, commencez par évaluer le proxy de mise en éveil sur une infrastructure réseau isolée et représentative. Utilisez ensuite les paramètres client personnalisés pour étendre votre test à une sélection d'ordinateurs situés sur plusieurs sous-réseaux. Pour plus d'informations sur le fonctionnement du proxy de mise en éveil, consultez Planifier la sortie de veille des clients dans System Center Configuration Manager.

## Pour configurer l'éveil par appel réseau pour un site

1. Dans la console Configuration Manager, accédez à **Administration > Configuration du site > Sites**.
2. Cliquez sur le site principal à configurer, puis sur **Propriétés**.
3. Cliquez sur l'onglet **Wake On LAN** et configurez les options dont vous avez besoin pour ce site. Pour activer la prise en charge du proxy de mise en éveil, veillez à sélectionner **Utiliser uniquement les paquets de mise en éveil** et **Monodiffusion**. Pour plus d'informations, consultez Planifier la sortie de veille des clients dans System Center Configuration Manager.
4. Cliquez sur **OK** et répétez cette procédure pour tous les sites principaux de la hiérarchie.

## Pour configurer les paramètres client du proxy de mise en éveil

1. Dans la console Configuration Manager, accédez à **Administration > Paramètres client**.

2. Cliquez sur **Paramètres client par défaut**, puis sur **Propriétés**.
3. Sélectionnez **Gestion de l'alimentation**, puis choisissez **Oui** pour **Autoriser le proxy de mise en éveil**.
4. Passez en revue les autres paramètres du proxy de mise en éveil et configurez-les si nécessaire. Pour plus d'informations sur ces paramètres, consultez Paramètres de gestion de l'alimentation.
5. Cliquez sur **OK** pour fermer la boîte de dialogue, puis cliquez de nouveau sur **OK** pour fermer la boîte de dialogue Paramètres client par défaut.

Vous pouvez utiliser les rapports de Wake On LAN suivants pour surveiller l'installation et la configuration du proxy de mise en éveil :

- Résumé de l'état de déploiement du proxy de mise en éveil
- Détails sur l'état du déploiement de proxy de mise en éveil

> **TIP**
> Pour vérifier le bon fonctionnement du proxy de mise en éveil, essayez de vous connecter à un ordinateur en veille. Essayez par exemple de vous connecter à un dossier partagé sur cet ordinateur ou de vous connecter à ce dernier via une connexion Bureau à distance. Si vous utilisez l'accès direct, vérifiez que les préfixes IPv6 fonctionnent en effectuant les mêmes tests sur un ordinateur en veille actuellement connecté à Internet.

# Comment déployer des clients sur des ordinateurs Windows dans System Center Configuration Manager

22/06/2018 • 54 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Avant d'installer des clients Configuration Manager, vérifiez que toutes les conditions préalables sont réunies et que vous avez réalisé toutes les configurations de déploiement requises.

## Guide pratique pour installer des clients à l'aide d'une installation poussée du client

Vous pouvez configurer une installation Push du client pour un site. L'installation du client s'exécute automatiquement sur les ordinateurs qui sont découverts dans les limites configurées du site, dans la mesure où ces limites sont configurées en tant que groupe de limites. Vous pouvez également lancer une installation poussée du client en exécutant l'Assistant Installation poussée du client pour un regroupement ou une ressource spécifique dans un regroupement.

L'Assistant Installation poussée du client permet également d'installer le client Configuration Manager selon les résultats d'une requête. Pour que l'installation réussisse, l'un des éléments retournés par la requête doit correspondre à l'attribut **ResourceID** de la classe **Ressource système**.

Si le serveur de site ne parvient pas à contacter l'ordinateur client ou à démarrer le processus d'installation, il tente à nouveau l'installation de façon automatique toutes les heures. Le serveur renouvelle les tentatives pendant sept jours, au maximum.

Pour vous aider à suivre le processus d'installation du client, installez un point d'état de secours avant d'installer les clients. Du moment qu'un point d'état de secours est installé, il est automatiquement attribué aux clients quand ces derniers sont installés selon la méthode d'installation Push du client. Pour suivre la progression d'installation du client, consultez les rapports de déploiement et d'attribution du client.

Les fichiers journaux du client fournissent des informations plus détaillées pour le dépannage. Les fichiers journaux ne nécessitent pas de point d'état de secours. Par exemple, le fichier **CCM.log** du serveur de site enregistre tous les problèmes de ce dernier au moment de se connecter à l'ordinateur. Le fichier **CCMSetup.log** du client enregistre le processus d'installation.

> **IMPORTANT**
> Afin que l'installation poussée du client réussisse, assurez-vous que toutes les conditions préalables sont respectées. Pour plus d'informations, consultez Dépendances liées aux méthodes d'installation.

**Configurer le site en vue de l'utilisation automatique de l'installation Push du client pour les ordinateurs découverts**

1. Dans la console Configuration Manager, choisissez **Administration** > **Configuration du site** > **Sites**.
2. Sélectionnez le site pour lequel vous souhaitez configurer l'installation poussée du client automatique à l'échelle du site.
3. Dans l'onglet **Accueil** du groupe **Paramètres**, choisissez **Paramètres d'installation du client** >

**Installation poussée du client**.

4. Dans l'onglet **Général** de la boîte de dialogue **Propriétés de l'installation poussée du client**, sélectionnez **Activer l'installation poussée du client automatique à l'échelle du site**. Sélectionnez les types de systèmes vers lesquels Configuration Manager doit transférer (push) le logiciel client.

5. Indiquez si vous souhaitez installer le client sur les contrôleurs de domaine.

6. Sous l'onglet **Comptes**, spécifiez le ou les comptes que Configuration Manager doit utiliser au moment de se connecter à l'ordinateur cible. Cliquez sur l'icône **Créer**, entrez le **nom d'utilisateur** et le **mot de passe** (pas plus de 38 caractères), confirmez le mot de passe, puis cliquez sur **OK**. Spécifiez au moins un compte d'installation Push du client. Ce compte doit disposer de droits d'administrateur local sur l'ordinateur cible pour pouvoir installer le client. Si vous ne spécifiez pas de compte d'installation Push du client, Configuration Manager essaie d'utiliser le compte d'ordinateur du système de site. L'utilisation du compte d'ordinateur système fait échouer l'installation Push du client sur plusieurs domaines.

   > **NOTE**
   > Pour utiliser l'installation Push du client sur un site secondaire, spécifiez le compte du site secondaire qui lance l'installation Push du client.
   >
   > Pour plus d'informations sur le compte d'installation Push du client, consultez la procédure suivante, Utiliser l'Assistant Installation Push du client.

7. Renseignez l'onglet **Propriétés de l'installation**.

   Si le schéma est étendu pour Configuration Manager, le site publie dans Active Directory Domain Services les Propriétés d'installation du client que vous spécifiez sous cet onglet. Ces propriétés sont lues par les installations du client dans lesquelles CCMSetup s'exécute sans propriétés d'installation.

   > **NOTE**
   > Si vous activez l'installation Push du client sur un site secondaire, veillez à ce que la propriété **SMSSITECODE** soit définie sur le nom de site Configuration Manager de son site principal parent. Si le schéma Active Directory est étendu pour Configuration Manager, vous pouvez aussi définir cette propriété sur AUTO pour rechercher automatiquement l'attribution de site correcte.

**Utiliser l'Assistant Installation Push du client**

1. Dans la console Configuration Manager, choisissez **Administration** > **Configuration du site** > **Sites**.

2. Sélectionnez le site pour lequel vous souhaitez configurer l'installation poussée du client automatique à l'échelle du site.

3. Dans l'onglet **Accueil** du groupe **Paramètres**, choisissez **Paramètres d'installation du client** > **Installation poussée du client**.

4. Renseignez l'onglet **Propriétés de l'installation**.

   Si le schéma est étendu pour Configuration Manager, le site publie dans Active Directory Domain Services les Propriétés d'installation du client que vous spécifiez sous cet onglet. Ces propriétés sont lues par les installations du client dans lesquelles CCMSetup s'exécute sans propriétés d'installation.

5. Dans la console Configuration Manager, choisissez **Ressources et Conformité**.

6. Dans l'espace de travail **Ressources et Conformité** , sélectionnez un ou plusieurs ordinateurs ou un regroupement d'ordinateurs.

7. Sous l'onglet **Accueil**, choisissez l'une des options suivantes :

   - Si vous souhaitez installer le client sur un seul ordinateur ou plusieurs ordinateurs, dans le groupe **Appareil**, choisissez **Installer le client**.
   - Si vous souhaitez installer le client dans un regroupement d'ordinateurs, dans le groupe **Regroupement**, choisissez **Installer le client**.

8. Dans la page **Avant de commencer** de l'**Assistant Installation du client**, consultez les informations, puis choisissez **Suivant**.

9. Renseignez la page **Options d'installation**.

10. Passez en revue les paramètres d'installation, puis fermez l'Assistant.

> **NOTE**
> Vous pouvez utiliser l'Assistant pour installer des clients même si le site n'est pas configuré pour l'installation Push du client.

## Guide pratique pour installer des clients à l'aide d'une installation basée sur une mise à jour logicielle

L'installation du client en fonction des mises à jour logicielles publie le client sur un point de mise à jour logicielle, sous forme de mise à jour logicielle. Utilisez cette méthode pour une première installation ou une mise à niveau.

Si le client Configuration Manager est installé sur un ordinateur, celle-ci reçoit la stratégie de configuration du client du site. Cette stratégie inclut le nom du serveur du point de mise à jour logicielle et le port à partir duquel les mises à jour logicielles sont obtenues.

> **IMPORTANT**
> Pour pouvoir utiliser l'installation basée sur les mises à jour logicielles, vous devez utiliser le même serveur Windows Server Update Services (WSUS) pour l'installation du client et les mises à jour logicielles. Ce serveur doit être utilisé comme le point de mise à jour logicielle actif dans un site principal. Pour plus d'informations, consultez Installer un point de mise à jour logicielle.

Si le client Configuration Manager n'est pas installé sur un ordinateur, configurez et attribuez un objet de stratégie de groupe dans Active Directory Domain Services pour spécifier le nom du serveur du point de mise à jour logicielle.

Il est impossible d'ajouter des propriétés de ligne de commande à une installation du client basée sur des mises à jour logicielles. Si vous avez étendu le schéma Active Directory pour Configuration Manager, les ordinateurs clients demandent automatiquement les propriétés d'installation à Active Directory Domain Services au moment de l'installation.

Si vous n'avez pas étendu le schéma Active Directory, vous pouvez utiliser la stratégie de groupe pour fournir les paramètres d'installation du client aux ordinateurs de votre site. Ces paramètres s'appliquent automatiquement à toutes les installations du client basé sur les mises à jour logicielles. Pour plus d'informations, consultez Comment fournir des propriétés d'installation du client (installation basée sur une stratégie de groupe et sur les mises à jour logicielles) et Comment attribuer des clients à un site.

Les procédures ci-dessous vous permettent de configurer des ordinateurs sans client Configuration Manager pour qu'ils utilisent le point de mise à jour logicielle pour l'installation du client et les mises à jour logicielles, et

pour qu'ils publient le logiciel client sur le point de mise à jour logicielle.

> **NOTE**
> Si les ordinateurs sont dans un état de redémarrage en attente suite à une précédente installation de logiciel, une installation du client basée sur une mise à jour logicielle peut entraîner le redémarrage de l'ordinateur.

**Configurez un objet de stratégie de groupe dans Active Directory Domain Services de façon à spécifier le point de mise à jour logicielle pour l'installation du client et les mises à jour logicielles :**

1. Utilisez la console de gestion des stratégies de groupe pour ouvrir un objet de stratégie de groupe nouveau ou existant.
2. Dans la console, développez **Configuration ordinateur**, **Modèles d'administration**, **Composants Windows**, puis choisissez **Windows Update**.
3. Ouvrez les propriétés du paramètre **Spécifier l'emplacement intranet du service de mise à jour Microsoft**, puis choisissez **Activé**.
4. Dans la zone **Set the intranet update service for detecting updates** (Définir le service intranet de mise à jour pour la détection des mises à jour), spécifiez le nom et le port du serveur du point de mise à jour logicielle :
   - Si le système de site Configuration Manager est configuré pour utiliser un nom de domaine complet (FQDN), utilisez le format de domaine complet.
   - Si le système de site Configuration Manager n'est pas configuré pour utiliser un nom de domaine complet (FQDN), utilisez un format de nom court.

   > **NOTE**
   > Pour déterminer le numéro de port, consultez Comment déterminer les paramètres de port utilisés par WSUS.

   Exemple : **http://server1.contoso.com:8530**
5. Dans la zone **Configurer le serveur intranet de statistiques**, spécifiez le nom du serveur intranet de statistiques. Cela ne doit pas être nécessairement le serveur du point de mise à jour logicielle. S'il s'agit du même serveur, le format ne doit pas nécessairement correspondre.
6. Attribuez l'objet de stratégie de groupe aux ordinateurs sur lesquels vous voulez installer le client et recevoir les mises à jour logicielles.

**Publier le client Configuration Manager sur le point de mise à jour logicielle**

1. Dans la console Configuration Manager, cliquez sur **Administration** > **Configuration de site** > **Sites**.
2. Sélectionnez le site pour lequel vous souhaitez configurer l'installation du client en fonction des mises à jour logicielles.
3. Dans l'onglet **Accueil** du groupe **Paramètres**, choisissez **Paramètres d'installation du client**, puis **Installation du client en fonction des mises à jour logicielles**.
4. Sélectionnez **Activer l'installation du client basée sur les mises à jour logicielles**.
5. Si la version du logiciel client est plus récente sur le serveur de site Configuration Manager que celle sur le point de mise à jour logicielle, la boîte de dialogue **Version plus récente du package client détectée** s'affiche. Cliquez sur **Oui** pour publier la version la plus récente.

> **NOTE**
> Si le logiciel client n'a pas été publié auparavant sur le point de mise à jour logicielle, cette boîte de dialogue est vide.

La mise à jour logicielle du client Configuration Manager n'est pas mise à jour automatiquement quand il existe une nouvelle version. Si vous mettez à niveau le site, ce qui comprend une nouvelle version du client, répétez cette procédure et cliquez sur **Oui** à l'étape 6.

## Guide pratique pour installer des clients à l'aide d'une stratégie de groupe

Vous pouvez utiliser la stratégie de groupe dans Active Directory Domain Services pour publier ou attribuer le client Configuration Manager en vue de l'installer sur des ordinateurs de votre entreprise. Le client s'installe au démarrage de l'ordinateur. Quand vous utilisez la stratégie de groupe, le client s'affiche dans **Ajout/Suppression de programmes** dans le Panneau de configuration pour permettre à l'utilisateur de procéder à l'installation.

Utilisez le package Windows Installer (CCMSetup.msi) pour les installations basées sur la stratégie de groupe. Ce fichier se trouve dans le dossier **<répertoire d'installation de ConfigMgr>\bin\i386** sur le serveur de site Configuration Manager. Vous ne pouvez pas ajouter des propriétés à ce fichier pour modifier le comportement à l'installation.

> **IMPORTANT**
> Vous devez disposer d'autorisations d'administrateur pour accéder aux fichiers d'installation du client.

- Si le schéma Active Directory est étendu pour Configuration Manager et que l'option **Publier ce site dans les services d'annuaire Active Directory** est sélectionnée sous l'onglet **Avancé** de la boîte de dialogue **Propriétés du site**, les ordinateurs clients demandent automatiquement les propriétés d'installation aux services de domaine Active Directory. Pour plus d'informations sur les propriétés d'installation publiées, consultez À propos de la publication des propriétés d'installation du client sur les services de domaine Active Directory.
- Si le schéma Active Directory n'a pas été étendu, vous pouvez appliquer la procédure de cette rubrique pour stocker les propriétés d'installation dans le Registre des ordinateurs : Comment fournir des propriétés d'installation du client (Stratégie de groupe et installation du client basé sur les mises à jour logicielles). Ces propriétés d'installation sont utilisées pendant l'installation du client.

Pour plus d'informations sur l'utilisation de la stratégie de groupe dans Active Directory Domain Services pour installer des logiciels, consultez la documentation Windows Server.

## Guide pratique pour installer des clients manuellement

Vous pouvez installer manuellement le logiciel client sur les ordinateurs dans votre entreprise à l'aide du programme CCMSetup.exe. Ce programme et ses fichiers de prise en charge se trouvent dans le dossier **Client** du dossier d'installation de Configuration Manager sur le serveur de site et sur les points de gestion dans votre site. Ce dossier est partagé sur le réseau sous

\\<*nom du serveur de site*> \SMS_<*code de site*> \Client\

où <*nom du serveur de site*> est le nom d'un des serveurs hébergeant un point de gestion et <*code de site*> est le code du site principal auquel le client est attribué. Pour exécuter CCMSetup.exe à partir de la ligne de

commande sur le client, vous devez mapper un lecteur réseau à cet emplacement, puis exécuter la commande.

> **IMPORTANT**
> Vous devez disposer d'autorisations d'administrateur pour accéder aux fichiers d'installation du client.

Le programme CCMSetup.exe copie toutes les conditions préalables nécessaires sur l'ordinateur client, puis fait appel au package Windows Installer (Client.msi) pour installer le client. Vous ne pouvez pas exécuter Client.msi directement.

Vous pouvez spécifier des propriétés de ligne de commande pour CCMSetup.exe et Client.msi afin de modifier le comportement de l'installation du client. Spécifiez les propriétés de CCMSetup (propriétés commençant par **/**) avant de spécifier les propriétés de Client.msi. Par exemple :

```
CCMSetup.exe /mp:SMSMP01 /logon SMSSITECODE=AUTO FSP=SMSFP01
```

et le client s'installe en utilisant les propriétés suivantes :

| PROPRIÉTÉ | DESCRIPTION |
|---|---|
| **/mp:SMSMP01** | Cette propriété de CCMSetup spécifie le point de gestion SMSMP01 pour télécharger les fichiers requis d'installation du client. |
| **/logon** | Cette propriété de CCMSetup spécifie que l'installation doit s'arrêter si un client Configuration Manager se trouve déjà sur l'ordinateur. |
| **SMSSITECODE=AUTO** | Cette propriété de Client.msi spécifie que le client doit essayer de trouver le code de site Configuration Manager à utiliser, par exemple, en utilisant les services de domaine Active Directory. |
| **FSP=SMSFP01** | Cette propriété de Client.msi précise que le point d'état de secours nommé SMSFP01 est utilisé pour recevoir les messages d'état envoyés par l'ordinateur client. |

Pour obtenir des détails sur toutes les propriétés de CCMSetup.exe, consultez À propos des propriétés d'installation du client.

> **TIP**
> Pour plus d'informations sur la procédure d'installation du client Configuration Manager sur un appareil Windows 10 moderne utilisant l'identité Azure AD, consultez Installer et affecter des clients Windows 10 Configuration Manager à l'aide d'Azure AD à des fins d'authentification. Cette procédure concerne les clients sur intranet ou Internet.

### Exemples

Ces exemples concernent les clients Active Directory sur intranet. Ils utilisent les valeurs suivantes pour représenter les différents aspects du site :

**MPSERVER** = serveur hébergeant le point de gestion
**FSPSERVER** = serveur hébergeant le point d'état de secours
**ABC** = code de site
**contoso.com** = nom de domaine

Tous les serveurs de système de site sont configurés avec un nom de domaine complet d'intranet. Le site est

publié dans la forêt Active Directory du client.

Sur l'ordinateur client, ouvrez une session en tant qu'administrateur local, mappez un lecteur (z:) à \\MPSERVER\SMS_ABC\Client, indiquez le lecteur z à l'invite de commandes, puis exécutez l'une des commandes suivantes :

**Exemple 1 :**

```
CCMSetup.exe
```

Cet exemple installe le client sans propriétés supplémentaires. Le client est configuré automatiquement par rapport aux propriétés d'installation du client publiées dans Active Directory Domain Services. Il est automatiquement configuré pour les paramètres suivants :

- Code de site. Ce paramètre exige que l'emplacement réseau du client soit inclus dans un groupe de limites configuré pour l'attribution du client.
- Point de gestion
- Point d'état de secours
- Communiquer à l'aide de HTTPS uniquement

Pour plus d'informations, consultez À propos de la publication des propriétés d'installation du client sur les services de domaine Active Directory.

**Exemple 2 :**

```
CCMSetup.exe /MP:mpserver.contoso.com /UsePKICert SMSSITECODE=ABC CCMHOSTNAME=server05.contoso.com
CCMFIRSTCERT=1 FSP=server06.constoso.com
```

Cet exemple ignore la configuration automatique fournie par Active Directory Domain Services. Il n'exige pas que l'emplacement réseau du client soit inclus dans un groupe de limites configuré pour l'attribution du client. En revanche, l'installation spécifie les paramètres suivants :

- Code de site
- Point de gestion intranet
- Point de gestion Internet
- Point d'état de secours qui accepte les connexions en provenance d'Internet
- Utiliser un certificat client PKI (si disponible) qui offre la plus longue période de validité

## Guide pratique pour installer des clients à l'aide de scripts d'ouverture de session

Configuration Manager prend en charge les scripts d'ouverture de session pour installer le logiciel client Configuration Manager. Vous pouvez utiliser le fichier programme **CCMSetup.exe** dans un script de connexion pour déclencher l'installation du client.

L'installation via un script d'ouverture de session utilise les mêmes méthodes que l'installation manuelle du client. Vous pouvez spécifier la propriété d'installation **/logon** pour CCMSsetup.exe. S'il existe déjà une version du client sur l'ordinateur, cette propriété empêche l'installation du client. Ce comportement empêche la réinstallation du client à chaque exécution du script d'ouverture de session.

Si aucune source d'installation n'est spécifiée par la propriété **/Source** et qu'aucun point de gestion à partir duquel obtenir l'installation n'est spécifié par la propriété **/MP**, CCMSetup.exe recherche le point de gestion dans Active Directory Domain Services. Ce comportement se produit uniquement si le schéma a été étendu pour Configuration Manager et que le site est publié dans Active Directory Domain Services. Alternativement, le client peut utiliser le service de nom de domaine (DNS) ou WINS pour rechercher un point de gestion.

# Guide pratique pour installer des clients à l'aide d'un package et d'un programme

Vous pouvez utiliser Configuration Manager pour créer et déployer un package et un programme qui mettent à niveau le logiciel client sur les ordinateurs sélectionnés dans votre hiérarchie. Un fichier de définition de package pour renseigner les propriétés du package avec les valeurs généralement utilisées est fourni avec Configuration Manager. Vous pouvez personnaliser le comportement de l'installation du client en spécifiant des propriétés de ligne de commande supplémentaires.

> **NOTE**
>
> Vous ne pouvez pas mettre à niveau des clients Configuration Manager 2007 avec cette méthode. Au lieu de cela, utilisez la mise à niveau automatique des clients, qui crée et déploie automatiquement un package contenant la dernière version du client. Pour plus d'informations, consultez Mettre à niveau les clients.
>
> Pour plus d'informations sur la migration à partir de versions plus anciennes du client Configuration Manager, consultez Planification d'une stratégie de migration de clients.

**Créer un package et un programme pour le logiciel client**

Pour créer un package et un programme Configuration Manager que vous pouvez déployer sur les ordinateurs clients Configuration Manager afin de mettre à niveau le logiciel client, utilisez la procédure suivante.

1. Dans la console Configuration Manager, choisissez **Bibliothèque de logiciels** > **Gestion des applications** > **Packages**.
2. Sous l'onglet **Accueil**, dans le groupe **Créer**, choisissez **Créer un package à partir de la définition**.
3. Dans la page **Définition du package** de l'Assistant, sélectionnez **Microsoft** dans la liste déroulante **Éditeur** et **Mise à niveau du client Configuration Manager** dans la liste **Définition du package**.
4. Dans la page **Fichiers sources**, sélectionnez **Toujours obtenir les fichiers depuis le dossier source**.
5. Dans la page **Dossier source**, sélectionnez **Chemin d'accès réseau (nom UNC)**. Entrez ensuite le chemin réseau de l'ordinateur et du dossier contenant les fichiers d'installation du client.

   > **NOTE**
   >
   > L'ordinateur sur lequel le déploiement de Configuration Manager s'effectue doit avoir accès au dossier réseau spécifié. Dans le cas contraire, l'installation échoue.

   Pour modifier l'une des propriétés d'installation du client, modifiez les paramètres de ligne de commande CCMSetup.exe sous l'onglet **Général** de la boîte de dialogue du programme **Propriétés des mises à niveau silencieuses de l'Agent Configuration Manager**. Les propriétés d'installation par défaut sont **/noservice SMSSITECODE=AUTO**.
6. Distribuez le package à tous les points de distribution qui doivent héberger le package de mise à niveau des clients. Vous pouvez ensuite déployer le package sur des regroupements d'ordinateurs contenant les clients à mettre à niveau.

# Comment installer des clients sur des appareils Windows gérés par Intune MDM

Vous pouvez déployer les fichiers d'installation du client sur les ordinateurs qui sont inscrits dans Microsoft Intune.

Cette procédure s'applique aux clients traditionnels connectés à l'intranet. Elle utilise des méthodes d'authentification de client classiques. Pour que l'appareil reste dans un état géré une fois le logiciel client installé, il doit se trouver sur l'intranet et dans une limite de site Configuration Manager.

Pour plus d'informations sur la procédure d'installation du client Configuration Manager sur un appareil Windows 10 moderne utilisant l'identité Azure AD, consultez Installer et affecter des clients Windows 10 Configuration Manager à l'aide d'Azure AD à des fins d'authentification.

> **NOTE**
> Une fois le logiciel client installé, l'appareil est désinscrit d'Intune.
>
> Depuis la version 1710, les clients ne se désinscrivent pas d'Intune. Ils peuvent disposer à la fois du client Configuration Manager et d'une inscription MDM. Pour plus d'informations, consultez Cogestion.

**Installez les clients avec Intune :**

1. Dans Intune, créez une application contenant le fichier d'installation du client Configuration Manager **ccmsetup.msi**. Ce fichier se trouve dans le dossier **<répertoire d'installation de ConfigMgr>\bin\i386** sur le serveur de site Configuration Manager.

2. Dans l'Éditeur de logiciel Intune, entrez des paramètres de ligne de commande. Par exemple, utilisez la ligne de commande suivante avec un client classique sur l'intranet :

   ```
   CCMSETUPCMD="/MP:&lt;FQDN of management point> SMSMP=&lt;FQDN of management point>
   SMSSITECODE=&lt;Your site code> DNSSUFFIX=&lt;DNS Suffix of management point>"
   ```

   > **NOTE**
   > Pour obtenir un exemple de ligne commande à utiliser avec un client Windows 10 moderne exploitant l'authentification Azure AD, consultez Préparer des appareils Windows 10 à la cogestion.

3. Déployez l'application sur les ordinateurs Windows inscrits.

## Guide pratique pour installer des clients à l'aide d'une image de l'ordinateur

Vous pouvez préinstaller le logiciel client Configuration Manager sur un ordinateur de référence que vous pouvez utiliser pour créer une image de système d'exploitation.

> **IMPORTANT**
> Quand vous utilisez la séquence de tâches Configuration Manager pour déployer l'image du système d'exploitation, l'étape Préparer le client ConfigMgr de la séquence de tâches supprime entièrement le client Configuration Manager.

**Préparer l'ordinateur client à la mise en image**

1. Installez manuellement le logiciel client Configuration Manager sur l'ordinateur de référence. Pour plus d'informations, voir Comment installer les clients Configuration Manager manuellement.

   > **IMPORTANT**
   > Ne spécifiez pas de code de site Configuration Manager pour le client dans les propriétés de ligne de commande CCMSetup.exe.

2. À l'invite de commandes, tapez `net stop ccmexec` pour vérifier que le service **Hôte de l'agent SMS** (Ccmexec.exe) ne s'exécute pas sur l'ordinateur de référence.
3. Supprimez le fichier **SMSCFG.INI** du dossier **Windows** sur l'ordinateur de référence.
4. Supprimez les certificats qui sont éventuellement stockés dans le magasin local de l'ordinateur de référence. Par exemple, si vous utilisez des certificats d'infrastructure à clé publique (PKI), vous devez supprimer les certificats dans le magasin **Personnel** de l' **Ordinateur** et de l' **Utilisateur** avant de mettre l'ordinateur en image.
5. Si les clients sont installés dans une hiérarchie Configuration Manager différente de celle de l'ordinateur de référence, supprimez la clé racine approuvée de cet ordinateur.

   > **NOTE**
   > Si les clients ne peuvent pas demander aux services de domaine Active Directory de localiser un point de gestion, ils peuvent utiliser une clé racine approuvée pour déterminer les points de gestion approuvés. Si tous les clients mis en image sont déployés dans la même hiérarchie que celle de l'ordinateur maître, conservez la clé racine approuvée. Si les clients sont déployés dans des hiérarchies différentes, supprimez la clé racine approuvée. De même, fournissez la nouvelle clé racine approuvée à ces clients. Pour plus d'informations, voir Planification de la clé racine approuvée.
6. Utilisez votre logiciel d'acquisition d'images pour capturer l'image de l'ordinateur maître.
7. Déployez l'image vers les ordinateurs de destination.

## Guide pratique pour installer des clients sur les ordinateurs d'un groupe de travail

Configuration Manager prend en charge l'installation du client sur des ordinateurs de groupe de travail. Installez le client sur les ordinateurs du groupe de travail à l'aide de la méthode spécifiée dans Comment installer les clients Configuration Manager manuellement.

Conditions préalables :

- Le client doit être installé manuellement sur chaque ordinateur du groupe de travail. Durant l'installation, l'utilisateur connecté doit disposer des droits d'administrateur local.
- Pour accéder aux ressources du domaine du serveur de site Configuration Manager, le compte d'accès réseau doit être configuré pour le site. Spécifiez ce compte comme une propriété du composant de distribution de logiciels. Pour plus d'informations, voir Site components for System Center Configuration Manager.

Limitations :

- Les clients du groupe de travail ne peuvent pas localiser les points de gestion depuis les services de domaine Active Directory et doivent à la place utiliser DNS, WINS ou un autre point de gestion.
- L'itinérance globale n'est pas prise en charge parce que les clients ne peuvent pas demander d'information de site aux services de domaine Active Directory.
- Les méthodes de découverte d'Active Directory ne découvriront pas les ordinateurs dans des groupes de travail.
- Vous ne pouvez pas déployer de logiciels vers les utilisateurs d'ordinateurs de groupe de travail.
- Vous ne pouvez pas utiliser la méthode d'installation poussée du client pour installer le client sur des ordinateurs du groupe de travail.

- Les clients du groupe de travail ne peuvent pas utiliser Kerberos pour l'authentification et peuvent donc nécessiter une approbation manuelle.
- Un client de groupe de travail ne peut pas être configuré comme point de distribution. Configuration Manager impose que les ordinateurs faisant office de points de distribution soient membres d'un domaine.

**Installer le client sur les ordinateurs d'un groupe de travail**

Vérifiez les prérequis, puis suivez les instructions de la section Comment installer les clients Configuration Manager manuellement.

Dans cet exemple, le client est installé pour être géré sur l'intranet, tandis que le code de site et le suffixe DNS sont spécifiés pour localiser un point de gestion. `CCMSetup.exe SMSSITECODE=ABC DNSSUFFIX=constoso.com`

Dans cet exemple, le client doit se trouver à un emplacement réseau configuré dans un groupe de limites. Cette exigence vise à ce que l'attribution automatique de site réussisse. La commande inclut un point d'état de secours sur le serveur FSPSERVER. Cette propriété facilite le suivi du déploiement du client et permet d'identifier les éventuels problèmes de communication du client. `CCMSetup.exe FSP=fspserver.constoso.com`

## Comment installer les clients pour assurer leur gestion sur Internet

> **NOTE**
> Cette section ne s'applique pas aux clients utilisant une passerelle de gestion cloud. Pour installer des clients basés sur Internet en utilisant une passerelle de gestion cloud, consultez Installer et affecter des clients Windows 10 Configuration Manager à l'aide d'Azure AD à des fins d'authentification.

Si le site Configuration Manager prend en charge la gestion des clients basée sur Internet pour des clients pouvant être sur l'intranet ou sur Internet, deux options s'offrent à vous au moment d'installer les clients sur l'intranet :

- Vous pouvez inclure la propriété Client.msi de CCMHOSTNAME=<*nom de domaine complet Internet du point de gestion Internet*> quand vous installez le client, par exemple avec la méthode d'installation manuelle ou Push du client. Lorsque vous utilisez cette méthode, vous devez également attribuer directement le client au site et vous ne pouvez pas utiliser l'attribution de site automatique. La section Comment installer les clients Configuration Manager manuellement de cette rubrique fournit un exemple de cette méthode de configuration.
- Vous pouvez installer le client dans l'optique d'une gestion des clients sur intranet, puis attribuer au client un point de gestion des clients basé sur Internet. Modifiez le point de gestion via les propriétés du client Configuration Manager dans le panneau de configuration ou à l'aide d'un script. Lorsque vous utilisez cette méthode, vous pouvez utiliser l'attribution automatique des clients. Pour plus d'informations, consultez la section Comment configurer les clients en vue de les gérer via Internet après leur installation de cette rubrique.

  Si vous devez installer des clients qui se trouvent sur Internet, choisissez l'une des méthodes prises en charge suivantes :

- Prévoyez un mécanisme permettant à ces clients de se connecter temporairement à l'intranet via un réseau privé virtuel (VPN). Installez ensuite le client en employant une méthode d'installation du client appropriée.
- Utilisez une méthode d'installation indépendante de Configuration Manager. Par exemple, empaquetez les fichiers sources d'installation du client sur un média amovible que vous pouvez envoyer aux utilisateurs avec des instructions d'installation. Les fichiers sources d'installation du client se trouvent

dans le dossier <*chemin_installation*> \Client sur le serveur de site et les points de gestion Configuration Manager. Incorporez au support un script à copier manuellement vers le dossier du client et depuis ce dossier, installez le client à l'aide de CCMSetup.exe et de toutes les propriétés de ligne commande CCMSetup appropriées.

> **NOTE**
> Configuration Manager ne prend pas en charge l'installation directe d'un client à partir du point de gestion Internet ou du point de mise à jour logicielle Internet.

Les clients gérés via internet doivent communiquer avec des systèmes de site basés sur Internet. Vérifiez que ces clients possèdent aussi des certificats d'infrastructure à clé publique (PKI) avant d'installer le client. Installez ces certificats indépendamment de Configuration Manager. Pour plus d'informations sur la configuration requise des certificats, consultez Configuration requise des certificats PKI.

**Installer des clients sur Internet en spécifiant des propriétés de ligne de commande CCMSetup**

1. Suivez les instructions de la section Comment installer les clients Configuration Manager manuellement et incluez toujours les éléments suivants :

   - Propriété de ligne de commande CCMSetup **/source:**<*chemin local du dossier Client copié*>
   - Propriété de ligne de commande CCMSetup **/UsePKICert:**
   - Propriété Client.msi **CCMHOSTNAME=**<*nom de domaine complet du point de gestion Internet*>
   - Propriété Client.msi **SMSSIGNCERT=**<*chemin local du certificat de signature du serveur de site exporté*>
   - Propriété Client.msi **SMSSITECODE=**<*code de site du point de gestion Internet*>

   > **NOTE**
   > Si le site comporte plusieurs points de gestion Internet, le choix du point de gestion Internet importe peu pour la propriété CCMHOSTNAME. Quand un client Configuration Manager se connecte au point de gestion Internet spécifié, le point de gestion envoie au client une liste des points de gestion Internet disponibles sur le site. Le client en sélectionne un de façon aléatoire dans la liste.

2. Si vous ne souhaitez pas que le client vérifie la liste de révocation de certificats (CRL), spécifiez la propriété de ligne de commande CCMSetup **/NoCRLCheck**.

3. Si vous utilisez un point d'état de secours Internet, spécifiez la propriété Client.msi **FSP=**<*nom de domaine complet Internet du point d'état de secours Internet*>.

4. Si vous installez le client pour la gestion des clients Internet uniquement, spécifiez la propriété Client.msi **CCMALWAYSINF=1**.

5. Vérifiez si vous devez spécifier des propriétés de ligne de commande CCMSetup supplémentaires. Par exemple, vous pouvez avoir besoin de spécifier un critère de sélection de certificat si le client possède plusieurs certificats d'infrastructure à clé publique (PKI) valides. Pour obtenir la liste des propriétés d'installation disponibles, consultez À propos des propriétés d'installation du client.

   Exemple :

   ```
   CCMSetup.exe /source: D:\Clients /UsePKICert CCMHOSTNAME=server1.contoso.com
   SMSSIGNCERT=siteserver.cer SMSSITECODE=ABC FSP=server2.contoso.com CCMALWAYSINF=1 CCMFIRSTCERT=1
   ```

   Cet exemple installe le client avec les comportements suivants :

- Utilisation des fichiers sources à partir d'un dossier situé sur le lecteur D
- Utilisation d'un certificat PKI du client
- Sélection du certificat présentant la plus longue période de validité
- Gestion des clients Internet uniquement
- Attribuer au client l'utilisation du point de gestion Internet nommé SERVER1
- Attribuer le point d'état de secours Internet dans le domaine contoso.com
- Attribuer le client au site ABC

**Pour configurer les clients en vue d'une gestion sur Internet après leur installation**

Pour attribuer le point de gestion Internet après avoir installé le client, utilisez l'une de ces procédures. La première procédure reposant sur une configuration manuelle, elle est adaptée à un nombre de clients limité. En revanche, si vous avez un grand nombre de clients à configurer, la deuxième procédure est plus appropriée.

#### Configurer les clients en vue d'une gestion via Internet après leur installation en leur attribuant le point de gestion Internet dans les propriétés de Configuration Manager

1. Accédez à **Configuration Manager** dans le Panneau de configuration de l'ordinateur client, puis double-cliquez dessus pour ouvrir ses propriétés.
2. Sous l'onglet **Internet**, entrez le nom de domaine complet du point de gestion Internet dans la zone de texte FQDN Internet.

   > **NOTE**
   > L'onglet **Internet** est disponible uniquement si le client dispose d'un certificat PKI client.

3. Si le client accède à Internet via un serveur proxy, entrez les paramètres de ce dernier.

#### Configurer les clients en vue d'une gestion via Internet après leur installation au moyen d'un script

1. Ouvrez un éditeur de texte, tel que le Bloc-notes.
2. Copiez l'exemple VBScript suivant et insérez-le dans le fichier. Remplacez *mp.contoso.com* par le nom de domaine complet Internet de votre point de gestion Internet.

```
on error resume next

' Create variables.
Dim newInternetBasedManagementPointFQDN
Dim client

newInternetBasedManagementPointFQDN = "mp.contoso.com"

' Create the client COM object.
Set client = CreateObject ("Microsoft.SMS.Client")

' Set the internet-based management point FQDN by calling the SetCurrentManagementPoint method.
client.SetInternetManagementPointFQDN newInternetBasedManagementPointFQDN

' Clear variables.
Set client = Nothing
Set internetBasedManagementPointFQDN = Nothing
```

> **NOTE**
> Si vous devez supprimer un point de gestion Internet spécifié pour éviter que le client utilise un point de gestion Internet, supprimez la valeur entre guillemets de sorte que cette ligne se présente ainsi :
> `newInternetBasedManagementPointFQDN = ""`

3. Enregistrez le fichier avec une extension .vbs.
4. Utilisez cscript.exe pour exécuter le script sur les ordinateurs clients en employant l'une des méthodes suivantes :
   - Déployez le fichier sur les clients Configuration Manager existants en utilisant un package et un programme.
   - Exécutez le fichier localement sur les clients Configuration Manager existants en double-cliquant sur le fichier de script dans l'Explorateur Windows.

   Vous devrez peut-être redémarrer le client pour que les modifications prennent effet.

## Guide pratique pour fournir les propriétés d'installation du client (installation basée sur une stratégie de groupe et sur les mises à jour logicielles)

Vous pouvez utiliser la stratégie de groupe Windows pour fournir les propriétés d'installation du client Configuration Manager aux ordinateurs. Ces propriétés sont stockées dans le Registre de l'ordinateur et lues quand le logiciel client est installé. Cette procédure n'est généralement pas obligatoire, mais peut s'avérer nécessaire dans certains scénarios d'installation du client, par exemple :

- Vous utilisez les paramètres de stratégie de groupe ou des méthodes d'installation du logiciel basée sur des mises à jour logicielles. Vous n'avez pas étendu le schéma Active Directory pour Configuration Manager.
- Vous souhaitez redéfinir les propriétés de l'installation du client sur certains ordinateurs.

> **NOTE**
> Si des propriétés d'installation sont fournies sur la ligne de commande CCMSetup.exe, les propriétés d'installation fournies aux ordinateurs ne sont pas utilisées.

Le modèle d'administration de stratégie de groupe nommé ConfigMgrInstallation.adm est fourni sur le média d'installation de Configuration Manager. Ce modèle permet de fournir les propriétés d'installation aux ordinateurs clients.

**Configurer et attribuer des propriétés d'installation du client à l'aide d'un objet de stratégie de groupe**

1. Importez le modèle d'administration ConfigMgrInstallation.adm dans un objet de stratégie de groupe nouveau ou existant, à l'aide d'un éditeur tel que l'Éditeur d'objets de stratégie de groupe Windows. Le fichier se trouve dans le dossier **TOOLS\ConfigMgrADMTemplates** du média d'installation de Configuration Manager.
2. Affichez les propriétés du paramètre importé **Configurer les paramètres de déploiement du client**.
3. Choisissez **Activé**.
4. Dans la zone **CCMSetup** , entrez les propriétés de ligne de commande CCMSetup requises. Pour obtenir la liste de toutes les propriétés de ligne de commande CCMSetup et des exemples montrant comment les utiliser, consultez À propos des propriétés d'installation du client.
5. Attribuez l'objet stratégie de groupe aux ordinateurs auxquels vous souhaitez fournir les propriétés d'installation du client Configuration Manager.

Pour plus d'informations sur la stratégie de groupe Windows, consultez la documentation Windows Server.

# Étapes suivantes

Pour obtenir de l'aide sur l'installation du client Configuration Manager, consultez Méthodes d'installation du client.

# Installer et affecter des clients Windows 10 Configuration Manager à l'aide d'Azure AD à des fins d'authentification

22/06/2018 • 7 minutes to read • Edit Online

Pour installer le client Configuration Manager sur des appareils Windows 10 en utilisant l'authentification Azure AD, intégrez Configuration Manager à Azure Active Directory (Azure AD). Les clients peuvent être sur l'intranet, communiquant directement avec un point de gestion HTTPS. Ils peuvent aussi communiquer sur Internet via la passerelle de gestion cloud ou avec un point de gestion Internet. Ce processus utilise Azure AD pour authentifier les clients auprès du site Configuration Manager. Azure AD élimine le besoin de configurer et d'utiliser des certificats d'authentification client.

## Avant de commencer

- Un locataire Azure AD est un prérequis.
- Conditions requises pour les appareils :
  - Windows 10
  - Joint à Azure AD, joint à un domaine pur cloud ou joint à Azure AD hybride
- Conditions requises pour les utilisateurs :
  - L'utilisateur connecté doit être une identité Azure AD.
  - Si l'utilisateur est une identité fédérée ou synchronisée, vous devez utiliser la découverte d'utilisateurs Active Directory de Configuration Manager ainsi que la découverte d'utilisateurs Azure AD. Pour plus d'informations sur les identités hybrides, consultez Définir une stratégie d'adoption des identités hybrides.
- En plus des prérequis pour le rôle de système de site du point de gestion, activez aussi **ASP.NET 4.5** sur ce serveur. Incluez toutes les autres options qui sont sélectionnées automatiquement quand vous activez ASP.NET 4.5.
- Configurez tous les points de gestion pour le mode HTTPS. Pour plus d'informations, consultez Spécifications pour les certificats d'infrastructure à clé publique et Déployer le certificat de serveur web pour les systèmes de site qui exécutent IIS.
  - Si vous utilisez la passerelle de gestion cloud, vous devez uniquement configurer HTTPS pour les points de gestion que vous activez pour celle-ci.
  - Si vous déployez des clients sur l'intranet à l'aide de l'authentification basée sur un jeton Azure AD, tous les points de gestion que ces clients peuvent contacter doivent être activés pour HTTPS.
- Vous pouvez aussi configurez une passerelle de gestion cloud pour déployer des clients Internet. Pour les clients locaux qui s'authentifient avec Azure AD, vous n'avez pas besoin d'une passerelle de gestion cloud.

## Configurer des services Azure pour la gestion cloud

La première étape consiste à connecter votre site Configuration Manager à Azure AD. Pour plus d'informations sur ce processus, consultez Configurer des services Azure. Créez une connexion au service de **gestion cloud**.

Activez Découverte d'utilisateurs Azure AD dans le cadre de l'intégration à la **gestion cloud**.

Une fois ces actions effectuées, votre site Configuration Manager est connecté à Azure AD.

## Configurer les paramètres client

Ces paramètres client permettent de joindre des appareils Windows 10 à Azure AD. Ils permettent également aux clients Internet d'utiliser la passerelle de gestion cloud et le point de distribution cloud.

1. Configurez les paramètres client suivants dans la section **Services cloud** en utilisant les informations du Guide pratique pour configurer les paramètres client.

   - **Autoriser l'accès au point de distribution cloud** : activez ce paramètre afin que les appareils Internet puissent obtenir le contenu nécessaire pour installer le client Configuration Manager. Si le contenu n'est pas disponible sur le point de distribution cloud, les appareils peuvent récupérer le contenu auprès de la passerelle de gestion cloud. Le programme d'amorçage de l'installation du client réessaye le point de distribution cloud pendant 4 heures avant de passer à la passerelle de gestion cloud.

   - **Inscrire automatiquement les nouveaux appareils joints à un domaine Windows 10 avec Azure Active Directory** : définissez ce paramètre sur **Oui** ou sur **Non**. La valeur par défaut est **Oui**. Ce comportement est également celui par défaut dans Windows 10, version 1709.

   - **Permettre aux clients d'utiliser une passerelle de gestion cloud** : réglez sur **Oui** (valeur par défaut) ou **Non**.

2. Déployez les paramètres client sur la collection requise d'appareils. Ne déployez pas ces paramètres sur des regroupements d'utilisateurs.

Pour vérifier que l'appareil est joint à Azure AD, exécutez `dsregcmd.exe /status` dans une invite de commandes. Le champ **AzureAdjoined** dans les résultats indique **OUI** si l'appareil est joint à Azure AD.

## Installer et inscrire le client avec l'identité Azure AD

Pour installer manuellement le client avec l'identité Azure AD, passez d'abord en revue le processus général dans Comment installer des clients manuellement.

> **NOTE**
> L'appareil a besoin d'accéder à Internet pour contacter Azure AD, mais n'a pas besoin d'être basé sur Internet.

L'exemple suivant montre la structure générale de la ligne de commande :

```
ccmsetup.exe /mp:<source management point> CCMHOSTNAME=<internet-based management point> SMSSiteCode=<site code>
SMSMP=<initial management point> AADTENANTID=<Azure AD tenant identifier> AADCLIENTAPPID=<Azure AD client app
identifier> AADRESOURCEURI=<Azure AD server app identifier>
```

Pour plus d'informations, consultez Propriétés de l'installation du client.

Les propriétés /mp et CCMHOSTNAME spécifient l'un des éléments suivants, en fonction du scénario :

- Point de gestion local. Spécifiez seulement la propriété /mp. CCMHOSTNAME n'est pas obligatoire.
- Passerelle de gestion cloud
- Point de gestion Internet. La propriété SMSMP spécifie le point de gestion Internet ou local.

Cet exemple utilise une passerelle de gestion cloud. Il remplace les exemples de valeurs pour chaque propriété :

```
ccmsetup.exe /mp:https://CONTOSO.CLOUDAPP.NET/CCM_Proxy_MutualAuth/72186325152220500
CCMHOSTNAME=CONTOSO.CLOUDAPP.NET/CCM_Proxy_MutualAuth/72186325152220500 SMSSiteCode=ABC
SMSMP=https://mp1.contoso.com AADTENANTID=daf4a1c2-3a0c-401b-966f-0b855d3abd1a AADCLIENTAPPID=7506ee10-f7ec-
415a-b415-cd3d58790d97 AADRESOURCEURI=https://contososerver
```

Pour automatiser l'installation en utilisant l'identité Azure AD via Microsoft Intune, consultez le processus pour Préparer les appareils Windows 10 pour la cogestion.

## Étapes suivantes

Une fois terminé, vous pouvez continuer à surveiller et gérer les clients.

# À propos des propriétés et des paramètres d'installation du client dans System Center Configuration Manager

22/06/2018 • 50 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez la commande CCMSetup.exe pour installer le client Configuration Manager. Si des paramètres d'installation du client sont indiqués en ligne de commande, ils modifient le comportement de l'installation. Si vous fournissez des propriétés d'installation du client en ligne de commande, elles modifient la configuration initiale de l'agent client installé.

## À propos de CCMSetup.exe

La commande CCMSetup.exe télécharge les fichiers nécessaires pour installer le client à partir d'un point de gestion ou d'un emplacement source. Ces fichiers peuvent être les suivants :

- Le fichier client.msi du package Windows Installer qui installe le logiciel client.
- Les fichiers d'installation du service BITS (Background Intelligent Transfer Service) de Microsoft.
- Les fichiers d'installation de Windows Installer.
- Les mises à jour et correctifs du client Configuration Manager.

> **NOTE**
> Dans Configuration Manager, vous ne pouvez pas exécuter directement le fichier Client.msi.

CCMSetup.exe fournit des paramètres de ligne de commande pour personnaliser l'installation. Ils sont précédés d'une barre oblique inverse et, par convention, sont en minuscules. La valeur d'un paramètre, si nécessaire, est spécifiée à l'aide d'un signe deux-points directement suivi de la valeur souhaitée. Vous pouvez également fournir des propriétés qui modifient le comportement de client.msi dans la ligne de commande de CCMSetup.exe. Par convention, les propriétés sont tout en majuscules. La valeur d'une propriété est spécifiée à l'aide d'un signe égal directement suivi de la valeur souhaitée.

> **IMPORTANT**
> Spécifiez les paramètres de CCMSetup avant de spécifier les propriétés de client.msi.

CCMSetup.exe et les fichiers de prise en charge se trouvent sur le serveur de site dans le dossier **Client** du dossier d'installation de Configuration Manager. Ce dossier est partagé sur le réseau sous **<Nom_Serveur_Site>\SMS_<Code_Site>\Client**.

À l'invite de commandes, la commande CCMSetup.exe utilise le format suivant :

```
CCMSetup.exe [<Ccmsetup parameters>] [<client.msi setup properties>]
```

Par exemple :

```
CCMSetup.exe /mp:SMSMP01 /logon SMSSITECODE=S01 FSP=SMSFSP01
```

Cet exemple effectue les opérations suivantes :

- Force le point de gestion SMSMP01 à demander la liste des points de distribution pour télécharger les fichiers d'installation du client.
- Force l'arrêt de l'installation si une version du client existe déjà sur l'ordinateur.
- Ordonne à client.msi d'attribuer le client au code de site S01.
- Ordonne à client.msi d'utiliser le point d'état de secours nommé SMSFP01.

> **NOTE**
> Si la valeur d'un paramètre contient des espaces, placez-la entre guillemets.

> **IMPORTANT**
> Si vous avez étendu le schéma Active Directory pour Configuration Manager, le site publie de nombreuses propriétés d'installation du client dans les services de domaine Active Directory. Le client Configuration Manager lit automatiquement ces propriétés. Pour plus d'informations, consultez À propos de la publication des propriétés d'installation du client sur les services de domaine Active Directory.

## Paramètres de ligne de commande de CCMSetup.exe

**/?**

Ouvre la boîte de dialogue **CCMSetup**, qui affiche les paramètres de ligne de commande de ccmsetup.exe.

Exemple : **ccmsetup.exe /?**

**/source:<Chemin>**

Spécifie l'emplacement de téléchargement des fichiers. Utilisez un chemin local ou UNC. Les fichiers sont téléchargés à l'aide du protocole SMB (server message block). Pour utiliser **/source**, le compte d'utilisateur Windows pour l'installation du client doit avoir les autorisations Lecture sur l'emplacement.

> **NOTE**
> Vous pouvez utiliser le paramètre **/source** plusieurs fois dans une ligne de commande pour spécifier d'autres emplacements de téléchargement.

Exemple : **ccmsetup.exe /source:"\\ordinateur\dossier"**

**/mp:<serveur>**

Spécifie un point de gestion source auquel les ordinateurs se connectent. Les ordinateurs utilisent ce point de gestion pour trouver le point de distribution le plus proche pour les fichiers d'installation. En l'absence de point de distribution ou si les ordinateurs ne peuvent pas télécharger les fichiers auprès des points de distribution au terme d'un délai de quatre heures, ils téléchargent les fichiers auprès du point de gestion spécifié.

> **IMPORTANT**
> Ce paramètre permet de spécifier un point de gestion initial utilisé par les ordinateurs qui recherchent une source de téléchargement. Il peut s'agir de n'importe quel point de gestion sur n'importe quel site. Elle *n'affecte pas* le client à un point de gestion.

Les ordinateurs téléchargent les fichiers via une connexion HTTP ou HTTPS, selon la configuration du rôle de système de site des connexions client. Si cette fonctionnalité est configurée, le téléchargement utilise la limitation BITS. Si tous les points de distribution et de gestion sont configurés seulement pour les connexions client HTTPS, vérifiez que l'ordinateur client a un certificat client valide.

Vous pouvez utiliser le paramètre de ligne de commande **/mp** pour spécifier plusieurs points de gestion. Si l'ordinateur ne parvient pas à se connecter au premier, il essaie le suivant dans la liste spécifiée. Quand vous spécifiez plusieurs points de gestion, séparez les valeurs par des points-virgules.

Si le client se connecte à un point de gestion via HTTPS, vous devez en général spécifier le nom de domaine complet, et non le nom de l'ordinateur. La valeur doit correspondre au nom d'objet ou à l'autre nom d'objet du certificat PKI du point de gestion. Même si Configuration Manager permet d'utiliser un nom d'ordinateur dans le certificat pour les connexions intranet, il est recommandé d'utiliser un nom de domaine complet.

Exemple utilisant le nom d'ordinateur : `ccmsetup.exe /mp:SMSMP01`

Exemple utilisant le nom de domaine complet : `ccmsetup.exe /mp:smsmp01.contoso.com`

Ce paramètre peut spécifier l'URL d'une passerelle de gestion cloud. Utilisez cette URL pour installer le client sur un appareil Internet. Pour obtenir la valeur de ce paramètre, suivez les étapes ci-dessous :

- Créez une passerelle de gestion cloud.
- Sur un client actif, ouvrez une invite de commandes Windows PowerShell en tant qu'administrateur.
- Exécutez la commande suivante :
  ```
  (Get-WmiObject -Namespace Root\Ccm\LocationServices -Class SMS_ActiveMPCandidate | Where-Object {$_.Type -eq "Internet"}).MP
  ```
- Ajoutez le préfixe « https:// » à utiliser avec le paramètre **/mp**.

Exemple pour l'utilisation de l'URL de la passerelle de gestion cloud :
`ccmsetup.exe /mp:https://CONTOSO.CLOUDAPP.NET/CCM_Proxy_MutualAuth/72057598037248100`

> **IMPORTANT**
> Si elle est spécifiée, l'URL de la passerelle de gestion cloud pour le paramètre **/mp** doit commencer par **https://**.

**/retry:<Minutes>**

Intervalle entre les tentatives si CCMSetup.exe ne réussit pas à télécharger les fichiers d'installation. CCMSetup renouvelle les tentatives jusqu'à atteindre la limite indiquée dans le paramètre **downloadtimeout**.

Exemple : `ccmsetup.exe /retry:20`

**/noservice**

Empêche l'exécution de CCMSetup comme service (comportement par défaut). Quand CCMSetup est exécuté en tant que service, il s'exécute dans le contexte du compte système local de l'ordinateur. Ce compte peut ne pas disposer des droits suffisants pour accéder aux ressources réseau nécessaires à l'installation. Avec **/noservice**, CCMSetup.exe s'exécute dans le contexte du compte d'utilisateur que vous utilisez pour démarrer l'installation. Par ailleurs, si vous utilisez un script pour exécuter CCMSetup.exe avec le paramètre

**/service**, CCMSetup.exe s'arrête après démarrage du service et risque de ne pas retourner correctement les détails de l'installation.

Exemple : `ccmsetup.exe /noservice`

**/service**

Indique que CCMSetup doit s'exécuter comme un service qui utilise le compte système local.

Exemple : `ccmsetup.exe /service`

**/uninstall**

Indique que le logiciel client doit être désinstallé. Pour plus d'informations, consultez Guide pratique pour gérer des clients.

Exemple : `ccmsetup.exe /uninstall`

**/logon**

Ce paramètre spécifie que l'installation doit s'arrêter si une version du client est déjà installée.

Exemple : `ccmsetup.exe /logon`

**/forcereboot**

Indique que CCMSetup doit forcer l'ordinateur client à redémarrer si nécessaire pour terminer l'installation. Si ce paramètre n'est pas spécifié, CCMSetup s'arrête quand un redémarrage est nécessaire. Il continue après le redémarrage manuel suivant.

Exemple : `CCMSetup.exe /forcereboot`

**/BITSPriority:<Priorité>**

Indique la priorité de téléchargement lorsque les fichiers d'installation du client sont téléchargés via une connexion HTTP. Les valeurs possibles sont les suivantes :

- FOREGROUND (avant-plan)
- HIGH (élevée)
- NORMAL (normale)
- LOW (faible)

  La valeur par défaut est NORMAL.

  Exemple : `ccmsetup.exe /BITSPriority:HIGH`

**/downloadtimeout:<Minutes>**

Durée (en minutes) pendant laquelle CCMSetup essaie de télécharger les fichiers d'installation avant d'arrêter. La valeur par défaut est de **1440** minutes (un jour).

Exemple : `ccmsetup.exe /downloadtimeout:100`

**/UsePKICert**

Quand cette propriété est spécifiée, le client utilise un certificat PKI qui inclut l'authentification du client, le cas échéant. Si le client ne peut pas trouver un certificat valide, il utilise une connexion HTTP avec un certificat auto-signé. Ce comportement est le même si ce paramètre n'est pas utilisé.

> **NOTE**
> Dans certains cas, il n'est pas nécessaire de spécifier ce paramètre lors de l'installation d'un client ; vous utilisez alors néanmoins un certificat client. C'est le cas, notamment, de l'installation d'un client via une installation Push et de l'installation d'un client basée sur un point de mise à jour logicielle. Toutefois, vous devrez spécifier ce paramètre à chaque fois que vous installerez un client manuellement et utiliser le paramètre **/mp** pour indiquer un point de gestion configuré pour accepter uniquement les connexions client HTTPS. Il est aussi nécessaire de préciser ce paramètre pour installer un client à des fins de communication Internet uniquement. Utilisez la propriété CCMALWAYSINF=1 conjointement avec les propriétés correspondant au point de gestion Internet (CCMHOSTNAME) et le code de site (SMSSITECODE). Pour plus d'informations sur la gestion des clients Internet, consultez Éléments à prendre en considération pour les communications de clients à partir d'Internet ou d'une forêt non approuvée.

Exemple : `CCMSetup.exe /UsePKICert`

**/NoCRLCheck**

Spécifie qu'un client ne doit pas vérifier la liste de révocation de certificats (CRL) quand il communique via HTTPS avec un certificat PKI.

Quand cette propriété n'est pas spécifiée, le client vérifie la liste de révocation de certificats avant d'établir une connexion HTTPS.

Pour plus d'informations sur la vérification de la liste de révocation de certificats par le client, consultez Planification de la révocation de certificats PKI.

Exemple : `CCMSetup.exe /UsePKICert /NoCRLCheck`

**/config:<fichier_configuration>**

Spécifie le nom d'un fichier texte qui répertorie les propriétés d'installation du client.

- Si vous ne spécifiez pas le paramètre **/noservice** de CCMSetup, ce fichier doit se trouver dans le dossier CCMSetup, c'est-à-dire %Windir%\Ccmsetup pour les systèmes d'exploitation 32 bits et 64 bits.
- Si le paramètre **/noservice** est précisé, ce fichier doit se trouver dans le dossier à partir duquel vous exécutez CCMSetup.exe.

Exemple : `CCMSetup.exe /config:<Configuration File Name.txt\>`

Pour fournir le format de fichier correct, utilisez le fichier mobileclienttemplate.tcf qui se trouve dans le répertoire <Configuration Manager>\bin\<plateforme> sur le serveur de site . Ce fichier contient également des commentaires sur les sections et leur utilisation. Spécifiez les propriétés d'installation du client dans la section [Client Install], à la suite du texte ci-après : **Install=INSTALL=ALL**.

Exemple d'entrée de section [Client Install] : `Install=INSTALL=ALL SMSSITECODE=ABC SMSCACHESIZE=100`

**/skipprereq:<nom_fichier>**

Spécifie que CCMSetup.exe ne doit pas installer le programme prérequis spécifié lors de l'installation du client Configuration Manager. Ce paramètre accepte plusieurs valeurs. Pour séparer chaque valeur, utilisez le point-virgule (;).

Exemples : `CCMSetup.exe /skipprereq:dotnetfx40_client_x86_x64.exe` ou
`CCMSetup.exe /skipprereq:dotnetfx40_client_x86_x64.exe;windowsupdateagent30_x86.exe`

**/forceinstall**

Spécifiez que CCMSetup.exe désinstalle le client existant et installe un nouveau client.

**/ExcludeFeatures:<fonctionnalité>**

Spécifie que CCMSetup.exe n'installe pas la fonctionnalité spécifiée lors de l'installation du client.

Exemple : `CCMSetup.exe /ExcludeFeatures:ClientUI` n'installe pas le Centre logiciel sur le client.

> **NOTE**
> **ClientUI** est la seule valeur prise en charge avec le paramètre **/ExcludeFeatures**.

## Codes de retour de CCMSetup.exe

La commande CCMSetup.exe fournit les codes de retour suivants à la fin de son exécution. Pour résoudre les problèmes, examinez le fichier ccmsetup.log sur l'ordinateur client pour déterminer le contexte et obtenir des détails supplémentaires sur les codes de retour.

| CODE DE RETOUR | SIGNIFICATION |
|---|---|
| 0 | Opération réussie |
| 6 | Erreur |
| 7 | Redémarrage obligatoire |
| 8 | Programme d'installation déjà en cours d'exécution |
| 9 | Échec d'évaluation de condition préalable |
| 10 | Échec de validation de hachage de manifeste de configuration |

## Propriétés de Ccmsetup.msi

Les propriétés suivantes peuvent modifier le comportement à l'installation de ccmsetup.msi.

### CCMSETUPCMD

Spécifie des propriétés et des paramètres de ligne de commande qui sont transmis à ccmsetup.exe après son installation par ccmsetup.msi. Placez les autres propriétés entre guillemets. Utilisez cette propriété lors de l'amorçage du client Configuration Manager à l'aide de la méthode d'installation d'Intune MDM.

Exemple : `ccmsetup.msi CCMSETUPCMD="/mp:https://mp.contoso.com CCMHOSTNAME=mp.contoso.com"`

> **TIP**
> Microsoft Intune limite la ligne de commande à 1 024 caractères.

## Propriétés de Client.msi

Les propriétés suivantes peuvent modifier le comportement d'installation de client.msi. Si vous utilisez la méthode d'installation push du client, vous pouvez également spécifier les propriétés sous l'onglet **Client** de la boîte de dialogue **Propriétés de l'installation push du client** .

### AADCLIENTAPPID

Spécifie l'identificateur d'application cliente Azure Active Directory (Azure AD). L'application cliente est créée ou importée quand vous configurez des services Azure pour la gestion cloud. Un administrateur Azure peut obtenir la valeur de cette propriété auprès du portail Azure. Pour plus d'informations, consultez Obtenir l'ID de l'application. Pour la propriété **AADCLIENTAPPID**, cet ID d'application concerne le type

d'application « Native ».

Exemple : `ccmsetup.exe AADCLIENTAPPID=aa28e7f1-b88a-43cd-a2e3-f88b257c863b`

### AADRESOURCEURI

Spécifie l'identificateur d'application serveur Azure AD. L'application serveur est créée ou importée quand vous configurez des services Azure pour la gestion cloud. Lors de la création de l'application serveur, dans la boîte de dialogue Créer une application serveur, cette propriété est **l'URI ID d'application**.

Un administrateur Azure peut obtenir la valeur de cette propriété auprès du portail Azure. Dans le panneau **Azure Active Directory**, recherchez l'application serveur sous **Inscriptions des applications**. Cette application est du type « Application/API web ». Ouvrez l'application, cliquez sur **Paramètres**, puis sur **Propriétés**. Utilisez la valeur de **URI ID d'application** pour cette propriété d'installation du client AADRESOURCEURI.

Exemple : `ccmsetup.exe AADRESOURCEURI=https://contososerver`

### AADTENANTID

Spécifie l'identificateur du locataire Azure AD. Ce client est lié à Configuration Manager quand vous configurez des services Azure pour la gestion cloud. Pour obtenir la valeur de cette propriété, utilisez les étapes suivantes :

- Sur un appareil Windows 10 qui est joint au même locataire Azure AD, ouvrez une invite de commandes.
- Exécutez la commande suivante : `dsregcmd.exe /status`
- Dans la section État de l'appareil, recherchez la valeur de **TenantId**. Par exemple, `TenantId : 607b7853-6f6f-4d5d-b3d4-811c33fdd49a`

  > **NOTE**
  > Un administrateur Azure peut également obtenir cette valeur dans le portail Azure. Pour plus d'informations, consultez Obtenir l'ID de locataire.

Exemple : `ccmsetup.exe AADTENANTID=607b7853-6f6f-4d5d-b3d4-811c33fdd49a`

### CCMADMINS

Indique un ou plusieurs groupes ou comptes d'utilisateurs Windows auxquels accorder l'accès aux paramètres et stratégies du client. Cette propriété est utile si l'administrateur de Configuration Manager ne dispose pas d'informations d'identification d'administration locale sur l'ordinateur client. Indiquez une liste de comptes séparés par des points-virgules.

Exemple : `CCMSetup.exe CCMADMINS="Domain\Account1;Domain\Group1"`

### CCMALLOWSILENTREBOOT

Spécifie que l'ordinateur est autorisé à redémarrer si nécessaire après l'installation du client.

> **IMPORTANT**
> L'ordinateur redémarre sans avertissement, même si un utilisateur y est connecté.

Exemple : **CCMSetup.exe CCMALLOWSILENTREBOOT**

### CCMALWAYSINF

Définissez sa valeur sur **1** pour spécifier que le client est toujours un client Internet et ne se connecte jamais à l'intranet. Le type de connexion du client affiche **Toujours Internet**.

Utilisez cette propriété en combinaison avec CCMHOSTNAME, qui spécifie le nom de domaine complet du point de gestion Internet. Utilisez-la également avec le paramètre /UsePKICert de CCMSetup et avec le code de site.

Pour plus d'informations sur la gestion des clients Internet, consultez Éléments à prendre en considération pour les communications de clients à partir d'Internet ou d'une forêt non approuvée.

Exemple : `CCMSetup.exe /UsePKICert CCMALWAYSINF=1 CCMHOSTNAME=SERVER3.CONTOSO.COM SMSSITECODE=ABC`

### CCMCERTISSUERS

Spécifie la liste des émetteurs de certificats, qui est une liste de certificats issus d'autorités de certification racines de confiance que le site Configuration Manager a approuvées.

Pour plus d'informations sur la liste des émetteurs de certificats et sur la façon dont les clients l'utilisent lors du processus de sélection de certificat, consultez Planification de la sélection des certificats client PKI.

Cette valeur est une correspondance qui respecte la casse pour les attributs d'objet qui se trouvent dans le certificat d'autorité de certification racine. Les attributs peuvent être séparés par une virgule (,) ou un point-virgule (;). Spécifiez plusieurs certificats d'autorité de certification racine en utilisant une barre de séparation. Exemple :

```
CCMCERTISSUERS=”CN=Contoso Root CA; OU=Servers; O=Contoso, Ltd; C=US &#124; CN=Litware Corporate Root CA; O=Litware, Inc.”
```

> **TIP**
>
> Pour copier **CertificateIssuers=<chaîne>** pour le site, référencez le fichier mobileclient.tcf dans le dossier du <répertoire Configuration Manager>\bin\<plateforme> sur le serveur de site.

### CCMCERTSEL

Spécifie les critères de sélection des certificats si le client a plusieurs certificats pour la communication HTTPS. Ce certificat est un certificat valide incluant les fonctionnalités d'authentification du client.

Vous pouvez rechercher une correspondance exacte (utilisez **Subject:**) ou une correspondance partielle (utilisez **SubjectStr:)** dans le nom d'objet ou l'autre nom de l'objet. Exemples :

`CCMCERTSEL="Subject:computer1.contoso.com"` recherche un certificat avec une correspondance exacte au nom d'ordinateur « computer1,contoso.com » dans le nom d'objet ou l'autre nom de l'objet.

`CCMCERTSEL="SubjectStr:contoso.com"` recherche un certificat contenant « contoso.com » dans le nom d'objet ou l'autre nom de l'objet.

Vous pouvez également utiliser un identificateur d'objet (OID) ou des attributs de nom unique dans les attributs du nom d'objet ou de l'autre nom de l'objet, par exemple :

`CCMCERTSEL="SubjectAttr:2.5.4.11 = Computers"` recherche l'attribut d'unité organisationnelle exprimé comme identificateur d'objet et nommé Computers.

`CCMCERTSEL="SubjectAttr:OU = Computers"` recherche l'attribut d'unité organisationnelle exprimé comme nom unique et nommé Computers.

> **IMPORTANT**
>
> Si vous utilisez la zone Nom d'objet, **Subject:** respecte la casse, mais **SubjectStr:** ne la respecte pas.
>
> Si vous utilisez la zone Autre nom de l'objet, **Subject:** et **SubjectStr:** respectent la casse tous les deux.

La liste complète des attributs que vous pouvez utiliser pour la sélection de certificat figure dans Valeurs d'attribut prises en charge pour les critères de sélection de certificat PKI.

Si plusieurs certificats correspondent à la recherche et si la propriété que CCMFIRSTCERT a été définie sur 1, le certificat dont la période de validité est la plus longue est sélectionné.

### CCMCERTSTORE

Spécifie un autre nom de magasin de certificats si le certificat client pour HTTPS ne se trouve pas dans le magasin de certificats par défaut de **Personnel** du magasin Ordinateur.

Exemple : `CCMSetup.exe /UsePKICert CCMCERTSTORE="ConfigMgr"`

### CCMDEBUGLOGGING

Active l'enregistrement du débogage dans le journal (journalisation). Les valeurs peuvent être définies sur 0 (désactivée, par défaut) ou sur 1 (activée). Cette propriété fait que le client enregistre dans le journal des informations détaillées pour le dépannage. Au titre de bonne pratique, évitez d'utiliser cette propriété dans les sites en production. Cela peut aboutir à une journalisation excessive, ce qui peut rendre difficile la recherche des informations pertinentes dans les fichiers journaux. Définissez aussi CCMENABLELOGGING sur TRUE pour activer la journalisation du débogage.

Exemple : `CCMSetup.exe CCMDEBUGLOGGING=1`

### CCMENABLELOGGING

Par défaut, cette propriété est définie sur TRUE pour activer la journalisation. Les fichiers journaux sont stockés dans le dossier **Logs** du dossier d'installation du client Configuration Manager. Par défaut, ce dossier est %Windir%\CCM\Logs.

Exemple : `CCMSetup.exe CCMENABLELOGGING=TRUE`

### CCMEVALINTERVAL

Fréquence d'exécution de l'outil d'évaluation de l'intégrité du client (ccmeval.exe). La valeur peut être comprise entre **1** et **1440** minutes. Par défaut, il est exécuté une fois par jour.

### CCMEVALHOUR

Heure d'exécution de l'outil d'évaluation de l'intégrité du client (ccmeval.exe), entre **0** (minuit) et **23** (23 h). S'exécute à minuit par défaut.

### CCMFIRSTCERT

Si la valeur est définie sur 1, cette propriété spécifie que le client doit sélectionner le certificat PKI dont la période de validité est la plus longue. Ce paramètre peut être nécessaire si vous utilisez la protection d'accès réseau avec application d'IPsec.

Exemple : `CCMSetup.exe /UsePKICert CCMFIRSTCERT=1`

### CCMHOSTNAME

Si le client est géré sur Internet, cette propriété spécifie le nom de domaine complet du point de gestion Internet.

Ne spécifiez pas cette option avec la propriété d'installation SMSSITECODE=AUTO. Les clients Internet doivent être affectés directement à leur site Internet.

Exemple : `CCMSetup.exe /UsePKICert CCMHOSTNAME="SMSMP01.corp.contoso.com"`

Cette propriété peut spécifier l'adresse d'une passerelle de gestion cloud. Pour obtenir la valeur de cette propriété, utilisez les étapes suivantes :

- Créez une passerelle de gestion cloud.

- Sur un client actif, ouvrez une invite de commandes Windows PowerShell en tant qu'administrateur.
- Exécutez la commande suivante :
  ```
  (Get-WmiObject -Namespace Root\Ccm\LocationServices -Class SMS_ActiveMPCandidate | Where-Object {$_.Type -eq "Internet"}).MP
  ```
- Utilisez la valeur retournée telle quelle avec la propriété **CCMHOSTNAME**.

Exemple : `ccmsetup.exe CCMHOSTNAME=CONTOSO.CLOUDAPP.NET/CCM_Proxy_MutualAuth/72057598037248100`

> **IMPORTANT**
> Quand vous spécifiez l'adresse d'une passerelle de gestion cloud pour la propriété **CCMHOSTNAME**, n'ajoutez *pas* un préfixe comme **https://**. Ce préfixe est utilisé seulement avec l'URL **/mp** d'une passerelle de gestion cloud.

### CCMHTTPPORT

Indique le port que le client doit utiliser lors de la communication sur HTTP avec des serveurs de système de site. Le port 80 est le port par défaut.

Exemple : `CCMSetup.exe CCMHTTPPORT=80`

### CCMHTTPSPORT

Indique le port que le client doit utiliser lors de la communication sur HTTPS avec des serveurs de système de site. Le port 443 est le port par défaut.

Exemple : `CCMSetup.exe /UsePKICert CCMHTTPSPORT=443`

### CCMINSTALLDIR

Indique le dossier dans lequel les fichiers du client Configuration Manager sont installés, *%Windir%* \CCM par défaut. Quel que soit l'emplacement d'installation de ces fichiers, le fichier Ccmcore.dll est toujours installé dans le dossier *%Windir%\System32*. En outre, sur un système d'exploitation 64 bits, une copie du fichier Ccmcore.dll est toujours installée dans le dossier *%Windir%* \SysWOW64. Ce fichier prend en charge les applications 32 bits qui utilisent la version 32 bits des API client du SDK Configuration Manager.

Exemple : `CCMSetup.exe CCMINSTALLDIR="C:\ConfigMgr"`

### CCMLOGLEVEL

Indique le niveau de détails à écrire dans les fichiers journaux de Configuration Manager. Spécifiez un entier entre 0 et 3, où 0 représente la journalisation la plus complète et où 3 ne consigne que les erreurs. La valeur par défaut est 1.

Exemple : `CCMSetup.exe CCMLOGLEVEL=3`

### CCMLOGMAXHISTORY

Quand un fichier journal de Configuration Manager atteint la taille maximale, le client le renomme en tant que sauvegarde et crée un nouveau fichier journal. La taille maximale est de 250 000 octets par défaut ou celle de la valeur spécifiée par la propriété CCMLOGMAXSIZE.

Cette propriété spécifie combien de versions précédentes du fichier journal doivent être conservées. La valeur par défaut est 1. Si la valeur est définie sur 0, aucun ancien fichier journal n'est conservé.

Exemple : `CCMSetup.exe CCMLOGMAXHISTORY=0`

### CCMLOGMAXSIZE

Taille maximale du fichier journal, en octets. Quand un journal atteint la taille spécifiée, le client le renomme en tant que fichier d'historique et crée un nouveau fichier. Cette propriété doit être définie sur au moins 10 000 octets. La valeur par défaut est de 250 000 octets.

Exemple : `CCMSetup.exe CCMLOGMAXSIZE=300000`

### DISABLESITEOPT

Si elle est définie sur TRUE, cette propriété désactive la possibilité pour les utilisateurs administratifs de changer le site affecté dans le panneau de configuration de **Configuration Manager**.

Exemple : **CCMSetup.exe DISABLESITEOPT=TRUE**

### DISABLECACHEOPT

Si elle est définie sur TRUE, cette propriété désactive la possibilité pour les utilisateurs administratifs de changer les paramètres du dossier du cache client dans le panneau de configuration de **Configuration Manager**.

Exemple : `CCMSetup.exe DISABLECACHEOPT=TRUE`

### DNSSUFFIX

Spécifie un domaine DNS pour que les clients localisent les points de gestion qui sont publiés dans DNS. Lorsqu'un point de gestion est localisé, il indique au client d'autres points de gestion dans la hiérarchie. Ce comportement signifie qu'il n'est pas nécessaire que le point de gestion localisé à l'aide de la publication DNS provienne du site du client, mais qu'il peut s'agir de n'importe quel point de gestion de la hiérarchie.

> **NOTE**
> Vous ne devez pas spécifier cette propriété si le client se trouve dans le même domaine qu'un point de gestion publié. Dans ce cas, le domaine du client est automatiquement utilisé pour rechercher des points de gestion dans DNS.

Pour plus d'informations sur la publication DNS comme méthode de localisation de services pour les clients Configuration Manager, consultez Emplacement du service et façon dont les clients déterminent leur point de gestion attribué.

> **NOTE**
> Par défaut, la publication DNS n'est pas activée dans Configuration Manager.

Exemple : `CCMSetup.exe SMSSITECODE=ABC DNSSUFFIX=contoso.com`

### FSP

Indique le point d'état de secours qui reçoit et traite les messages d'état envoyés par les ordinateurs clients Configuration Manager.

Pour plus d'informations sur le point d'état de secours, consultez Déterminer si vous avez besoin d'un point d'état de secours.

Exemple : `CCMSetup.exe FSP=SMSFP01`

### IGNOREAPPVVERSIONCHECK

Spécifie que la présence de la version minimale requise de Microsoft Application Virtualization (App-V) n'est pas vérifiée avant l'installation du client.

> **IMPORTANT**
> Si vous installez le client Configuration Manager sans installer App-V, vous ne pouvez pas déployer des applications virtuelles.

Exemple : `CCMSetup.exe IGNOREAPPVVERSIONCHECK=TRUE`

### NOTIFYONLY

Spécifie que le client signale l'état, mais ne corrige pas les problèmes qu'il trouve.

Exemple : `CCMSetup.exe NOTIFYONLY=TRUE`

Pour plus d'informations, consultez Guide pratique pour configurer l'état du client.

### RESETKEYINFORMATION

Si un client a la mauvaise clé racine approuvée de Configuration Manager et ne peut pas contacter de point de gestion approuvé pour recevoir la nouvelle clé racine approuvée, utilisez cette propriété pour supprimer manuellement l'ancienne clé racine approuvée. Cette situation peut se produire quand vous déplacez un client d'une hiérarchie de site à une autre. Cette propriété s'applique aux clients qui utilisent la communication client HTTP et HTTPS.

Exemple : `CCMSetup.exe RESETKEYINFORMATION=TRUE`

### SITEREASSIGN

Permet la réattribution de site automatique pour les mises à niveau du client si cette propriété est utilisée avec SMSSITECODE=AUTO.

Exemple : `CCMSetup.exe SMSSITECODE=AUTO SITEREASSIGN=TRUE`

### SMSCACHEDIR

Spécifie l'emplacement du dossier de cache du client sur l'ordinateur client, qui stocke les fichiers temporaires. Par défaut, l'emplacement est *%Windir\ccmcache*.

Exemple : `CCMSetup.exe SMSCACHEDIR="C:\Temp"`

Cette propriété peut être utilisée avec la propriété SMSCACHEFLAGS pour contrôler l'emplacement du dossier du cache du client.

Exemple : `CCMSetup.exe SMSCACHEDIR=Cache SMSCACHEFLAGS=MAXDRIVE` installe le dossier du cache du client sur le lecteur de disque disponible le plus grand du client.

### SMSCACHEFLAGS

Spécifie davantage les détails d'installation pour le dossier mis dans la mémoire cache du client. Vous pouvez utiliser les propriétés de SMSCACHEFLAGS individuellement ou en combinaison, séparées par des points-virgules. Si cette propriété n'est pas spécifiée, le dossier du cache client est installé en fonction de la propriété SMSCACHEDIR, il n'est pas compressé et la valeur de SMSCACHESIZE est utilisée pour sa taille en Mo.

Ce paramètre est ignoré lorsque vous mettez à niveau un client existant.

Propriétés :

- PERCENTDISKSPACE : indique la taille du dossier sous forme de pourcentage de l'espace disque total. Si vous indiquez cette propriété, vous devez également indiquer la propriété SMSCACHESIZE comme valeur de pourcentage à utiliser.
- PERCENTFREEDISKSPACE : indique la taille du dossier sous forme de pourcentage de l'espace disque disponible. Si vous indiquez cette propriété, vous devez également indiquer la propriété SMSCACHESIZE comme valeur de pourcentage à utiliser. Par exemple, si le disque dispose de 10 Mo libres et que SMSCACHESIZE indique 50, cela signifie que la taille du dossier est définie sur 5 Mo. Vous ne pouvez pas utiliser cette propriété avec la propriété PERCENTDISKSPACE.
- MAXDRIVE : indique que le dossier doit être installé sur le disque le plus volumineux disponible.

Cette valeur est ignorée si un chemin a été spécifié avec la propriété SMSCACHEDIR.

- MAXDRIVESPACE : indique que le dossier doit être installé sur le lecteur de disque possédant l'espace disponible le plus important. Cette valeur est ignorée si un chemin a été spécifié avec la propriété SMSCACHEDIR.
- NTFSONLY : indique que le dossier peut être installé uniquement sur des lecteurs de disque NTFS. Cette valeur est ignorée si un chemin a été spécifié avec la propriété SMSCACHEDIR.
- COMPRESS : spécifie que le dossier doit être conservé sous une forme compressée.
- FAILIFNOSPACE : indique que le logiciel client doit être supprimé si l'espace est insuffisant pour installer le dossier.

Exemple : `CCMSetup.exe SMSCACHEFLAGS=NTFSONLY;COMPRESS`

### SMSCACHESIZE

> **IMPORTANT**
> Des paramètres client sont disponibles pour spécifier la taille du dossier du cache client. L'ajout de ces paramètres du client remplace l'utilisation de SMSCACHESIZE comme propriété client.msi pour spécifier la taille du cache du client. Pour plus d'informations, consultez les paramètres du client pour la taille du cache.

> **NOTE**
> Si un nouveau package qui doit être téléchargé peut provoquer le dépassement de la taille maximale du dossier et que le dossier ne peut pas être vidé pour libérer un espace suffisant, le téléchargement du package échoue, et le programme ou l'application ne s'exécute pas.

Ce paramètre est ignoré quand vous mettez à niveau un client existant et quand le client télécharge des mises à jour logicielles.

Exemple : `CCMSetup.exe SMSCACHESIZE=100`

> **NOTE**
> Si vous réinstallez un client, vous ne pouvez pas utiliser les propriétés d'installation SMSCACHESIZE ou SMSCACHEFLAGS pour définir une taille de cache inférieure à la taille antérieure. Si vous essayez d'effectuer cette action, votre valeur est ignorée. La taille du cache est automatiquement définie à la taille antérieure.

### SMSCONFIGSOURCE

Indique l'emplacement et l'ordre dans lesquels le programme d'installation de Configuration Manager vérifie les paramètres de configuration. La propriété est une chaîne d'un ou plusieurs caractères, chacun définissant une source de configuration spécifique. Utilisez les caractères R, P, M et U seuls ou en combinaison :

- R : vérification des paramètres de configuration dans le Registre.

  Pour plus d'informations, consultez Informations sur le stockage des propriétés d'installation du client dans le Registre.

- P : vérification des paramètres de configuration dans les propriétés d'installation fournies à l'invite de commandes.
- M : vérification des paramètres existants à l'occasion de la mise à niveau d'un ancien client avec le

logiciel client Configuration Manager.

- U : mise à niveau du client installé vers une version plus récente (et utilisation du code de site attribué).

  Par défaut, l'installation du client utilise `PU` pour vérifier d'abord les propriétés d'installation, puis les paramètres existants.

  Exemple : `CCMSetup.exe SMSCONFIGSOURCE=RP`

### SMSDIRECTORYLOOKUP

Indique si le client peut utiliser les services WINS (Windows Internet Name Service) pour trouver un point de gestion qui accepte les connexions HTTP. Les clients utilisent cette méthode quand ils ne peuvent pas trouver de point de gestion dans les services de domaine Active Directory ou dans DNS.

Cette propriété n'a pas d'impact sur le fait que le client utilise ou non WINS pour la résolution de noms.

Vous pouvez configurer deux modes différents pour cette propriété :

- NOWINS : cette valeur est le paramètre le plus sûr pour cette propriété et empêche les clients de rechercher un point de gestion dans WINS. Lorsque vous utilisez ce paramètre, les clients doivent disposer d'une autre méthode de localisation d'un point de gestion sur l'Intranet, telle que les services de domaine Active Directory ou en utilisant la publication DNS.
- WINSSECURE (valeur par défaut) : dans ce mode, un client qui utilise la communication HTTP peut utiliser WINS pour trouver un point de gestion. Toutefois, le client doit disposer d'une copie de la clé racine approuvée avant de pouvoir se connecter correctement au point de gestion. Pour plus d'informations, voir Planification de la clé racine approuvée.

Exemple : `CCMSetup.exe SMSDIRECTORYLOOKUP=NOWINS`

### SMSMP

Spécifie un point de gestion initial à utiliser par le client Configuration Manager.

> **IMPORTANT**
> Si le point de gestion accepte uniquement les connexions clientes sur HTTPS, vous devez ajouter le préfixe https:// au nom du point de gestion.

Exemple : `CCMSetup.exe SMSMP=smsmp01.contoso.com`

Exemple : `CCMSetup.exe SMSMP=https://smsmp01.contoso.com`

### SMSPUBLICROOTKEY

Indique la clé racine approuvée de Configuration Manager lorsque celle-ci ne peut pas être récupérée à partir des services de domaine Active Directory. Cette propriété s'applique aux clients qui utilisent la communication client HTTP et HTTPS. Pour plus d'informations, voir Planification de la clé racine approuvée.

Exemple : `CCMSetup.exe SMSPUBLICROOTKEY=<key\>`

### SMSROOTKEYPATH

Utilisée pour réinstaller la clé racine approuvée de Configuration Manager. Indique le chemin d'accès complet et le nom de fichier d'un fichier contenant la clé racine approuvée. Cette propriété s'applique aux clients qui utilisent la communication client HTTP et HTTPS. Pour plus d'informations, voir Planification de la clé racine approuvée.

Exemple : 'CCMSetup.exe SMSROOTKEYPATH=<chemin_complet_et_nom_de_fichier>`

**SMSSIGNCERT**

Spécifie le chemin d'accès complet et le nom de fichier .cer du certificat auto-signé exporté sur le serveur de site.

Ce certificat est stocké dans le magasin de certificats **SMS** et porte le nom d'objet **Serveur de site** et le nom convivial **Certificat de signature du serveur de site**.

Exemple : **CCMSetup.exe /UsePKICert SMSSIGNCERT=<chemin _complet_et_nom_de_fichier>**

**SMSSITECODE**

Spécifie le site Configuration Manager auquel affecter le client. Cette valeur peut être un code de site à trois caractères ou le mot AUTO. Si vous spécifiez AUTO ou si vous ne spécifiez pas cette propriété, le client tente de déterminer l'affectation de son site à partir des services de domaine Active Directory ou d'un point de gestion spécifié. Pour activer AUTO pour les mises à niveau du client, vous devez également affecter à SITEREASSIGN la valeur TRUE.

> **NOTE**
> N'utilisez pas AUTO si vous spécifiez également le point de gestion Internet (CCMHOSTNAME). Dans ce cas, vous devez directement attribuer le client à son site.

Exemple : `CCMSetup.exe SMSSITECODE=XZY`

## Valeurs d'attribut prises en charge pour les critères de sélection de certificat PKI

Configuration Manager prend en charge les valeurs d'attribut suivantes pour les critères de sélection de certificat PKI :

| ATTRIBUT D'OID | ATTRIBUT DE NOM UNIQUE | DÉFINITION DE L'ATTRIBUT |
|---|---|---|
| 0.9.2342.19200300.100.1.25 | DC | Composant de domaine |
| 1.2.840.113549.1.9.1 | E ou E-mail | Adresse de messagerie |
| 2.5.4.3 | CN | Nom commun |
| 2.5.4.4 | SN | Nom d'objet |
| 2.5.4.5 | SERIALNUMBER | Numéro de série |
| 2.5.4.6 | C | Code du pays |
| 2.5.4.7 | L | Localité |
| 2.5.4.8 | S ou ST | Nom de département/province |
| 2.5.4.9 | STREET | Adresse |
| 2.5.4.10 | O | Nom de l'organisation |

| ATTRIBUT D'OID | ATTRIBUT DE NOM UNIQUE | DÉFINITION DE L'ATTRIBUT |
|---|---|---|
| 2.5.4.11 | OU | Unité d'organisation |
| 2.5.4.12 | T ou Title | Titre |
| 2.5.4.42 | G ou GN ou GivenName | Prénom |
| 2.5.4.43 | I ou Initials | Initiales |
| 2.5.29.17 | (aucune valeur) | Autre nom de l'objet |

# À propos de la publication des propriétés d'installation du client sur les services de domaine Active Directory

22/06/2018 • 9 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Quand vous étendez le schéma Active Directory pour System Center Configuration Manager et que le site est publié dans les services de domaine Active Directory, de nombreuses propriétés d'installation du client sont publiées dans les services de domaine Active Directory. Si un ordinateur peut localiser ces propriétés d'installation du client, il peut les utiliser au cours du déploiement du client Configuration Manager.

Les avantages de l'utilisation des services de domaine Active Directory pour publier les propriétés d'installation du client sont les suivants :

- Les installations du client basées sur des points de mise à jour logicielle et sur une stratégie de groupe ne nécessitent pas la configuration de paramètres d'installation sur chaque ordinateur.
- Ces informations étant générées automatiquement, le risque d'erreur humaine propre à la saisie manuelle des propriétés d'installation est éliminé.

> **NOTE**
> Pour plus d'informations sur la façon d'étendre le schéma Active Directory pour Configuration Manager et de publier un site, consultez Extensions de schéma pour System Center Configuration Manager.

## Propriétés d'installation du client publiées dans les services de domaine Active Directory

Voici une liste de propriétés d'installation du client. Pour plus d'informations sur chaque élément répertorié ci-dessous, consultez À propos des propriétés d'installation du client dans System Center Configuration Manager.

- Code de site Configuration Manager.
- Certificat de signature du serveur de site.
- Clé racine approuvée.
- Ports de communication client pour HTTP et HTTPS.
- Point d'état de secours. Si le site a plusieurs points d'état de secours, seul le premier qui a été installé est publié dans les services de domaine Active Directory.
- Un paramètre pour indiquer que le client doit communiquer à l'aide de HTTPS uniquement.
- Paramètres relatifs aux certificats PKI :
  - Si vous souhaitez utiliser un certificat PKI du client.
  - Critères de sélection des certificats. Ceci peut être nécessaire dans le cas où le client a plusieurs certificats PKI valides qui peuvent être utilisés pour Configuration Manager.

- Un paramètre pour déterminer le certificat à utiliser si le client possède plusieurs certificats valides après le processus de sélection de certificat.
- Liste d'émetteurs de certificats qui contient une liste de certificats d'autorité de certification racine de confiance.

- Propriétés d'installation client.msi qui sont définies sous l'onglet **Client** de la boîte de dialogue **Propriétés de l'installation poussée du client** .

L'installation du client (CCMSetup) utilise les propriétés publiées dans les services de domaine Active Directory seulement si aucune autre propriété n'est spécifiée selon une des méthodes suivantes :

- La méthode d'installation manuelle (décrite plus loin dans cet article).
- La méthode d'installation via la stratégie de groupe (décrite plus loin dans cet article).

> **NOTE**
> Les propriétés d'installation du client sont utilisées pour installer le client. Ces propriétés peuvent être remplacées par de nouveaux paramètres provenant du site qui lui a été affecté une fois que le client est installé et qu'il a été affecté à un site Configuration Manager.

Utilisez les informations données dans les sections suivantes pour déterminer quelle méthode d'installation du client Configuration Manager utilise les services de domaine Active Directory pour obtenir les propriétés d'installation du client.

## Installation poussée du client

L'installation poussée du client n'utilise pas les services de domaine Active Directory pour accéder aux propriétés d'installation.

Au lieu de cela, vous pouvez spécifier les propriétés d'installation du client dans l'onglet **Client** de la boîte de dialogue **Propriétés de l'installation push du client**. Ces options et paramètres de site liés aux clients sont stockés dans un fichier que le client lit pendant l'installation du client.

> **NOTE**
> Vous n'avez pas à spécifier de propriétés CCMSetup pour l'installation poussée du client, ni de point d'état de secours ou la clé racine de confiance dans l'onglet **Client** . Ces paramètres sont automatiquement fournis aux clients, lorsqu'ils sont installés par l'installation poussée du client.

Toutes les propriétés que vous spécifiez dans l'onglet **Client** sont publiées dans les services de domaine Active Directory si le site y est publié. Ces paramètres sont lus par les installations du client où CCMSetup est exécuté sans propriété d'installation.

## Installation basée sur un point de mise à jour logicielle

La méthode d'installation basée sur un point de mise à jour logicielle ne prend pas en charge l'ajout de propriétés d'installation supplémentaires sur la ligne de commande CCMSetup.

Si aucune propriété de ligne de commande n'a été configurée sur l'ordinateur client utilisant la stratégie de groupe, CCMSetup recherche des propriétés d'installation dans les services de domaine Active Directory.

## Installation via la stratégie de groupe

La méthode d'installation via la stratégie de groupe ne prend pas en charge l'ajout de propriétés d'installation sur la ligne de commande CCMSetup.

Si aucune propriété de ligne de commande n'a été configurée sur l'ordinateur client, CCMSetup recherche des propriétés d'installation dans les services de domaine Active Directory.

## Installation manuelle

CCMSetup recherche des propriétés d'installation dans les services de domaine Active Directory dans les circonstances suivantes :

- Lorsqu'aucune propriété de ligne de commande n'est spécifiée à la suite de la commande CCMSetup.exe.
- Lorsque l'ordinateur n'a pas été configuré avec des propriétés d'installation à l'aide de la stratégie de groupe.

## Installation via un script d'ouverture de session

CCMSetup recherche des propriétés d'installation dans les services de domaine Active Directory dans les circonstances suivantes :

- Lorsqu'aucune propriété de ligne de commande n'est spécifiée à la suite de la commande CCMSetup.exe.
- Lorsque l'ordinateur n'a pas été configuré avec des propriétés d'installation à l'aide de la stratégie de groupe.

## Installation via la distribution de logiciels

CCMSetup recherche des propriétés d'installation dans les services de domaine Active Directory dans les circonstances suivantes :

- Lorsqu'aucune propriété de ligne de commande n'est spécifiée à la suite de la commande CCMSetup.exe.
- Lorsque l'ordinateur n'a pas été configuré avec des propriétés d'installation à l'aide de la stratégie de groupe.

## Installations pour les clients qui ne peuvent pas accéder aux services de domaine Active Directory

Ces ordinateurs clients ne peuvent pas lire ou accéder aux propriétés d’installation publiées à partir des services de domaine Active Directory.

Ces clients incluent les suivants :

- Ordinateurs d'un groupe de travail.
- Clients affectés à un site Configuration Manager qui n’est pas publié dans les services de domaine Active Directory.
- Clients installés quand ils sont sur Internet.

# Comment déployer des clients sur des serveurs UNIX et Linux dans System Center Configuration Manager

22/06/2018 • 25 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Avant de pouvoir gérer un serveur Linux ou UNIX avec System Center Configuration Manager, vous devez installer le client Configuration Manager pour Linux et UNIX sur chaque serveur Linux ou UNIX. Vous pouvez soit installer manuellement le client sur chaque ordinateur, soit utiliser un script Shell qui installe le client à distance. Configuration Manager ne prend pas en charge l'installation Push du client pour les serveurs Linux ou UNIX. Vous pouvez éventuellement configurer un Runbook pour System Center Orchestrator pour automatiser l'installation du client sur le serveur Linux ou UNIX.

Quelle que soit la méthode d'installation utilisée, le processus d'installation nécessite un script nommé **install** pour gérer le processus d'installation. Ce script est inclus lorsque vous téléchargez le Client pour Linux et UNIX.

Le script d'installation pour le client Configuration Manager pour Linux et UNIX prend en charge les propriétés de ligne de commande. Certaines propriétés de ligne de commande sont requises, tandis que d'autres sont facultatives. Par exemple, lorsque vous installez le client, vous devez spécifier un point de gestion à partir du site est utilisé par le serveur Linux ou UNIX pour son contact initial avec le site. Pour obtenir la liste complète des propriétés de ligne de commande, consultez Propriétés de ligne de commande pour installer le client sur des serveurs Linux et UNIX.

Après avoir installé le client, spécifiez les paramètres du client dans la console Configuration Manager pour configurer l'agent du client. Suivez la même procédure que pour un client Windows. Pour plus d'informations, consultez Paramètres client pour les serveurs Linux et UNIX.

## À propos des Packages d'Installation de Client et l'Agent universel

Pour installer le client pour Linux et UNIX sur une plateforme spécifique, vous devez utiliser le package d'installation du client applicable pour l'ordinateur sur lequel vous installez le client. Les packages d'installation de client applicables sont inclus dans chaque téléchargement du client effectué à partir du Centre de téléchargement Microsoft. En plus des packages d'installation de client, le téléchargement du client comprend le script **install** qui gère l'installation du client sur chaque ordinateur.

Lorsque vous installez un client, vous pouvez utiliser les mêmes propriétés de processus et de ligne de commande que vous utilisez le package d'installation client.

Pour plus d'informations sur les systèmes d'exploitation, les plateformes et les packages d'installation de client pris en charge par chaque version du client Configuration Manager pour Linux et UNIX, consultez Serveurs Linux et UNIX.

## Installer le Client sur des serveurs Linux et UNIX

Pour installer le client pour Linux et UNIX, vous exécutez un script sur chaque ordinateur Linux ou UNIX. Le script est nommé **installer** et prend en charge les propriétés de ligne de commande qui modifient le comportement d'installation et de référencent le package d'installation du client. Le package d'installation installation script et le client doit se trouver sur le client. Le package d'installation client contient les fichiers du client Configuration Manager pour une plate-forme et un système d'exploitation Linux ou UNIX spécifiques.

Chaque package d'installation du client contient tous les fichiers nécessaires pour terminer l'installation du client et contrairement aux ordinateurs fonctionnant sous Windows, ne pas télécharge des fichiers supplémentaires à partir d'un point de gestion ou un autre emplacement source.

Après avoir installé le client Configuration Manager pour Linux et UNIX, vous n'avez pas besoin de redémarrer l'ordinateur. Dès que l'installation est terminé, le client est opérationnel. Si vous redémarrez l'ordinateur, le client Configuration Manager redémarre automatiquement.

Le client installé s'exécute avec les informations d'identification racine. Des informations d'identification racine sont nécessaires pour collecter l'inventaire matériel et effectuer les déploiements de logiciels.

Le format de la commande est le suivant :

**./install -mp <ordinateur> -sitecode <code_site> <propriété 1> <propriété 2> <package d'installation du client>**

- **installer** est le nom du fichier de script qui installe le client pour Linux et UNIX. Ce fichier est fourni avec le logiciel client.
- **-mp <ordinateur** spécifie le point de gestion initial utilisé par le client.

  Exemple : smsmp.contoso.com
- **-sitecode <code_site>** spécifie le code de site auquel le client est affecté.

  Exemple : S01
- <propriété 1> <propriété 2> spécifie les propriétés de ligne de commande à utiliser avec le script d'installation.

  > **NOTE**
  > Pour plus d'informations, consultez Propriétés de ligne de commande pour installer le client sur des serveurs Linux et UNIX
- **package d'installation du client** est le nom du package .tar d'installation du client pour le système d'exploitation, la version et l'architecture d'UC de l'ordinateur. Le fichier .tar d'installation client doit être spécifié en dernier.

  Exemple : ccm-Universal-x64.<build>.tar

**Pour installer le Client Configuration Manager sur des serveurs Linux et UNIX**

1. Sur un ordinateur Windows, téléchargez le fichier client approprié pour le serveur Linux ou UNIX que vous souhaitez gérer.
2. Exécutez le fichier .exe à extraction automatique sur l'ordinateur Windows pour extraire le script d'installation et le fichier .tar d'installation du client.
3. Copiez le script d' **installation** et le fichier .tar dans un dossier sur le serveur que vous souhaitez gérer.
4. Sur le serveur UNIX ou Linux, exécutez la commande suivante pour autoriser le script à s'exécuter comme un programme : **chmod +x install**

   > **IMPORTANT**
   > Vous devez utiliser des informations d'identification racine pour installer le client.
5. Ensuite, exécutez la commande suivante pour installer le client Configuration Manager : **./install –mp**

**<nom_hôte> -sitecode <code> ccm-Universal-x64.<build>.tar**

Lorsque vous entrez cette commande, utilisez les propriétés de ligne de commande supplémentaires que vous avez besoin. Pour obtenir la liste des propriétés de ligne de commande, consultez Propriétés de ligne de commande pour installer le client sur des serveurs Linux et UNIX.

6. Une fois le script exécuté, validez l'installation en examinant le fichier **/var/opt/microsoft/scxcm.log** . De plus, vous pouvez vérifier que le client est installé et qu'il communique avec le site en affichant les détails relatifs au client dans le nœud **Appareils** de l'espace de travail **Ressources et Conformité** dans la console Configuration Manager.

**Propriétés de ligne de commande pour installer le client sur des serveurs Linux et UNIX**

Les propriétés suivantes sont disponibles pour modifier le comportement du script d'installation :

> **NOTE**
> Utilisez la propriété **-h** pour afficher la liste des propriétés prises en charge.

- **-mp <nom_de_domaine_complet_du_serveur>**

  Obligatoire. Spécifie le nom de domaine complet, le serveur de point de gestion que le client utilisera comme un point de contact initial.

  > **IMPORTANT**
  > Cette propriété n'indique pas le point de gestion auquel le client sera attribué après l'installation.

  > **NOTE**
  > Quand vous utilisez la propriété **-mp** pour spécifier un point de gestion qui est configuré pour accepter uniquement les connexions client HTTPS, vous devez également employer la propriété **-UsePKICert** .

- **-sitecode <code_site>**

  Obligatoire. Spécifie le site principal Configuration Manager auquel attribuer le client Configuration Manager.

  Exemple : -sitecode S01

- **-fsp <nom_de_domaine_complet_du_serveur>**

  Facultatif. Spécifie le nom de domaine complet, le serveur de point d'état de secours que le client utilise pour envoyer des messages d'état.

  Pour plus d'informations sur le point d'état de secours, consultez Déterminer si vous avez besoin d'un point d'état de secours .

- **-dir <répertoire>**

  Facultatif. Spécifie un autre emplacement pour installer les fichiers du client Configuration Manager.

  Par défaut, le client est installé à l'emplacement suivant : **/opt/microsoft**.

- **-nostart**

  Facultatif. Empêche le démarrage automatique du service client Configuration Manager, **ccmexec.bin**, après l'installation du client.

Une fois le client installé, vous devez démarrer manuellement le service client.

Par défaut, le service client démarre après la fin de l'installation du client, et chaque fois que l'ordinateur redémarre.

- **-nettoyage**

  Facultatif. Spécifie la suppression de tous les fichiers du client et les données à partir d'un client installé précédemment pour Linux et UNIX, avant le démarrage de la nouvelle installation. Cela supprime le magasin de certificats et la base de données du client.

- **-keepdb n' n'**

  Facultatif. Spécifie que la base de données client local est conservée et réutilisée, lorsque vous réinstallez un client. Par défaut, lorsque vous réinstallez un client de cette base de données est supprimé.

- **-UsePKICert <paramètre>**

  Facultatif. Spécifie le chemin d'accès et le nom complet à un certificat X.509 PKI au format Public Key Certificate Standard (PKCS #12). Ce certificat est utilisé pour l'authentification du client. Si aucun certificat n'est spécifié pendant l'installation et que vous devez en ajouter ou en modifier un, faites appel à l'utilitaire **certutil** . Pour plus d'informations sur certutil, consultez Comment gérer des certificats sur le client pour Linux et UNIX .

  Quand vous utilisez **-UsePKICert**, vous devez également fournir le mot de passe associé au fichier PKCS #12 à l'aide du paramètre de ligne de commande **-certpw** .

  Si vous n'utilisez pas cette propriété pour spécifier un certificat PKI, le client utilise un certificat auto-signé et sont des systèmes de site de toutes les communications via HTTP.

  Si vous spécifiez un certificat non valide sur le client installation de ligne de commande, aucune erreur n'est retournée. Il s'agit, car la validation de certificat se produit après l'installation du client. Lorsque le client démarre, les certificats sont validés avec le point de gestion et si un certificat de validation échoue le message suivant apparaît dans **scxcm.log**, le fichier journal du client Unix et Linux Configuration Manager : **Échec de valider le certificat de Point de gestion**. L'emplacement par défaut du fichier journal est : **/var/opt/microsoft/scxcm.log**.

  > **NOTE**
  > Vous devez spécifier cette propriété quand vous installez un client et utiliser la propriété **-mp** pour indiquer un point de gestion qui est configuré pour accepter uniquement les connexions client HTTPS.

  Exemple : -UsePKICert <chemin_complet_et_nom_de_fichier> -certpw <mot_de_passe>

- **-certpw <paramètre>**

  Facultatif. Spécifie le mot de passe associé au fichier PKCS #12 que vous avez spécifié à l'aide de la **-/usepkicert** propriété.

  Exemple : -UsePKICert <chemin_complet_et_nom_de_fichier> -certpw <mot_de_passe>

- **-/Nocrlcheck**

  Facultatif. Spécifie qu'un client ne doit pas vérifier la liste de révocation de certificats (CRL) lorsqu'il communique via HTTPS à l'aide d'un certificat PKI. Lorsque cette option n'est pas spécifiée, le client vérifie la révocation de certificats avant d'établir une connexion HTTPS à l'aide de certificats PKI. Pour plus d'informations sur la vérification de révocation de certificats client, consultez Planification de la révocation de certificats PKI.

Exemple : -UsePKICert <chemin_complet_et_nom_de_fichier> -certpw <mot_de_passe> -NoCRLCheck

- **-rootkeypath <emplacement_fichier>**

  Facultatif. Spécifie le chemin d'accès complet et le nom de fichier de la clé racine approuvée Configuration Manager. La clé racine approuvée Configuration Manager fournit un mécanisme que les clients Linux et UNIX utilisent pour vérifier qu'ils sont connectés à un système de site qui appartient à la hiérarchie appropriée.

  Si vous ne spécifiez pas la clé racine approuvée sur la ligne de commande, le client approuve le premier point de gestion avec lequel il communique et récupère automatiquement la clé racine approuvée à partir de ce point de gestion.

  Pour plus d'informations, consultez Planning for the Trusted Root Key.

  Exemple : -rootkeypath >chemin_complet_et_nom_de_fichier<

- **-httpport <port>**

  Facultatif. Spécifie le port est configuré sur les points de gestion que le client utilise lors de la communication aux points de gestion via HTTP. Si le port n'est pas spécifié, la valeur par défaut 80 est utilisée.

  Exemple : -httpport 80

- **-httpsport <port>**

  Facultatif. Spécifie le port est configuré sur les points de gestion que le client utilise lors de la communication aux points de gestion via HTTPS. Si le port n'est pas spécifié, la valeur par défaut 443 est utilisée.

  Exemple : -UsePKICert <chemin_complet_et_nom_de_certificat> -httpsport 443

- **-ignoreSHA256validation**

  Facultatif. Spécifie que l'installation du client ignore la validation de l'algorithme SHA-256. Utilisez cette option quand vous installez le client sur des systèmes d'exploitation publiés avec une version d'OpenSSL qui ne prend pas en charge SHA-256. Pour plus d'informations, voirÀ propos des systèmes d'exploitation Linux et UNIX qui ne prennent pas en charge SHA-256.

- **-signcertpath <emplacement_fichier>**

  Facultatif. Spécifie le chemin d'accès complet et **.cer** nom de fichier du certificat auto-signé exporté sur le serveur de site. Si les certificats PKI ne sont pas disponibles, le serveur de site Configuration Manager génère automatiquement des certificats auto-signés.

  Ces certificats sont utilisés pour valider que les stratégies client téléchargés à partir du point de gestion ont été envoyés à partir du site de destination. Si aucun certificat auto-signé n'est spécifié pendant l'installation ou que vous devez modifier le certificat, faites appel à l'utilitaire **certutil** . Pour plus d'informations sur certutil, consultez Comment gérer des certificats sur le client pour Linux et UNIX .

  Ce certificat, qui peut être récupéré dans le magasin de certificats **SMS** , porte le nom d'objet **Serveur de site** et le nom convivial **Certificat de signature du serveur de site**.

  Si cette option n'est pas spécifiée lors de l'installation, les clients Linux et UNIX approuvent le premier point de gestion qu'ils communiquent avec et récupère automatiquement le certificat de signature à partir de ce point de gestion.

  Exemple : -signcertpath <chemin_complet_et_nom_de_fichier>

- **-rootcerts**

Facultatif. Spécifie les autres certificats PKI pour importer qui ne font pas partie d'une hiérarchie d'autorité de certification gestion des points. Si vous spécifiez plusieurs certificats dans la ligne de commande, ils doivent être séparés par des virgules.

Utilisez cette option si vous utilisez des certificats clients PKI qui ne se lient pas à un certificat d'autorité de certification racine approuvée par les points de gestion de vos sites. Les points de gestion rejettent le client si le certificat client n'est pas associé à un certificat racine approuvé dans la liste des émetteurs de certificat du site.

Si vous n'utilisez pas cette option, le client Linux et UNIX vérifiera la hiérarchie d'approbation en utilisant uniquement le certificat dans le **- /usepkicert** option.

Exemple : -rootcerts <chemin_complet_et_nom_de_fichier>,<chemin_complet_et_nom_de_fichier>

**Désinstallation du client sur des serveurs Linux et UNIX**

Pour désinstaller le client Configuration Manager pour Linux et UNIX, vous utilisez l'utilitaire de désinstallation, **uninstall**. Par défaut, ce fichier se trouve dans le **/opt/microsoft/configmgr/bin/** dossier sur l'ordinateur client. Cette commande de désinstallation ne prend pas en charge des paramètres de ligne de commande et supprimera tous les fichiers liés au logiciel client à partir du serveur.

Pour désinstaller le client, utilisez la ligne de commande suivante : **/opt/microsoft/configmgr/bin/uninstall**

Après avoir désinstallé le client Configuration Manager pour Linux et UNIX, vous n'avez pas besoin de redémarrer l'ordinateur.

# Configurer les Ports de requêtes pour le Client pour Linux et UNIX

Comme les clients basés sur Windows, le client Configuration Manager pour Linux et UNIX utilise HTTP et HTTPS pour communiquer avec les systèmes de site Configuration Manager. Les ports que le client Configuration Manager utilise pour communiquer sont appelés ports de demande.

Lorsque vous installez le client Configuration Manager pour Linux et UNIX, vous pouvez modifier les ports de demande par défaut du client en spécifiant les propriétés d'installation **-httpport** et **-httpsport**. Lorsque vous ne spécifiez pas la propriété d'installation et une valeur personnalisée, le client utilise les valeurs par défaut. Les valeurs par défaut sont **80** pour le trafic HTTP et **443** pour le trafic HTTPS.

Après avoir installé le client, vous ne pouvez pas modifier sa configuration de port de demande. En revanche, pour modifier la configuration du port, vous devez réinstaller le client et spécifier la configuration du port. Lorsque vous réinstallez le client pour modifier les numéros de port de requête, exécutez le **installer** commande semblable à l'installation du client, mais utilisez la propriété de ligne de commande supplémentaires de **- keepdb ne**. Ce commutateur indique à l'installation pour conserver la base de données client et les fichiers, notamment le magasin GUID et des certificats clients.

Pour plus d'informations sur les numéros de port de communication client, consultez Comment configurer les ports de communication des clients dans System Center Configuration Manager.

# Configurer le Client pour Linux et UNIX de localiser des Points de gestion

Lorsque vous installez le client Configuration Manager pour Linux et UNIX, vous devez spécifier un point de gestion à utiliser comme point de contact initial.

Le client Configuration Manager pour Linux et UNIX contacte ce point de gestion au moment de l'installation du client. Si le client ne parvient pas à contacter le point de gestion, le logiciel client renouvelle les tentatives jusqu'à ce que le contact soit établi.

Pour plus d'informations sur la manière dont les clients localisent les points de gestion, consultez Localisation de

points de gestion.

# Services de composants et leurs commandes sur des clients Linux et UNIX pour System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Le tableau ci-dessous identifie les services de composants clients du client Configuration Manager pour Linux et UNIX.

| NOM DE FICHIER | PLUS D'INFORMATIONS |
|---|---|
| ccmexec.bin | Ce service équivaut au service ccmexc sur un client Windows. Il est responsable de toutes les communications avec les rôles de système de site Configuration Manager et communique également avec le service omiserver.bin pour procéder à l'inventaire matériel de l'ordinateur local.<br><br>Pour obtenir la liste des arguments de ligne de commande pris en charge, exécutez **ccmexec -h** |
| omiserver.bin | Ce service est le serveur CIM. Le serveur CIM fournit une infrastructure pour des modules logiciels enfichables appelés fournisseurs. Les fournisseurs interagissent avec les ressources informatiques Linux et UNIX, et recueillent les données de l'inventaire matériel. Par exemple, le **fournisseur process** pour une Linux ordinateur collecte les données associées avec les processus du système d'exploitation Linux. |

Les commandes de liste de tables suivantes que vous pouvez utiliser pour démarrer, arrêter ou redémarrer les services du client (ccmexec.bin et omiserver.bin) sur chaque version de Linux ou UNIX. Quand vous démarrez ou arrêtez le service ccmexec, le service omiserver démarre ou s'arrête également.

| SYSTÈME D'EXPLOITATION | COMMANDES |
|---|---|
| Agent universel<br><br>RHEL 4 et SLES 9 | Démarrer : **/etc/init d/ccmexecd start**<br><br>Arrêter : **/etc/init d/ccmexecd stop**<br><br>Redémarrer : **/etc/init d/ccmexecd restart** |
| Solaris 9 | Démarrer : **/etc/init d/ccmexecd start**<br><br>Arrêter : **/etc/init d/ccmexecd stop**<br><br>Redémarrer : **/etc/init d/ccmexecd restart** |

| SYSTÈME D'EXPLOITATION | COMMANDES |
| --- | --- |
| Solaris 10 | Démarrer :<br><br>**svcadm enable -s svc:/application/management/omiserver**<br><br>**svcadm enable -s svc:/application/management/ccmexecd**<br><br>Arrêter :<br><br>**svcadm disable -s svc:/application/management/ccmexecd**<br><br>**svcadm disable -s svc:/application/management/omiserver** |
| Solaris 11 | Démarrer :<br><br>**svcadm enable -s svc:/application/management/omiserver**<br><br>**svcadm enable -s svc:/application/management/ccmexecd**<br><br>Arrêter :<br><br>**svcadm disable -s svc:/application/management/ccmexecd**<br><br>**svcadm disable -s svc:/application/management/omiserver** |
| AIX | Démarrer :<br><br>**startsrc -s omiserver**<br><br>**startsrc -s ccmexec**<br><br>Arrêter :<br><br>**stopsrc -s ccmexec**<br><br>**stopsrc -s omiserver** |
| HP-UX | Démarrer : **/sbin/init.d/ccmexecd start**<br><br>Arrêter : **/sbin/init.d/ccmexecd stop**<br><br>Redémarrer : **/sbin/init.d/ccmexecd restart** |

# Préparer le déploiement du logiciel client pour ordinateurs Mac

22/06/2018 • 16 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Procédez comme suit pour vérifier que vous êtes prêt à déployer le client Configuration Manager sur les ordinateurs Mac.

## Prérequis des ordinateurs Mac

Le package d'installation de client Mac n'est pas fourni avec le support d'installation de Configuration Manager. Téléchargez les **clients pour d'autres systèmes d'exploitation** à partir du Centre de téléchargement Microsoft.

**Versions prises en charge :**

- **Mac OS X 10.6** (Snow Leopard)
- **Mac OS X 10.7** (Lion)
- **Mac OS X 10.8** (Mountain Lion)
- **Mac OS X 10.9** (Mavericks)
- **Mac OS X 10.9** (Mavericks)
- **Mac OS X 10.10** (Yosemite)
- **Mac OS X 10.11** (El Capitan)
- **Mac OS X 10.12** (macOS Sierra)
- **Mac OS X 10.13** (macOS High Sierra)

## Conditions de certificat

L'installation et la gestion de clients pour les ordinateurs Mac nécessitent des certificats d'infrastructure à clé publique (PKI). Les certificats PKI permettent de sécuriser les communications entre les ordinateurs Mac et le site Configuration Manager grâce à une authentification mutuelle et des transferts de données chiffrés. Configuration Manager peut demander et installer un certificat client utilisateur à l'aide des services de certificat Microsoft avec une autorité de certification d'entreprise (CA) et les rôles de système de site du point d'inscription et du point proxy d'inscription de Configuration Manager. Vous pouvez également demander et installer un certificat d'ordinateur indépendamment de Configuration Manager si le certificat répond aux critères de Configuration Manager.

Les clients Mac Configuration Manager procèdent toujours à une vérification de la révocation des certificats. Vous ne pouvez pas désactiver cette fonction.

Si les clients Mac ne peuvent pas vérifier l'état de révocation du certificat d'un serveur du fait de leur incapacité à localiser la liste CRL, ils ne peuvent pas se connecter aux systèmes de site Configuration Manager. Vérifiez la conception de votre liste CRL pour être certain que les clients Mac (plus particulièrement ceux appartenant à une forêt différente de celle de l'autorité de certification émettrice) seront en mesure de localiser et de se connecter à un point de distribution de la liste CRL (CDP) pour la connexion des serveurs de système de site.

Avant d'installer le client Configuration Manager sur un ordinateur Mac, choisissez le mode d'installation du

certificat client :

- Utilisez l'inscription Configuration Manager à l'aide de l'outil CMEnroll. Le processus d'inscription ne prenant pas en charge le renouvellement automatique de certificats, vous devez réinscrire les ordinateurs Mac avant l'expiration du certificat installé.
- Utilisez une demande de certificat et une méthode d'installation indépendantes de Configuration Manager.

Pour plus d'informations sur le certificat client Mac requis et sur les autres certificats PKI nécessaires à la prise en charge des ordinateurs Mac, consultez Configuration requise des certificats PKI pour System Center Configuration Manager.

Les clients Mac sont attribués automatiquement au site Configuration Manager qui les gère. Les clients Mac s'installent en tant que clients Internet uniquement, même si la communication est limitée à l'intranet. Cette configuration de client signifie qu'ils communiquent avec les rôles de système de site (points de gestion et points de distribution) sur le site qui leur est attribué si vous configurez ces rôles pour autoriser les connexions client depuis Internet. Les ordinateurs Mac ne communiquent pas avec les rôles de système de site extérieurs au site qui leur est attribué.

> **IMPORTANT**
> Vous ne pouvez pas utiliser le client Mac Configuration Manager pour vous connecter à un point de gestion configuré pour utiliser un réplica de base de données.

## Déployer un certificat de serveur web sur des serveurs de système de site

Si ces systèmes de site n'en ont pas, déployez un certificat de serveur web sur les ordinateurs qui ont ces rôles de système de site :

- Point de gestion
- Point de distribution
- Point d'inscription
- Point proxy d'inscription

Le certificat de serveur Web doit contenir le nom de domaine Internet complet qui est spécifié dans les propriétés de système de site. Le serveur ne doit pas nécessairement être accessible sur Internet pour prendre en charge les ordinateurs Mac. Si vous n'exigez pas de gestion des clients basée sur Internet, vous pouvez spécifier la valeur du nom de domaine complet intranet pour le nom de domaine complet Internet.

Spécifiez la valeur du nom de domaine complet Internet du système de site dans le certificat de serveur web pour le point de gestion, le point de distribution et le point proxy d'inscription.

Pour voir un exemple de déploiement qui crée et installe ce certificat de serveur web, consultez Déploiement du certificat de serveur web pour les systèmes de site qui exécutent IIS.

## Déployer un certificat d'authentification client sur des serveurs de système de site

Si ces systèmes de site n'en ont pas, déployez un certificat d'authentification client sur les ordinateurs qui hébergent les rôles de système de site suivants :

- Point de gestion

- Point de distribution

  Pour obtenir un exemple de déploiement qui crée et installe le certificat client pour les points de gestion, consultez Déploiement du certificat client pour les ordinateurs Windows.

  Pour obtenir un exemple de déploiement qui crée et installe le certificat client pour les points de distribution, consultez Déploiement du certificat client pour les points de distribution.

> **IMPORTANT**
> Pour déployer le client sur des appareils macOS Sierra, vous devez configurer correctement le nom du sujet du certificat de point de gestion, par exemple en utilisant le nom de domaine complet du serveur de point de gestion.

## Préparer le modèle de certificat client pour les ordinateurs Mac

Le modèle de certificat doit disposer d'autorisations de **lecture** et d' **inscription** pour le compte d'utilisateur appelé à inscrire le certificat sur l'ordinateur Mac.

Consultez Déploiement du certificat client pour les ordinateurs Mac.

## Configurer le point de gestion et le point de distribution

Configurez des points de gestion pour les options suivantes :

- HTTPS
- Autorisez les connexions client à partir d'Internet. Cette valeur de configuration est nécessaire pour gérer les ordinateurs Mac. Toutefois, cela ne signifie pas que les serveurs de système de site doivent être accessibles sur Internet.
- Autoriser les appareils mobiles et les ordinateurs Mac à utiliser ce point de gestion

  Même si les points de distribution ne sont pas indispensables à l'installation du client, vous devez en configurer pour permettre au client de se connecter à partir d'Internet si vous voulez déployer des logiciels sur ces ordinateurs après avoir installé le client.

**Pour configurer les points de gestion et les points de distribution pour prendre en charge les ordinateurs Mac**

Avant d'entamer cette procédure, assurez-vous que le serveur de système de site exécutant le point de gestion et le point de distribution est configuré avec un nom de domaine Internet complet. Si ces serveurs de système de site ne prennent pas en charge la gestion des clients sur Internet, vous pouvez spécifier le nom de domaine complet intranet comme valeur du nom de domaine complet Internet.

Les rôles de système de site doivent se trouver dans un site principal.

1. Dans la console Configuration Manager, choisissez **Administration** > **Configuration du site** > **Serveurs et rôles de système de site**, puis choisissez le serveur disposant des rôles de système de site appropriés.
2. Dans le volet des détails, cliquez avec le bouton droit sur **Point de gestion**, choisissez **Propriétés du rôle** et, dans la boîte de dialogue **Propriétés du point de gestion**, configurez les options suivantes:

   a. Choisissez **HTTPS**.

   b. Choisissez **Autoriser les connexions au client Internet uniquement** ou **Autoriser les connexions au client Internet et intranet**. Ces options nécessitent un nom de domaine complet Internet ou intranet.

   c. Choisissez **Autoriser les périphériques mobiles et les ordinateurs Mac à utiliser ce point de gestion**.

3. Dans le volet des détails, cliquez avec le bouton droit sur **Point de distribution**, choisissez **Propriétés du rôle**, puis dans la boîte de dialogue **Propriétés du point de distribution**, configurez les options suivantes :

   - Choisissez **HTTPS**.
   - Choisissez **Autoriser les connexions au client Internet uniquement** ou **Autoriser les connexions au client Internet et intranet**. Ces options nécessitent un nom de domaine complet Internet ou intranet.
   - Choisissez **Importer un certificat**, accédez au fichier du certificat de point de distribution client exporté, puis spécifiez le mot de passe.

4. Répétez les étapes 2 à 4 pour tous les points de gestion et les points de distribution des sites principaux que vous prévoyez d'utiliser avec des ordinateurs Mac.

## Configurer le point proxy d'inscription et le point d'inscription

Vous devez installer ces deux rôles de système de site sur le même site, mais il n'est pas nécessaire de les installer sur le même serveur de système de site ni sur la même forêt Active Directory.

Pour plus d'informations sur la sélection élective des rôles de système de site et sur les éléments à prendre en considération, consultez Rôles de système de site dans Planifier des serveurs de système de site et des rôles système de site pour System Center Configuration Manager.

Ces procédures permettent de configurer les rôles de système de site pour prendre en charge les ordinateurs Mac.

- Nouveau serveur de système de site
- Serveur de système de site existant

**Nouveau serveur de système de site**

1. Dans la console Configuration Manager, choisissez **Administration** > **Configuration du site** > **Serveurs et rôles de système de site**.
2. Sous l'onglet **Accueil**, dans le groupe **Créer**, choisissez **Créer un serveur de système de site**.
3. Dans la page **Général**, spécifiez les paramètres généraux du système de site. Vérifiez que vous spécifiez une valeur pour le nom de domaine complet Internet. Si le serveur n'est pas accessible à partir d'Internet, utilisez le nom de domaine complet intranet.
4. Dans la page **Sélection du rôle système**, sélectionnez **Point proxy d'inscription** et **Point d'inscription** dans la liste des rôles disponibles.
5. Dans la page **Point proxy d'inscription**, vérifiez les paramètres et apportez les modifications nécessaires.
6. Dans la page **Paramètres du point d'inscription**, vérifiez les paramètres et apportez les modifications nécessaires. Ensuite, exécutez l'Assistant.

**Serveur de système de site existant**

1. Dans la console Configuration Manager, choisissez **Administration** > **Configuration du site** > **Serveurs et rôles de système de site**, puis choisissez le serveur à utiliser pour prendre en charge les ordinateurs Mac.
2. Sous l'onglet **Accueil**, dans le groupe **Créer**, choisissez **Ajouter des rôles de système de site**.
3. Sur la page **Général** , spécifiez les paramètres généraux du système de site, puis cliquez sur **Suivant**. Vérifiez que vous spécifiez une valeur pour le nom de domaine complet Internet. Si le serveur n'est pas accessible à partir d'Internet, utilisez le nom de domaine complet intranet.
4. Dans la page **Sélection du rôle système**, choisissez **Point proxy d'inscription** et **Point d'inscription**

dans la liste des rôles disponibles.

5. Dans la page **Point proxy d'inscription**, vérifiez les paramètres et apportez les modifications nécessaires.
6. Dans la page **Paramètres du point d'inscription**, vérifiez les paramètres et apportez les modifications nécessaires. Ensuite, exécutez l'Assistant.

## Installez le point de Reporting Services.

Installez le point de Reporting Services si vous voulez exécuter des rapports pour les ordinateurs Mac.

**Étapes suivantes**

Déployez le client Configuration Manager sur des ordinateurs Mac.

# How to deploy clients to Macs

22/06/2018 • 26 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cette rubrique décrit comment déployer et gérer le client Configuration Manager sur des ordinateurs Mac. Pour en savoir plus sur les éléments à configurer avant de déployer les clients sur des ordinateurs Mac, consultez Préparer le déploiement du logiciel client pour ordinateurs Mac.

Quand vous installez un nouveau client pour les ordinateurs Mac, vous devez peut-être également installer des mises à jour Configuration Manager pour refléter les nouvelles informations client dans la console Configuration Manager.

Dans ces procédures, vous avez deux options pour l'installation des certificats clients. En savoir plus sur les certificats clients pour Mac dans Préparer le déploiement du logiciel client pour ordinateurs Mac.

- Utilisez l'inscription Configuration Manager à l'aide de l'outil CMEnroll. Le processus d'inscription ne prenant pas en charge le renouvellement automatique de certificats, vous devez réinscrire les ordinateurs Mac avant l'expiration du certificat installé.
- Utilisez une demande de certificat et une méthode d'installation indépendantes de Configuration Manager.

> **IMPORTANT**
> Pour déployer le client sur des appareils macOS Sierra, vous devez configurer correctement le nom du sujet du certificat de point de gestion, par exemple en utilisant le nom de domaine complet du serveur de point de gestion.

## Configurer les paramètres client pour l'inscription

Vous devez utiliser les paramètres client par défaut pour configurer l'inscription pour les ordinateurs Mac ; vous ne pouvez pas utiliser de paramètres client personnalisés.

Cela est nécessaire pour permettre à Configuration Manager de demander et d'installer le certificat sur l'ordinateur Mac.

**Pour configurer les paramètres client par défaut pour permettre à Configuration Manager d'inscrire des certificats pour les ordinateurs Mac**

1. Dans la console Configuration Manager, choisissez **Administration** > **Paramètres client** > **Paramètres client par défaut**.
2. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
3. Sélectionnez la section **Inscription**, puis configurez ces paramètres :
   a. **Autoriser les utilisateurs à inscrire des appareils mobiles et des ordinateurs Mac : Oui**
   b. **Profil d'inscription :** choisissez **Définir un profil**.
4. Dans la boîte de dialogue **Profil d'inscription d'appareil mobile**, choisissez **Créer**.
5. Dans la boîte de dialogue **Créer un profil d'inscription** , entrez un nom pour ce profil d'inscription, puis configurez le **Code du site de gestion**. Sélectionnez le site principal Configuration Manager contenant les points de gestion qui géreront les ordinateurs Mac.

> **NOTE**
> Si vous ne pouvez pas sélectionner le site, vérifiez qu'au moins un point de gestion dans le site est configuré pour la prise en charge des appareils mobiles.

6. Choisissez **Ajouter**.
7. Dans la boîte de dialogue **Ajouter une autorité de certification pour les appareils mobiles**, sélectionnez le serveur de l'autorité de certification émettrice des certificats pour les ordinateurs Mac.
8. Dans la boîte de dialogue **Créer un profil d'inscription**, sélectionnez le modèle de certificat d'ordinateur Mac que vous avez créé à l'étape 3.
9. Cliquez sur **OK** pour fermer la boîte de dialogue **Profil d'inscription**, puis la boîte de dialogue **Paramètres client par défaut**.

> **TIP**
> Si vous voulez modifier l'intervalle de la stratégie client, utilisez le paramètre **Intervalle d'interrogation de stratégie client** dans le groupe de paramètres client **Stratégie client**.

Tous les utilisateurs sont configurés avec ces paramètres la prochaine fois qu'ils téléchargent la stratégie du client. Pour lancer la récupération de stratégie pour un seul client, consultez Lancer une récupération de stratégie pour un client Configuration Manager.

Outre les paramètres client d'inscription, vérifiez que vous avez configuré les paramètres d'appareil client suivants :

- **Inventaire matériel** : Activez et configurez ce paramètre si vous voulez collecter l'inventaire matériel des ordinateurs clients Mac et Windows. Pour plus d'informations, consultez Comment étendre l'inventaire matériel dans System Center Configuration Manager.
- **Paramètres de compatibilité** : Activez et configurez ce paramètre si vous voulez évaluer et corriger les paramètres sur les ordinateurs clients Mac et Windows. Pour plus d'informations, consultez Planifier et configurer les paramètres de compatibilité.

> **NOTE**
> Pour plus d'informations sur les paramètres client Configuration Manager, consultez Guide pratique pour configurer les paramètres client dans System Center Configuration Manager.

## Télécharger les fichiers sources du client pour les ordinateurs Mac

1. Téléchargez le package de fichiers du client Mac OS X, **ConfigmgrMacClient.msi**, et enregistrez-le sur un ordinateur exécutant Windows.

   Ce fichier n'est pas fourni dans le support d'installation de Configuration Manager. Vous pouvez télécharger ce fichier à partir du Centre de téléchargement Microsoft.
2. Sur l'ordinateur Windows, exécutez **ConfigmgrMacClient.msi** pour extraire le package du client Mac (Macclient.dmg) dans un dossier du disque local (par défaut, **C:\Program Files (x86)\Microsoft\System Center 2012 Configuration Manager Mac Client**).
3. Copiez le fichier Macclient.dmg dans un dossier de l'ordinateur Mac.

4. Sur l'ordinateur Mac, exécutez le fichier Macclient.dmg pour extraire les fichiers dans un dossier du disque local.

5. Dans ce dossier, assurez-vous que les fichiers Ccmsetup et CMClient.pkg ont été extraits, qu'un dossier nommé Outils a été créé et qu'il contient les outils CMDiagnostics, CMUninstall, CMAppUtil et CMEnroll.

   - **Ccmsetup** : permet d'installer le client Configuration Manager sur les ordinateurs Mac.
   - **CMDiagnostics** : permet de collecter les informations de diagnostic relatives au client Configuration Manager sur les ordinateurs Mac.
   - **CMUninstall** : permet de désinstaller le client des ordinateurs Mac.
   - **CMAppUtil** : permet de convertir les packages d'applications Apple dans un format qui peut être déployé sous forme d'application Configuration Manager.
   - **CMEnroll** : permet de demander et d'installer le certificat client d'un ordinateur Mac en vue d'installer le client Configuration Manager.

## Installer le client, puis inscrire le certificat client sur l'ordinateur Mac

Vous pouvez inscrire des clients individuels avec l'Assistant Inscription d'ordinateur Mac.

Pour activer l'automatisation qui permet d'inscrire un grand nombre de clients, servez-vous de l'outil CMEnroll.

**Inscrire le client à l'aide de l'Assistant Inscription d'ordinateur Mac**

1. Quand vous avez terminé l'installation du client, l'Assistant Inscription d'ordinateur s'ouvre. Si l'Assistant ne s'ouvre pas ou si vous le fermez par inadvertance, cliquez sur **Inscription** dans la page des préférences **Configuration Manager** pour l'ouvrir.

2. Dans la deuxième page de l'Assistant, entrez les informations suivantes :

   - **Nom d'utilisateur** : le nom d'utilisateur peut se présenter sous l'une des formes suivantes :
     - « domaine\nom ». Par exemple: « contoso\mnorth »
     - « user@domain ». Par exemple : « mnorth@contoso.com »

     > **IMPORTANT**
     > Lorsque vous utilisez une adresse électronique pour renseigner le champ **Nom d'utilisateur**, Configuration Manager utilise automatiquement le nom de domaine de l'adresse électronique et le nom par défaut du serveur de point proxy d'inscription pour renseigner le champ **Nom du serveur**. Si ce nom de domaine et ce nom de serveur ne correspondent pas au nom du serveur de point proxy d'inscription, indiquez aux utilisateurs le nom correct à utiliser lors de l'inscription de leurs ordinateurs Mac.

     Le nom d'utilisateur et le mot de passe correspondant doivent correspondre à un compte d'utilisateur Active Directory disposant des autorisations de lecture et d'inscription dans le modèle de certificat client Mac.

   - **Mot de passe** : entrez un mot de passe correspondant au nom d'utilisateur spécifié.
   - **Nom du serveur** : entrez le nom du serveur de point proxy d'inscription.

**Automatisation du client et du certificat avec CMEnroll**

Utilisez cette procédure pour l'automatisation de l'installation du client ainsi que la demande et l'inscription de certificats clients avec l'outil CMEnroll. Pour exécuter l'outil, vous devez disposer d'un compte d'utilisateur Active Directory.

1. Sur l'ordinateur Mac, accédez au dossier dans lequel vous avez extrait le contenu du fichier macclient.dmg.
2. Entrez la ligne de commande suivante : **sudo ./ccmsetup**
3. Patientez jusqu'à ce que le message **Installation terminée** s'affiche à l'écran. Même si le programme d'installation affiche un message vous demandant de redémarrer maintenant, ne suivez pas cette instruction et passez à l'étape suivante.
4. Dans le dossier Outils sur l'ordinateur Mac, tapez la commande suivante : **sudo ./CMEnroll -s <nom_serveur_proxy_inscription> -ignorecertchainvalidation -u <nom_utilisateur>**

   Une fois le client installé, l'Assistant Inscription d'ordinateur Mac s'ouvre pour vous aider à inscrire l'ordinateur Mac. Pour inscrire le client par cette méthode, consultez To enroll the client by using the Mac Computer Enrollment Wizard dans cette rubrique.
5. Tapez le mot de passe du compte d'utilisateur Active Directory. Quand vous entrez cette commande, vous êtes invité à entrer deux mots de passe : la première invite concerne le compte de superutilisateur qui exécute la commande. La seconde invite est pour le compte d'utilisateur Active Directory. Les invites semblent identiques, assurez-vous que vous les spécifiez dans le bon ordre.

   Le nom d'utilisateur peut se présenter sous l'une des formes suivantes :

   - « domaine\nom ». Par exemple: « contoso\mnorth »
   - « user@domain ». Par exemple : « mnorth@contoso.com »

     Le nom d'utilisateur et le mot de passe correspondant doivent correspondre à un compte d'utilisateur Active Directory disposant des autorisations de lecture et d'inscription dans le modèle de certificat client Mac.

     Exemple : si le serveur de point proxy d'inscription se nomme **server02.contoso.com** et que des autorisations ont été accordées au nom d'utilisateur **contoso\mnorth** pour le modèle de certificat client Mac, tapez la ligne suivante : **sudo ./CMEnroll -s server02.contoso.com -ignorecertchainvalidation -u 'contoso\mnorth'**

     > **NOTE**
     > Si le nom d'utilisateur contient l'un des caractères **<>"+=,**, l'inscription échoue. Obtenez un certificat hors bande avec un nom d'utilisateur qui ne contient pas ces caractères.
     >
     > Pour une expérience utilisateur plus transparente, vous pouvez mettre les étapes d'installation et les commandes sous forme de script afin que les utilisateurs n'aient qu'à fournir leurs nom d'utilisateur et mot de passe.
6. Patientez jusqu'à l'affichage d'un message indiquant que l' **inscription s'est déroulée correctement** .
7. Pour limiter le certificat inscrit à Configuration Manager, sur l'ordinateur Mac, ouvrez une fenêtre de terminal et apportez les modifications suivantes :

   a. Entrez la commande **sudo /Applications/Utilities/Keychain\ Access.app/Contents/MacOS/Keychain\ Access**

   b. Dans la boîte de dialogue **Trousseau d'accès**, dans la zone **Trousseau**, choisissez **Système**, puis dans la zone **Catégorie**, choisissez **Clés**.

   c. Développez les clés pour afficher les certificats clients. Lorsque vous avez identifié le certificat avec une clé privée que vous venez d'installer, double-cliquez sur la clé.

   d. Sous l'onglet **Contrôle d'accès**, choisissez **Confirmer avant d'autoriser l'accès**.

e. Accédez à **/Library/Application Support/Microsoft/CCM**, sélectionnez **CCMClient**, puis choisissez **Ajouter**.

f. Choisissez **Enregistrer les modifications** et fermez la boîte de dialogue **Trousseau d'accès**.

8. Redémarrez l'ordinateur Mac.

   Vérifiez que l'installation du client a abouti en ouvrant l'élément **Configuration Manager** dans les **Préférences Système** de l'ordinateur Mac. Vous pouvez également mettre à jour et afficher le regroupement **Tous les systèmes** pour vérifier que l'ordinateur Mac figure désormais dans ce regroupement en tant que client géré.

> **TIP**
> Pour vous aider à résoudre les problèmes liés au client Mac, vous pouvez utiliser le programme CMDiagnostics inclus avec le package client Mac OS X afin de recueillir les informations de diagnostic suivantes :
>
> - Liste des processus en cours.
>   - Version du système d'exploitation Mac OS X.
>   - Rapports des défaillances du système Mac OS X liées au client Configuration Manager, y compris les fichiers **CCM*.crash** et **System Preference.crash**.
>   - Le fichier de nomenclature et le fichier de liste des propriétés (.plist) créés par l'installation du client Configuration Manager.
>   - Le contenu du dossier /Library/Application Support/Microsoft/CCM/Logs.
>
> Les informations recueillies par le programme CmDiagnostics sont ajoutées à un fichier zip enregistré sur le bureau de l'ordinateur et nommé `cmdiag-<hostname>-<datetime>.zip`.

## Utiliser une demande de certificat et une méthode d'installation indépendantes de Configuration Manager

Tout d'abord, effectuez ces tâches spécifiques à partir de Préparer le déploiement du logiciel client pour ordinateurs Mac :

1. Déployer un certificat de serveur web sur les serveurs de système de site
2. Déployer un certificat d'authentification client sur les serveurs de système de site
3. Configurer le point de gestion et le point de distribution
4. Facultatif : Installer le point Reporting Services

Effectuez ensuite ces tâches :

1. Télécharger les fichiers sources du client pour les ordinateurs Mac.
2. Utilisez les instructions qui accompagnent la méthode de déploiement de certificat choisie pour demander et installer le certificat client sur l'ordinateur Mac.
3. Accédez au dossier dans lequel vous avez extrait le contenu du fichier macclient.dmg, téléchargé depuis le Centre de téléchargement Microsoft.
4. Entrez la ligne de commande suivante : **sudo ./ccmsetup -MP <nom_de_domaine_complet_Internet_du_point_de_gestion> -SubjectName <valeur_objet_certificat>**. La valeur de l'objet Certificat est sensible à la casse, vous devez l'entrer exactement telle qu'elle apparaît dans les détails du certificat.

   Exemple : si le nom de domaine complet Internet dans les propriétés du système de site est **server03.contoso.com** et que le certificat client Mac porte le nom de domaine complet

**mac12.contoso.com** comme nom commun dans l'objet certificat, tapez : **sudo ./ccmsetup -MP server03.contoso.com -SubjectName mac12.contoso.com**

5. Patientez jusqu'à l'affichage du message d' **installation terminée** , puis redémarrez l'ordinateur Mac.
6. Pour vérifier que Configuration Manager peut accéder à ce certificat, sur l'ordinateur Mac, ouvrez une fenêtre de terminal et apportez les modifications suivantes :

   a. Entrez la commande **sudo /Applications/Utilities/Keychain\ Access.app/Contents/MacOS/Keychain\ Access**

   b. Dans la boîte de dialogue **Trousseau d'accès**, dans la zone **Trousseau**, choisissez **Système**, puis dans la zone **Catégorie**, choisissez **Clés**.

   c. Développez les clés pour afficher les certificats clients. Lorsque vous avez identifié le certificat avec une clé privée que vous venez d'installer, double-cliquez sur la clé.

   d. Sous l'onglet **Contrôle d'accès**, choisissez **Confirmer avant d'autoriser l'accès**.

   e. Accédez à **/Library/Application Support/Microsoft/CCM**, sélectionnez **CCMClient**, puis choisissez **Ajouter**.

   f. Choisissez **Enregistrer les modifications** et fermez la boîte de dialogue **Trousseau d'accès**.
7. Si vous disposez de plusieurs certificats qui contiennent la même valeur d'objet, vous devez spécifier le numéro de série du certificat pour identifier le certificat que vous voulez utiliser pour le client Configuration Manager. Pour ce faire, utilisez la commande suivante : **sudo defaults write com.microsoft.ccmclient SerialNumber -data "<numéro_série>"**.

   Exemple : **sudo defaults write com.microsoft.ccmclient SerialNumber -data "17D4391A00000003DB"**

   Vérifiez que l'installation du client a abouti en ouvrant l'élément **Configuration Manager** dans les **Préférences système** de l'ordinateur Mac. Vous pouvez également mettre à jour et afficher le regroupement **Tous les systèmes** pour vérifier que l'ordinateur Mac figure désormais dans ce regroupement comme client géré.

## Renouvellement du certificat client Mac

Utilisez la procédure suivante avant de renouveler le certificat d'ordinateur sur les ordinateurs Mac.

Cette procédure supprime l'ID SMS qui est requis par le client pour utiliser un certificat nouveau ou renouvelé sur l'ordinateur Mac.

> **IMPORTANT**
> Lorsque vous supprimez et remplacez l'ID SMS client, tout historique client stocké, tel que l'inventaire, est supprimé après la suppression du client de la console Configuration Manager.

**Pour renouveler le certificat client Mac**

1. Créez et remplissez un regroupement d'appareils pour les ordinateurs Mac qui doivent renouveler les certificats d'ordinateur.
2. Dans l'espace de travail **Ressources et compatibilité** , démarrez l' **Assistant Création d'élément de configuration**.
3. Sur la page **Général** de l'Assistant, spécifiez les informations suivantes :

   - **Nom :Supprimer l'ID SMS pour Mac**

- **Type :Mac OS X**

4. Sur la page **Plateformes prises en charge** de l'Assistant, assurez-vous que toutes les versions de Mac OS X sont sélectionnées.
5. Sur la page **Paramètres** de l'Assistant, cliquez sur **Nouveau** , puis dans la boîte de dialogue **Créer un paramètre** , spécifiez les informations suivantes :
   - **Nom :Supprimer l'ID SMS pour Mac**
   - **Type de paramètre :Script**
   - **Type de données :Chaîne**
6. Dans la boîte de dialogue **Créer un paramètre** , sous **Script de découverte**, cliquez sur **Ajouter un script** pour définir un script de découverte des ordinateurs Mac configurés avec un ID SMS.
7. Dans la boîte de dialogue **Modifier un script de découverte** , entrez le script Shell suivant :

   ```
   defaults read com.microsoft.ccmclient SMSID
   ```

8. Choisissez **OK** pour fermer la boîte de dialogue **Modifier un script de découverte**.
9. Dans la boîte de dialogue **Créer un paramètre**, sous **Script de correction (facultatif)**, choisissez **Ajouter un script** pour spécifier un script de suppression du SMSID détecté sur les ordinateurs Mac.
10. Dans la boîte de dialogue **Créer un script de correction** , entrez le script Shell suivant :

    ```
    defaults delete com.microsoft.ccmclient SMSID
    ```

11. Choisissez **OK** pour fermer la boîte de dialogue **Créer un script de correction**.
12. Dans la page **Règles de compatibilité** de l'Assistant, choisissez **Nouveau**, puis dans la boîte de dialogue **Créer une règle**, spécifiez les informations suivantes :
    - **Nom :Supprimer l'ID SMS pour Mac**
    - **Paramètre sélectionné :** Choisissez **Parcourir**, puis sélectionnez le script de découverte que vous avez spécifié précédemment.
    - Dans **les valeurs suivantes** , entrez **la paire domaine/par défaut (com.microsoft.ccmclient, ID SMS) n'existe pas**.
    - Activez l'option **Exécuter le script de correction spécifié lorsque ce paramètre n'est pas compatible**.
13. Effectuez toutes les étapes de l'Assistant Création d'élément de configuration.
14. Créez une ligne de base de configuration contenant l'élément de configuration que vous venez de créer et déployez-la sur le regroupement de périphériques créé à l'étape 1.

    Pour plus d'informations sur la création et le déploiement de bases de référence de configuration, consultez Comment créer des bases de référence de configuration dans System Center Configuration Manager.
15. Après avoir installé un nouveau certificat sur les ordinateurs Mac sur lesquels l'ID SMS a été supprimé, exécutez la commande suivante pour configurer le client de sorte à utiliser le nouveau certificat :

```
sudo defaults write com.microsoft.ccmclient SubjectName -string <Subject_Name_of_New_Certificate>
```

16. Si vous disposez de plusieurs certificats qui contiennent la même valeur d'objet, vous devez spécifier le numéro de série du certificat pour identifier le certificat que vous voulez utiliser pour le client Configuration Manager. Pour ce faire, utilisez la commande suivante : **sudo defaults write com.microsoft.ccmclient SerialNumber -data "<numéro_série>"**.

    Exemple : **sudo defaults write com.microsoft.ccmclient SerialNumber -data "17D4391A00000003DB"**

17. Redémarrer.

## Voir aussi

Gérer les clients Mac

# Comment affecter des clients à un site dans System Center Configuration Manager

22/06/2018 • 24 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Une fois un client System Center Configuration Manager installé, il doit rejoindre un site principal Configuration Manager avant de pouvoir être géré. Le site qu'un client rejoint est appelé le *site attribué*. Les clients ne peuvent pas être attribués à un site d'administration centrale ou à un site secondaire.

Le processus d'attribution se produit une fois le client installé et détermine le site qui gère l'ordinateur client. Vous avez le choix entre une attribution directe à un site et une attribution automatique de site. Dans ce cas, le client trouve automatiquement un site approprié, en fonction de son emplacement réseau actuel, ou un site de secours qui a été configuré pour la hiérarchie.

Quand vous installez le client d'appareil mobile lors de l'inscription de Configuration Manager, l'appareil est toujours attribué automatiquement à un site. Quand vous installez le client sur un ordinateur, vous pouvez choisir d'attribuer ou non le client à un site. Toutefois, lorsque le client est installé mais pas attribué, client n'est pas géré tant que l'attribution de site n'a pas été menée à bien.

> **NOTE**
> Attribuez toujours des clients à des sites exécutant la même version de Configuration Manager. Évitez d'attribuer un client Configuration Manager d'une version plus récente à un site d'une version antérieure. Si nécessaire, mettez à jour le site principal vers la même version de Configuration Manager que vous utilisez pour les clients.

Une fois le client attribué à un site, il y reste associé même dans les cas où il modifie son adresse IP ou se déplace vers un autre site. Seul un administrateur peut attribuer manuellement le client à un autre site ou supprimer l'attribution du client.

> **WARNING**
> Le client ne reste pas attribué à un site si vous attribuez ce client sur un appareil Windows Embedded et que les filtres d'écriture sont activés, ce qui constitue une exception. Si vous ne désactivez pas les filtres d'écriture avant d'attribuer le client, celui-ci retrouve son état d'attribution de site initial au prochain redémarrage de l'appareil.
>
> Par exemple, si le client est configuré pour l'attribution automatique de site, il fera l'objet d'une réattribution au démarrage et pourra être attribué à un site différent. Si le client n'est pas configuré pour l'attribution automatique de site, mais qu'il nécessite une attribution de site manuelle, vous devez le réattribuer manuellement après le démarrage pour pouvoir le gérer à nouveau à l'aide de Configuration Manager.
>
> Pour éviter ce comportement, désactivez les filtres d'écriture avant d'attribuer le client sur des appareils embarqués, puis activez-les après avoir vérifié que l'attribution de site a abouti.

En cas d'échec de l'attribution du client, le logiciel client reste installé, mais il n'est pas géré. Un client est considéré non géré lorsqu'il est installé mais pas attribué à un site ou lorsqu'il est attribué à un site, mais ne peut pas communiquer avec un point de gestion.

## Utilisation de l'attribution manuelle de site pour les ordinateurs

Vous pouvez attribuer des ordinateurs clients à un site manuellement en employant l'une des deux méthodes

suivantes :

- Utilisez une propriété d'installation du client qui spécifie le code de site.
- Dans le panneau de configuration, dans **Configuration Manager**, indiquez le code de site.

> **NOTE**
> Si vous attribuez manuellement un ordinateur client à un code de site Configuration Manager qui n'existe pas, l'attribution de site échoue.

## Utilisation de l'attribution automatique de site pour les ordinateurs

L'attribution automatique de site peut se produire lors du déploiement du client ou lorsque vous cliquez sur **Rechercher un site** sous l'onglet **Avancé** des **Propriétés du Configuration Manager** dans le panneau de configuration. Le client Configuration Manager compare son propre emplacement réseau avec les limites qui sont configurées dans la hiérarchie Configuration Manager. Lorsque l'emplacement réseau du client se situe dans un groupe de limites qui est activé pour l'attribution de site ou lorsque la hiérarchie est configurée pour un site de secours, le client est automatiquement affecté à ce site sans que vous deviez spécifier un code de site.

Vous pouvez configurer des limites à l'aide de l'un ou de plusieurs des éléments suivants :

- Sous-réseau IP
- Site Active Directory
- Préfixe IP v6
- Plage d'adresses IP

> **NOTE**
> Si un client Configuration Manager a plusieurs cartes réseau et donc plusieurs adresses IP, l'adresse IP utilisée pour évaluer l'attribution de site client est attribuée de façon aléatoire.

Pour plus d'informations sur la configuration de groupes de limites pour l'attribution de site et sur la configuration d'un site de secours pour l'attribution automatique de site, consultez Définir des limites de site et les groupes de limites pour System Center Configuration Manager.

Les clients Configuration Manager qui utilisent l'attribution automatique de site tentent de trouver les groupes de limites qui sont publiés dans les services de domaine Active Directory. En cas d'échec (par exemple, le schéma Active Directory n'est pas étendu pour Configuration Manager ou les clients sont des ordinateurs de groupes de travail), les clients peuvent obtenir les informations sur les groupes de limites à partir d'un point de gestion.

Vous pouvez spécifier un point de gestion pour les ordinateurs clients lorsqu'ils sont installés, ou les clients peuvent localiser un point de gestion à l'aide de la publication DNS ou WINS.

Si le client ne trouve pas de site associé à un groupe de limites qui contient son emplacement réseau et que la hiérarchie ne dispose pas d'un site de secours, le client essaie de nouveau toutes les 10 minutes jusqu'à ce qu'il puisse être attribué à un site.

Les ordinateurs clients Configuration Manager ne peuvent pas être attribués automatiquement à un site si l'un des scénarios suivants s'applique et doivent être attribués manuellement :

- Ils sont actuellement attribués à un site.
- Ils se trouvent sur Internet ou sont configurés comme des clients Internet uniquement.

- Leur emplacement réseau ne tombe pas dans l'un des groupes de limites configurés dans la hiérarchie de Configuration Manager et il n'existe aucun site de secours pour la hiérarchie.

## Fin de l'attribution de site par la vérification de la compatibilité du site

Dès lors qu'un client a trouvé le site auquel il est attribué, la version et le système d'exploitation du client sont vérifiés pour s'assurer qu'un site Configuration Manager peut le gérer. Par exemple, Configuration Manager ne peut pas gérer les clients Configuration Manager 2007, System Center 2012 Configuration Manager ou les clients qui exécutent Windows 2000.

L'attribution de site échoue si vous attribuez un client Windows 2000 à un site Configuration Manager. Quand vous attribuez un client Configuration Manager 2007 ou un client System Center 2012 Configuration Manager à un site Configuration Manager (Current Branch), l'attribution de site parvient à prendre en charge la mise à niveau automatique du client. Toutefois, tant qu'un client de génération antérieure n'est pas mis à niveau vers un client Configuration Manager (Current Branch), Configuration Manager ne peut pas gérer ce client en utilisant des paramètres, applications ou mises à jour logicielles du client.

> **NOTE**
> Pour prendre en charge l'attribution de site d'un site Configuration Manager 2007 ou d'un client System Center 2012 Configuration Manager à un site Configuration Manager (Current Branch), vous devez configurer la mise à niveau automatique des clients pour la hiérarchie. Pour plus d'informations, consultez Comment mettre à niveau les clients pour les ordinateurs Windows dans System Center Configuration Manager.

Configuration Manager vérifie également que vous avez attribué le client Configuration Manager (Current Branch) à un site qui le prend en charge. Les scénarios suivants peuvent se produire durant une migration à partir de versions précédentes de Configuration Manager.

- Scénario : Vous avez utilisé une attribution automatique de site et vos limites chevauchent celles définies dans une version précédente de Configuration Manager.

  Dans ce cas, le client essaie automatiquement de trouver un site Configuration Manager (Current Branch).

  Le client vérifie d'abord les services de domaine Active Directory et, s'il trouve un site Configuration Manager (Current Branch) publié, l'attribution de site réussit. En cas d'échec (par exemple le site Configuration Manager n'est pas publié ou l'ordinateur est un client de groupe de travail), le client recherche les informations de site sur le point de gestion qui lui est attribué.

  > **NOTE**
  > Vous pouvez attribuer un point de gestion au client lors de l'installation de celui-ci en utilisant la propriété Client.msi **SMSMP=<nom_serveur**.

  Si ces deux méthodes échouent, l'attribution de site échoue et vous devez attribuer le client manuellement.

- Scénario : Vous avez attribué le client Configuration Manager (Current Branch) en utilisant un code de site spécifique au lieu d'utiliser l'attribution automatique de site, et spécifié par erreur un code de site pour une version de Configuration Manager antérieure à System Center 2012 R2 Configuration Manager.

  Dans ce cas, l'attribution de site échoue et vous devez réattribuer manuellement le client à un site Configuration Manager (Current Branch).

  La vérification de la compatibilité du site requiert l'une des conditions suivantes :

- Le client peut accéder aux informations de site publiées dans les services de domaine Active Directory.

- Le client peut communiquer avec un point de gestion du site.

  Si la vérification de la compatibilité du site échoue avant la fin de l'opération, l'attribution de site échoue et le client reste non géré, jusqu'à ce que la vérification de la compatibilité du site se termine sans problème lors de l'exécution suivante.

  La seule exception à cette vérification de la compatibilité du site survient lorsqu'un client est configuré pour un point de gestion Internet. Dans ce cas, aucune vérification de la compatibilité du site n'est effectuée. Si vous attribuez des clients à un site qui contient des systèmes de site Internet et que vous spécifiez un point de gestion Internet, assurez-vous d'attribuer le client au site approprié. Si vous attribuez le client à un site Configuration Manager 2007, un site System Center 2012 Configuration Manager ou un site Configuration Manager qui n'a pas de rôle de système de site basé sur Internet, le client n'est pas géré.

## Localisation de points de gestion

Une fois qu'un client est correctement attribué à un site, il localise un point de gestion dans le site.

Les ordinateurs clients téléchargent la liste des points de gestion auxquels ils peuvent se connecter dans le site. Cette opération se produit à chaque redémarrage du client, c'est-à-dire toutes les 25 heures, ou quand le client détecte un changement sur le réseau (par exemple, déconnexion et reconnexion de l'ordinateur sur le réseau ou attribution d'une nouvelle adresse IP). La liste répertorie les points de gestion présents sur l'intranet et indique s'ils acceptent les connexions client via HTTP ou HTTPS. Lorsque l'ordinateur client est sur Internet et qu'il ne dispose pas encore d'une liste de points de gestion, il se connecte au point de gestion Internet spécifié pour obtenir une liste de points de gestion. Lorsque le client dispose d'une liste de points de gestion pour son site attribué, il en sélectionne un auquel se connecter :

- Lorsque le client se trouve sur l'intranet et qu'il possède un certificat PKI valide qu'il peut utiliser, il choisit les points de gestion HTTPS avant les points de gestion HTTP. Il localise ensuite le point de gestion le plus proche, en fonction de son appartenance à une forêt.
- Quand le client se trouve sur Internet, il choisit de façon aléatoire l'un des points de gestion basés sur Internet.

Les clients d'appareil mobile inscrits par Configuration Manager se connectent à un seul point de gestion du site auquel ils sont attribués et ne se connectent jamais aux points de gestion de sites secondaires. Ces clients se connectent toujours via HTTPS et le point de gestion doit être configuré pour accepter les connexions client sur Internet. Quand le site principal propose plusieurs points de gestion pour les clients d'appareil mobile, Configuration Manager en choisit un de façon aléatoire pendant l'attribution et le client d'appareil mobile continue d'utiliser le même point de gestion.

Une fois que le client a téléchargé la stratégie du client depuis un point de gestion du site, il devient un client géré.

## Téléchargement des paramètres du site

Une fois que le site est attribué et que le client a trouvé un point de gestion, un ordinateur client utilisant les services de domaine Active Directory pour la vérification de sa compatibilité avec le site télécharge les paramètres client du site auquel il est attribué. Ces paramètres incluent les critères de sélection de certificat du client, s'il faut utiliser une liste de révocation de certificat et les numéros de port de demande de client. Le client continue de vérifier régulièrement ces paramètres.

Lorsque les ordinateurs clients ne peuvent pas obtenir les paramètres du site auprès des services de domaine Active Directory, ils les téléchargent à partir de leur point de gestion. Les ordinateurs clients peuvent également obtenir les paramètres du site quand ils sont installés à l'aide de l'installation Push du client, ou vous pouvez les spécifier manuellement à l'aide de CCMSetup.exe et des propriétés d'installation du client. Pour plus d'informations sur les propriétés d'installation du client, consultez À propos des propriétés d'installation du client

dans System Center Configuration Manager.

## Téléchargement des paramètres du client

Tous les clients téléchargent la stratégie de paramètres client par défaut, ainsi que toute stratégie de paramètres client personnalisée. Le Centre logiciel repose sur ces stratégies de configuration du client pour les ordinateurs Windows et informe les utilisateurs que le Centre logiciel ne peut pas fonctionner correctement tant que ces informations de configuration ne sont pas téléchargées. En fonction des paramètres client configurés, le téléchargement initial des paramètres client peut prendre un certain temps et certaines tâches de gestion risquent de ne pas s'exécuter tant que ce processus n'est pas terminé.

## Vérification de l'attribution de site

Vous pouvez vérifier que l'attribution de site a abouti en employant l'une des méthodes suivantes :

- Pour les clients sur ordinateurs Windows, utilisez Configuration Manager dans le Panneau de configuration et vérifiez que le code de site est correctement affiché sous l'onglet **Site**.
- Pour les ordinateurs clients, dans l'espace de travail **Actifs et Conformité** > nœud **Appareils**, vérifiez que l'ordinateur affiche **Oui** pour la colonne **Client** et le code de site principal correct pour la colonne **Code de site**.
- Pour les clients d'appareil mobile, dans l'espace de travail **Ressources et compatibilité** , utilisez le nœud **Tous les périphériques mobiles** pour vérifier que l'appareil mobile affiche **Oui** pour la colonne **Client** et le code de site principal correct pour la colonne **Code de site** .
- Utilisez les rapports pour l'attribution de client et l'inscription d'appareil mobile.
- Pour les ordinateurs clients, utilisez le fichier LocationServices.log sur le client.

## Itinérance vers d'autres sites

Lorsque des ordinateurs clients de l'intranet sont attribués à un site principal, mais que leur emplacement réseau change au profit d'un groupe de limites configuré pour un autre site, ils ont été déplacés vers un autre site (itinérance). Lorsque ce site est un site secondaire du site auquel ils sont attribués, les clients peuvent utiliser un point de gestion du site secondaire pour télécharger la stratégie client et les données client, ce qui évite l'envoi de ces données via un réseau potentiellement lent. Toutefois, si ces clients itinérants sont déplacés dans les limites d'un autre site principal ou d'un site secondaire qui n'est pas un site enfant du site auquel ils sont attribués, ces clients utilisent toujours un point de gestion du site auquel ils sont attribués pour télécharger la stratégie client et les données vers leur site.

Ces ordinateurs clients itinérants qui sont déplacés vers d'autres sites (tous les sites principaux et tous les sites secondaires) peuvent toujours utiliser les points de gestion d'autres sites pour les demandes d'emplacement du contenu. Les points de gestion du site actuel peuvent fournir aux clients une liste des points de distribution qui disposent du contenu demandé par les clients.

Pour les ordinateurs clients configurés pour être gérés uniquement par le biais d'Internet et pour les appareils mobiles et les ordinateurs Mac inscrits par Configuration Manager, ces clients communiquent uniquement avec les points de gestion du site auxquels ils sont attribués. Ces clients ne communiquent jamais avec les points de gestion de sites secondaires ou d'autres sites principaux.

# Comment configurer l'état du client dans System Center Configuration Manager

22/06/2018 • 8 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Afin de surveiller l'état du client System Center Configuration Manager et de corriger les problèmes rencontrés, vous devez configurer votre site pour spécifier les paramètres qui sont utilisés pour marquer des clients comme inactifs et configurer des options pour vous avertir si l'activité du client passe sous un seuil spécifié. Il est également possible de désactiver la résolution automatique par les ordinateurs des problèmes rencontrés par l'état du client.

## Pour configurer l'état du client

1. Dans la console Configuration Manager, cliquez sur **Surveillance**.
2. Dans l'espace de travail **Surveillance** , cliquez sur **État du client**, puis dans l'onglet **Accueil** , dans le groupe **État du client** , cliquez sur **Paramètres d'état du client**.
3. Dans la boîte de dialogue **Propriétés des paramètres d'état des clients** , spécifiez les valeurs suivantes pour déterminer l'activité du client :

   > **NOTE**
   > Si aucun des paramètres n'est satisfait, le client sera marqué comme inactif.

   - **Demandes de stratégie client lors des jours suivants :** Spécifiez le nombre de jours depuis qu'un client a demandé une stratégie. La valeur par défaut est **7** jours.
   - **Découverte par pulsations d'inventaire lors des jours suivants :** Spécifiez le nombre de jours depuis que l'ordinateur client a envoyé un enregistrement de découverte par pulsations d'inventaire à la base de données du site. La valeur par défaut est **7** jours.
   - **Inventaire matériel lors des jours suivants :** Spécifiez le nombre de jours depuis que l'ordinateur client a envoyé un enregistrement d'inventaire matériel à la base de données du site. La valeur par défaut est **7** jours.
   - **Inventaire des logiciels lors des jours suivants :** Spécifiez le nombre de jours depuis que l'ordinateur client a envoyé un enregistrement d'inventaire logiciel à la base de données du site. La valeur par défaut est **7** jours.
   - **Messages d'état lors des jours suivants :** Spécifiez le nombre de jours depuis que l'ordinateur client a envoyé des messages d'état à la base de données du site. La valeur par défaut est **7** jours.
4. Dans la boîte de dialogue **Propriétés des paramètres d'état des clients** , spécifiez la valeur suivante pour déterminer la durée pendant laquelle les données de l'historique d'état du client sont conservées :
   - **Conserver l'historique de l'état du client pendant le nombre de jours suivant :** Spécifiez la durée pendant laquelle vous voulez que l'historique de l'état du client soit conservé dans la base de données du site. La valeur par défaut est **31** jours.
5. Cliquez sur **OK** pour enregistrer les propriétés et fermer la boîte de dialogue **Propriétés des paramètres**

**d'état des clients** .

## Pour configurer le calendrier de l'état du client

1. Dans la console Configuration Manager, cliquez sur **Surveillance**.
2. Dans l'espace de travail **Surveillance** , cliquez sur **État du client**, puis dans l'onglet **Accueil** , dans le groupe **État du client** , cliquez sur **Planifier la mise à jour de l'état des clients**.
3. Dans la boîte de dialogue **Planifier la mise à jour de l'état des clients** , configurez la fréquence à laquelle vous souhaitez que l'état des clients soit mis à jour, puis cliquez sur OK.

> **NOTE**
> Lorsque vous modifiez la planification des mises à jour de l'état des clients, la mise à jour ne prend effet que lors de la mise à jour de l'état des clients suivante (selon le calendrier précédemment configuré).

## Pour configurer des alertes liées à l'état du client

1. Dans la console Configuration Manager, cliquez sur **Ressources et Conformité**.
2. Dans l'espace de travail **Ressources et Conformité** , cliquez sur **Regroupements de périphériques**.
3. Dans la liste **Regroupements de périphériques** , sélectionnez le regroupement pour lequel vous souhaitez configurer des alertes, puis cliquez sur **Propriétés** dans l'onglet **Accueil** , du groupe **Propriétés**.

> **NOTE**
> Vous ne pouvez pas configurer d'alertes pour les regroupements d'utilisateurs.

4. Sous l'onglet **Alertes** de la boîte de dialogue *Propriétés de <Nom du regroupement>*, cliquez sur **Ajouter**.

> **NOTE**
> L'onglet **Alertes** n'est visible que si le rôle de sécurité auquel vous êtes associé dispose d'autorisations pour les alertes.

5. Dans la boîte de dialogue **Ajouter de nouvelles alertes de regroupement** , choisissez les alertes que vous souhaitez générer lorsque les seuils d'état du client passent sous une valeur spécifique, puis cliquez sur **OK**.
6. Dans la liste **Conditions** de l'onglet **Alertes** , sélectionnez chaque alerte relative à l'état du client, puis spécifiez les informations suivantes.
   - **Nom d'alerte** – Acceptez le nom par défaut ou entrez un nouveau nom pour l'alerte.
   - **Gravité d'alerte** – Dans la liste déroulante, choisissez la gravité d'alerte qui sera affichée dans la console Configuration Manager.
   - **Déclencher l'alerte** – Spécifiez le pourcentage seuil pour l'alerte.
7. Cliquez sur **OK** pour fermer la boîte de dialogue *Propriétés de <nom_regroupement>*.

## Pour exclure des ordinateurs de la résolution automatique

1. Ouvrez l'éditeur du Registre sur l'ordinateur client pour lequel vous souhaitez désactiver la résolution automatique.

   > **WARNING**
   > Une utilisation incorrecte de l'Éditeur du Registre peut éventuellement provoquer de graves problèmes, lesquels nécessitent parfois la réinstallation complète du système d'exploitation. Microsoft ne garantit pas la résolution des erreurs résultant d'une utilisation incorrecte de l'Éditeur du Registre. Les opérations exécutées dans l'Éditeur du Registre le sont à vos propres risques.

2. Accédez à **HKEY_LOCAL_MACHINE\Software\Microsoft\CCM\CcmEval\NotifyOnly**.

3. Entrez l'une des valeurs suivantes pour cette clé de Registre :

   - **Vrai** – L'ordinateur client ne résoudra pas automatiquement les problèmes détectés. Vous serez toutefois alerté dans l'espace de travail **Surveillance** des problèmes survenus pour ce client.
   - **Faux** – L'ordinateur client résoudra automatiquement les problèmes détectés et vous serez alerté dans l'espace de travail **Surveillance**. Il s'agit du paramètre par défaut.

4. Fermez l'éditeur du Registre.

   Vous pouvez également installer des clients à l'aide de la propriété d'installation CCMSetup **NotifyOnly** pour les exclure de la résolution automatique. Pour plus d'informations sur cette propriété d'installation du client, consultez À propos des propriétés d'installation du client dans System Center Configuration Manager.

# Guide pratique pour surveiller l'état de déploiement des clients dans System Center Configuration Manager

22/06/2018 • 4 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Le déploiement de clients sur votre site prend du temps et certaines installations ne réussissent pas dès la première fois. La console System Center Configuration Manager permet de garder un œil sur les déploiements de clients au sein d'un regroupement en signalant l'état de déploiement des clients en temps réel.

> **NOTE**
> Le moyen le plus efficace et le plus fiable de surveiller le déploiement des clients est d'utiliser la console Configuration Manager (comme décrit dans cet article). La section **État du client** de l'espace de travail **Analyse** dans la console indique l'état du déploiement des clients avec précision et en temps réel. Vous pouvez surveiller les déploiements de client avec d'autres outils, tels le Gestionnaire de serveur dans Windows Server ou System Center Operations Manager, mais vous risquez de recevoir des alarmes en relation avec l'activité normale d'installation de clients. En raison de la façon dont le programme d'installation client (CCMSetup.exe) s'exécute dans différents environnements, ces autres outils peuvent générer de faux avertissements ou alarmes ne reflétant pas fidèlement l'état de déploiement des clients.

Dans l'espace de travail **Analyse** de la console, vous pouvez surveiller les états suivants des déploiements de clients se produisant à l'intérieur d'un regroupement que vous spécifiez :

- conformité
- En cours
- Non conforme
- Échec
- Inconnu

  Configuration Manager génère des rapports sur les déploiements de clients en production ou en pré-production. La console Configuration Manager fournit également un graphique illustrant les déploiements de clients ayant échoué au cours d'une période donnée, pour vous aider à déterminer si les actions que vous exécutez pour résoudre les problèmes de déploiements améliorent le taux de réussite des déploiements au fil du temps.

## Pour analyser les déploiements de clients

- Dans la console Configuration Manager, cliquez sur **Surveillance** > **État du client**.
- Cliquez sur **Déploiement des clients en production** ou **Déploiement des clients en préproduction**, selon la version du client que vous souhaitez analyser.
- Consulter les graphiques d'état du déploiement des clients et d'échec de déploiement des clients.
- Si vous souhaitez modifier l'étendue du rapport, cliquez sur **Parcourir...**, puis choisissez un autre regroupement.

Pour en savoir plus sur les déploiements de clients en préproduction, consultez Comment tester les mises à niveau du client dans un regroupement de préproduction dans System Center Configuration Manager.

> **NOTE**
>
> L'état du déploiement sur les ordinateurs hébergeant des rôles de système de site dans un regroupement de préproduction peut être signalé comme **Non conforme**, même quand le client a été correctement déployé. Lors de la promotion du client en production, l'état du déploiement est correctement signalé.

Pour analyser l'état des clients déployés, consultez Comment surveiller les clients dans System Center Configuration Manager

Vous pouvez utiliser des rapports Configuration Manager pour obtenir un complément d'informations sur l'état des clients de votre site. Pour plus d'informations sur la façon d'exécuter des rapports, consultez Génération de rapports dans System Center Configuration Manager.

# Surveiller et gérer les clients dans System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

System Center Configuration Manager (également appelé ConfigMgr ou SCCM) propose plusieurs manières de surveiller et de gérer le logiciel client une fois celui-ci déployé sur les ordinateurs et les appareils de votre organisation. Vous pouvez surveiller les clients pour vérifier leur état et, dans certains cas, Configuration Manager peut effectuer des corrections automatiques en fonction du problème détecté. La console Configuration Manager offre aussi différentes manières de gérer les clients pour chaque appareil ou regroupement d'appareils.

Consultez les rubriques suivantes pour découvrir comment surveiller et gérer les clients, et comment obtenir des détails supplémentaires pour surveiller et gérer les clients pour les serveurs Linux et UNIX :

- Guide pratique pour surveiller les clients dans System Center Configuration Manager
- Guide pratique pour surveiller les clients pour des serveurs Linux et UNIX dans System Center Configuration Manager
- Guide pratique pour gérer les clients dans System Center Configuration Manager
- Guide pratique pour gérer les clients pour des serveurs Linux et UNIX dans System Center Configuration Manager

# Guide pratique pour surveiller des clients dans System Center Configuration Manager

22/06/2018 • 14 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Une fois l'application cliente System Center Configuration Manager installée sur les ordinateurs et appareils Windows de votre site, vous pouvez surveiller leur intégrité et leur activité dans la console Configuration Manager.

## À propos du statut du client

Configuration Manager présente les types d'informations suivants sous forme d'état du client :

- **État en ligne du client** : à compter de la version 1602 de Configuration Manager, cet état indique si l'ordinateur est en ligne ou non. Un ordinateur est considéré comme étant en ligne s'il est connecté au point de gestion qui lui est affecté. Pour indiquer que le client est en ligne, il envoie des messages de type ping au point de gestion. Si le point de gestion n'a pas reçu de message après environ 5 minutes, le client est considéré comme étant hors connexion.
- **Activité du client** : cet état indique si le client a été activement en contact avec Configuration Manager au cours des 7 derniers jours. Si le client n'a pas demandé de mise à jour de la stratégie, a envoyé un message de pulsation, ou a envoyé un inventaire matériel dans les 7 jours, il est considéré comme inactif.
- **Intégrité du client** : cet état indique la réussite de l'évaluation périodique de l'exécution du client Configuration Manager sur l'ordinateur. L'évaluation vérifie l'ordinateur et peut corriger certains problèmes détectés. Pour plus d'informations, consultez Vérifications et corrections effectuées par la fonction d'intégrité du client.

  Sur les ordinateurs qui exécutent Windows 7, l'intégrité du client s'exécute en tant que tâche planifiée. Sur les systèmes d'exploitation ultérieurs, l'intégrité du client s'exécute automatiquement pendant la fenêtre de maintenance de Windows.

  Vous pouvez configurer la mise à jour de manière à ne pas l'exécuter sur des ordinateurs spécifiques, par exemple, sur un serveur essentiel pour l'entreprise. En outre, si vous souhaitez évaluer d'autres éléments, vous pouvez utiliser les paramètres de compatibilité de Configuration Manager pour fournir une solution complète de surveillance de l'intégrité, de l'activité et de la conformité globales des ordinateurs de votre organisation. Pour plus d'informations sur les paramètres de compatibilité, consultez Planifier et configurer les paramètres de compatibilité dans System Center Configuration Manager.

## Surveiller le statut de clients individuels

1. Dans la console Configuration Manager, cliquez sur **Ressources et Conformité** > **Appareils** ou choisissez un regroupement sous **Regroupements d'appareils**.

   À compter de la version 1602 de Configuration Manager, les icônes au début de chaque ligne indiquent le statut de connexion de l'appareil :

| | |
|---|---|
|  | L'appareil est en ligne. |

| | |
|---|---|
| | |
|  | L'appareil est hors connexion. |
|  | Le statut de connexion est inconnu. |
|  | Le client n'est pas installé sur l'appareil. |

2. Pour obtenir un statut de connexion plus détaillé, ajoutez les informations de statut de connexion du client à l'affichage du périphérique, en double-cliquant sur l'en-tête de colonne et en cliquant sur les champs de statut de connexion que vous souhaitez ajouter. Les colonnes que vous pouvez ajouter sont les suivantes :

   - **Statut de connexion de l'appareil** indique si le client est actuellement en ligne ou hors connexion. (Il s'agit des mêmes informations que celles fournies par les icônes).
   - **Heure de la dernière connexion** indique à quel moment le statut de connexion du client est passé en ligne.
   - **Heure de la dernière déconnexion** indique à quel moment le statut est passé hors connexion.

3. Cliquez sur un client individuel dans le volet Liste pour voir plus d'informations sur le statut dans le volet Détails, dont des informations sur l'activité du client et l'intégrité du client.

## Surveiller le statut de tous les clients

1. Dans la console Configuration Manager, cliquez sur **Surveillance** > **État du client**. Dans cette page de la console, vous pouvez consulter les statistiques générales relatives à l'activité du client et à l'intégrité du client sur le site. Vous pouvez également modifier l'étendue des informations en choisissant un autre regroupement.

2. Pour explorer en détail les statistiques renvoyées, cliquez sur le nom des informations communiquées (par exemple, **Clients actifs ayant réussi la vérification ou sans résultats**) et passez en revue les informations sur les différents clients.

3. Cliquez sur **Activité des clients** pour afficher des graphiques illustrant l'activité des clients sur votre site Configuration Manager.

4. Cliquez sur **Intégrité du client** pour afficher des graphiques illustrant l'état de vérification de l'intégrité des clients de votre site Configuration Manager.

   Vous pouvez configurer des alertes pour vous avertir lorsque les résultats de l'intégrité des clients ou l'activité des clients passent au-dessous d'un pourcentage de clients spécifié dans un enregistrement ou lorsque la mise à jour échoue sur un pourcentage de clients spécifié. Pour plus d'informations sur la configuration de l'état du client, consultez Comment configurer l'état du client dans System Center Configuration Manager.

## Vérifications et corrections effectuées par la fonction d'intégrité du client

Les vérifications et corrections suivantes peuvent être effectuées par la fonction d'intégrité du client.

| INTÉGRITÉ DU CLIENT | ACTION CORRECTIVE | PLUS D'INFORMATIONS |
|---|---|---|
| Vérifier que la fonction d'intégrité du client a été exécutée récemment | Exécuter l'intégrité du client | Vérifie que l'intégrité du client a été exécutée au moins une fois au cours des trois derniers jours. |
| Vérifier que la configuration requise du client est installée | Installer la configuration requise du client | Vérifie que la configuration requise du client est installée. Lit le fichier ccmsetup.xml dans le dossier d'installation client pour découvrir les composants requis. |
| Test d'intégrité de l'espace de stockage WMI | Réinstaller le client Configuration Manager | Vérifie que les entrées de client Configuration Manager sont présentes dans WMI. |
| Vérifier que le service client est en cours d'exécution | Démarrer le service client (Hôte de l'agent SMS) | Aucune information supplémentaire |
| Test du récepteur d'événements WMI. | Redémarrer le service client | Vérifier si le récepteur d'événements WMI lié à Configuration Manager est perdu |
| Vérifier l'existence du service WMI (Windows Management Instrumentation) | Aucune correction | Aucune information supplémentaire |
| Vérifier que le client a été installé correctement | Réinstaller le client | Aucune information supplémentaire |
| Test de lecture/d'écriture de l'espace de stockage WMI | Réinitialiser le référentiel WMI et réinstaller le client Configuration Manager | La correction de cette intégrité du client est effectuée uniquement sur les ordinateurs qui exécutent Windows Server 2003, Windows XP (64 bits) ou des versions antérieures. |
| Vérifier que le type de démarrage du service anti-programme malveillant est automatique | Réinitialiser le type de démarrage du service sur automatique | Aucune information supplémentaire |
| Vérifier que le service anti-programme malveillant est en cours d'exécution | Démarrer le service anti-programme malveillant | Aucune information supplémentaire |
| Vérifier que le type de démarrage du service Windows Update est automatique ou manuel | Réinitialiser le type de démarrage du service sur automatique | Aucune information supplémentaire |
| Vérifier que le type de démarrage du service client (Hôte de l'agent SMS) est automatique | Réinitialiser le type de démarrage du service sur automatique | Aucune information supplémentaire |
| Vérifier que le service WMI (Windows Management Instrumentation) est en cours d'exécution | Démarrer le service WMI (Windows Management Instrumentation) | Aucune information supplémentaire |
| Vérifier l'intégrité de la base de données Microsoft SQL CE | Réinstaller le client Configuration Manager | Aucune information supplémentaire |

| INTÉGRITÉ DU CLIENT | ACTION CORRECTIVE | PLUS D'INFORMATIONS |
|---|---|---|
| Test d'intégrité WMI Microsoft Policy Platform | Réparer Microsoft Policy Platform | Aucune information supplémentaire |
| Vérifier que le service Microsoft Policy Platform existe | Réparer Microsoft Policy Platform | Aucune information supplémentaire |
| Vérifier que le type de démarrage du service Microsoft Policy Platform est manuel | Réinitialiser le type de démarrage du service sur manuel | Aucune information supplémentaire |
| Vérifier l'existence du service de transfert intelligent en arrière-plan | Aucune correction | Aucune information supplémentaire |
| Vérifier que le type de démarrage du service de transfert intelligent en arrière-plan est automatique ou manuel | Réinitialiser le type de démarrage du service sur automatique | Aucune information supplémentaire |
| Vérifier que le type de démarrage du service d'inspection du réseau est manuel | Réinitialiser le type de démarrage du service sur manuel, s'il est installé | Aucune information supplémentaire |
| Vérifier que le type de démarrage du service WMI (Windows Management Instrumentation) est automatique | Réinitialiser le type de démarrage du service sur automatique | Aucune information supplémentaire |
| Vérifier que le type de démarrage du service Windows Update sur les ordinateurs Windows 8 est automatique ou manuel | Réinitialiser le type de démarrage du service sur manuel | Aucune information supplémentaire |
| Vérifier l'existence du service client (hôte d'Agent SMS) | Aucune correction | Aucune information supplémentaire |
| Vérifier que le type de démarrage du service de contrôle à distance de Configuration Manager est automatique ou manuel | Réinitialiser le type de démarrage du service sur automatique | Aucune information supplémentaire |
| Vérifier que le service de contrôle à distance de Configuration Manager est en cours d'exécution | Démarrer le service de contrôle à distance | Aucune information supplémentaire |
| Vérifier l'intégrité du fournisseur WMI du client | Redémarrer le service WMI (Windows Management Instrumentation) | La correction de cette intégrité du client est effectuée uniquement sur les ordinateurs qui exécutent Windows Server 2003, Windows XP (64 bits) ou des versions antérieures. |
| Vérifier que le service de proxy de mise en éveil (proxy de mise en éveil ConfigMgr) est en cours d'exécution | Démarrer le service de proxy de mise en éveil ConfigMgr | Cette vérification du client est effectuée uniquement si le paramètre client **Gestion de l'alimentation**: **Autoriser le proxy de mise en éveil** est défini sur **Oui** sur les systèmes d'exploitation clients pris en charge. |

| INTÉGRITÉ DU CLIENT | ACTION CORRECTIVE | PLUS D'INFORMATIONS |
| --- | --- | --- |
| Vérifier que le type de démarrage du service de proxy de mise en éveil (proxy de mise en éveil ConfigMgr) est automatique | Réinitialiser le type de démarrage du service de proxy de mise en éveil ConfigMgr sur automatique | Cette vérification du client est effectuée uniquement si le paramètre client **Gestion de l'alimentation**: **Autoriser le proxy de mise en éveil** est défini sur **Oui** sur les systèmes d'exploitation clients pris en charge. |

## Fichiers journaux de déploiement du client

Pour plus d'informations sur les fichiers journaux utilisés par les opérations de déploiement et de gestion du client, consultez Fichiers journaux dans System Center Configuration Manager.

# Guide pratique pour surveiller des clients dans System Center Configuration Manager

22/06/2018 • 14 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Une fois l'application cliente System Center Configuration Manager installée sur les ordinateurs et appareils Windows de votre site, vous pouvez surveiller leur intégrité et leur activité dans la console Configuration Manager.

## À propos du statut du client

Configuration Manager présente les types d'informations suivants sous forme d'état du client :

- **État en ligne du client** : à compter de la version 1602 de Configuration Manager, cet état indique si l'ordinateur est en ligne ou non. Un ordinateur est considéré comme étant en ligne s'il est connecté au point de gestion qui lui est affecté. Pour indiquer que le client est en ligne, il envoie des messages de type ping au point de gestion. Si le point de gestion n'a pas reçu de message après environ 5 minutes, le client est considéré comme étant hors connexion.
- **Activité du client** : cet état indique si le client a été activement en contact avec Configuration Manager au cours des 7 derniers jours. Si le client n'a pas demandé de mise à jour de la stratégie, a envoyé un message de pulsation, ou a envoyé un inventaire matériel dans les 7 jours, il est considéré comme inactif.
- **Intégrité du client** : cet état indique la réussite de l'évaluation périodique de l'exécution du client Configuration Manager sur l'ordinateur. L'évaluation vérifie l'ordinateur et peut corriger certains problèmes détectés. Pour plus d'informations, consultez Vérifications et corrections effectuées par la fonction d'intégrité du client.

  Sur les ordinateurs qui exécutent Windows 7, l'intégrité du client s'exécute en tant que tâche planifiée. Sur les systèmes d'exploitation ultérieurs, l'intégrité du client s'exécute automatiquement pendant la fenêtre de maintenance de Windows.

  Vous pouvez configurer la mise à jour de manière à ne pas l'exécuter sur des ordinateurs spécifiques, par exemple, sur un serveur essentiel pour l'entreprise. En outre, si vous souhaitez évaluer d'autres éléments, vous pouvez utiliser les paramètres de compatibilité de Configuration Manager pour fournir une solution complète de surveillance de l'intégrité, de l'activité et de la conformité globales des ordinateurs de votre organisation. Pour plus d'informations sur les paramètres de compatibilité, consultez Planifier et configurer les paramètres de compatibilité dans System Center Configuration Manager.

## Surveiller le statut de clients individuels

1. Dans la console Configuration Manager, cliquez sur **Ressources et Conformité** > **Appareils** ou choisissez un regroupement sous **Regroupements d'appareils**.

   À compter de la version 1602 de Configuration Manager, les icônes au début de chaque ligne indiquent le statut de connexion de l'appareil :

| | |
|---|---|
|  | L'appareil est en ligne. |

| | |
|---|---|
|  | L'appareil est hors connexion. |
|  | Le statut de connexion est inconnu. |
|  | Le client n'est pas installé sur l'appareil. |

2. Pour obtenir un statut de connexion plus détaillé, ajoutez les informations de statut de connexion du client à l'affichage du périphérique, en double-cliquant sur l'en-tête de colonne et en cliquant sur les champs de statut de connexion que vous souhaitez ajouter. Les colonnes que vous pouvez ajouter sont les suivantes :

   - **Statut de connexion de l'appareil** indique si le client est actuellement en ligne ou hors connexion. (Il s'agit des mêmes informations que celles fournies par les icônes).
   - **Heure de la dernière connexion** indique à quel moment le statut de connexion du client est passé en ligne.
   - **Heure de la dernière déconnexion** indique à quel moment le statut est passé hors connexion.

3. Cliquez sur un client individuel dans le volet Liste pour voir plus d'informations sur le statut dans le volet Détails, dont des informations sur l'activité du client et l'intégrité du client.

## Surveiller le statut de tous les clients

1. Dans la console Configuration Manager, cliquez sur **Surveillance** > **État du client**. Dans cette page de la console, vous pouvez consulter les statistiques générales relatives à l'activité du client et à l'intégrité du client sur le site. Vous pouvez également modifier l'étendue des informations en choisissant un autre regroupement.

2. Pour explorer en détail les statistiques renvoyées, cliquez sur le nom des informations communiquées (par exemple, **Clients actifs ayant réussi la vérification ou sans résultats**) et passez en revue les informations sur les différents clients.

3. Cliquez sur **Activité des clients** pour afficher des graphiques illustrant l'activité des clients sur votre site Configuration Manager.

4. Cliquez sur **Intégrité du client** pour afficher des graphiques illustrant l'état de vérification de l'intégrité des clients de votre site Configuration Manager.

   Vous pouvez configurer des alertes pour vous avertir lorsque les résultats de l'intégrité des clients ou l'activité des clients passent au-dessous d'un pourcentage de clients spécifié dans un enregistrement ou lorsque la mise à jour échoue sur un pourcentage de clients spécifié. Pour plus d'informations sur la configuration de l'état du client, consultez Comment configurer l'état du client dans System Center Configuration Manager.

## Vérifications et corrections effectuées par la fonction d'intégrité du client

Les vérifications et corrections suivantes peuvent être effectuées par la fonction d'intégrité du client.

| INTÉGRITÉ DU CLIENT | ACTION CORRECTIVE | PLUS D'INFORMATIONS |
|---|---|---|
| Vérifier que la fonction d'intégrité du client a été exécutée récemment | Exécuter l'intégrité du client | Vérifie que l'intégrité du client a été exécutée au moins une fois au cours des trois derniers jours. |
| Vérifier que la configuration requise du client est installée | Installer la configuration requise du client | Vérifie que la configuration requise du client est installée. Lit le fichier ccmsetup.xml dans le dossier d'installation client pour découvrir les composants requis. |
| Test d'intégrité de l'espace de stockage WMI | Réinstaller le client Configuration Manager | Vérifie que les entrées de client Configuration Manager sont présentes dans WMI. |
| Vérifier que le service client est en cours d'exécution | Démarrer le service client (Hôte de l'agent SMS) | Aucune information supplémentaire |
| Test du récepteur d'événements WMI. | Redémarrer le service client | Vérifier si le récepteur d'événements WMI lié à Configuration Manager est perdu |
| Vérifier l'existence du service WMI (Windows Management Instrumentation) | Aucune correction | Aucune information supplémentaire |
| Vérifier que le client a été installé correctement | Réinstaller le client | Aucune information supplémentaire |
| Test de lecture/d'écriture de l'espace de stockage WMI | Réinitialiser le référentiel WMI et réinstaller le client Configuration Manager | La correction de cette intégrité du client est effectuée uniquement sur les ordinateurs qui exécutent Windows Server 2003, Windows XP (64 bits) ou des versions antérieures. |
| Vérifier que le type de démarrage du service anti-programme malveillant est automatique | Réinitialiser le type de démarrage du service sur automatique | Aucune information supplémentaire |
| Vérifier que le service anti-programme malveillant est en cours d'exécution | Démarrer le service anti-programme malveillant | Aucune information supplémentaire |
| Vérifier que le type de démarrage du service Windows Update est automatique ou manuel | Réinitialiser le type de démarrage du service sur automatique | Aucune information supplémentaire |
| Vérifier que le type de démarrage du service client (Hôte de l'agent SMS) est automatique | Réinitialiser le type de démarrage du service sur automatique | Aucune information supplémentaire |
| Vérifier que le service WMI (Windows Management Instrumentation) est en cours d'exécution | Démarrer le service WMI (Windows Management Instrumentation) | Aucune information supplémentaire |
| Vérifier l'intégrité de la base de données Microsoft SQL CE | Réinstaller le client Configuration Manager | Aucune information supplémentaire |

| INTÉGRITÉ DU CLIENT | ACTION CORRECTIVE | PLUS D'INFORMATIONS |
|---|---|---|
| Test d'intégrité WMI Microsoft Policy Platform | Réparer Microsoft Policy Platform | Aucune information supplémentaire |
| Vérifier que le service Microsoft Policy Platform existe | Réparer Microsoft Policy Platform | Aucune information supplémentaire |
| Vérifier que le type de démarrage du service Microsoft Policy Platform est manuel | Réinitialiser le type de démarrage du service sur manuel | Aucune information supplémentaire |
| Vérifier l'existence du service de transfert intelligent en arrière-plan | Aucune correction | Aucune information supplémentaire |
| Vérifier que le type de démarrage du service de transfert intelligent en arrière-plan est automatique ou manuel | Réinitialiser le type de démarrage du service sur automatique | Aucune information supplémentaire |
| Vérifier que le type de démarrage du service d'inspection du réseau est manuel | Réinitialiser le type de démarrage du service sur manuel, s'il est installé | Aucune information supplémentaire |
| Vérifier que le type de démarrage du service WMI (Windows Management Instrumentation) est automatique | Réinitialiser le type de démarrage du service sur automatique | Aucune information supplémentaire |
| Vérifier que le type de démarrage du service Windows Update sur les ordinateurs Windows 8 est automatique ou manuel | Réinitialiser le type de démarrage du service sur manuel | Aucune information supplémentaire |
| Vérifier l'existence du service client (hôte d'Agent SMS) | Aucune correction | Aucune information supplémentaire |
| Vérifier que le type de démarrage du service de contrôle à distance de Configuration Manager est automatique ou manuel | Réinitialiser le type de démarrage du service sur automatique | Aucune information supplémentaire |
| Vérifier que le service de contrôle à distance de Configuration Manager est en cours d'exécution | Démarrer le service de contrôle à distance | Aucune information supplémentaire |
| Vérifier l'intégrité du fournisseur WMI du client | Redémarrer le service WMI (Windows Management Instrumentation) | La correction de cette intégrité du client est effectuée uniquement sur les ordinateurs qui exécutent Windows Server 2003, Windows XP (64 bits) ou des versions antérieures. |
| Vérifier que le service de proxy de mise en éveil (proxy de mise en éveil ConfigMgr) est en cours d'exécution | Démarrer le service de proxy de mise en éveil ConfigMgr | Cette vérification du client est effectuée uniquement si le paramètre client **Gestion de l'alimentation**: **Autoriser le proxy de mise en éveil** est défini sur **Oui** sur les systèmes d'exploitation clients pris en charge. |

| INTÉGRITÉ DU CLIENT | ACTION CORRECTIVE | PLUS D'INFORMATIONS |
| --- | --- | --- |
| Vérifier que le type de démarrage du service de proxy de mise en éveil (proxy de mise en éveil ConfigMgr) est automatique | Réinitialiser le type de démarrage du service de proxy de mise en éveil ConfigMgr sur automatique | Cette vérification du client est effectuée uniquement si le paramètre client **Gestion de l'alimentation**: **Autoriser le proxy de mise en éveil** est défini sur **Oui** sur les systèmes d'exploitation clients pris en charge. |

## Fichiers journaux de déploiement du client

Pour plus d'informations sur les fichiers journaux utilisés par les opérations de déploiement et de gestion du client, consultez Fichiers journaux dans System Center Configuration Manager.

# Utiliser Windows Analytics avec Configuration Manager

22/06/2018 • 7 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Windows Analytics est un ensemble de solutions qui s'exécutent sur Operations Management Suite (OMS). Ces solutions vous permettent d'obtenir des insights sur l'état actuel de votre environnement. Les appareils de votre environnement envoient des données de télémétrie Windows qui sont exploitées et analysées au moyen de solutions dans le portail web Operations Management Suite. En connectant Upgrade Readiness à Configuration Manager, vous pouvez accéder directement aux données dans le nœud **Surveillance** de la console Configuration Manager.

Les données de télémétrie Windows utilisées par Windows Analytics ne sont pas transférées directement au serveur de site Configuration Manager. Les ordinateurs clients envoient les données de télémétrie Windows au service de télémétrie Windows. Ce service transfère ensuite les données pertinentes aux solutions Windows Analytics hébergées dans l'un des espaces de travail OMS de votre organisation. Configuration Manager peut alors soit vous diriger vers les données pertinentes dans le portail web avec des liens en contexte, soit afficher directement les données qui font partie de solutions connectées à Configuration Manager. Vous pouvez également exécuter directement des requêtes sur les données à partir du portail web Operation Management Suite.

> **IMPORTANT**
> Les données de diagnostic et d'utilisation Configuration Manager, qui sont envoyées à Microsoft à partir du serveur de site Configuration Manager, n'ont rien à voir avec Windows Analytics et la télémétrie Windows.

## Configurer les clients pour envoyer des données à Windows Analytics

Pour que les appareils clients envoient des données à Windows Analytics, vous devez les configurer avec une clé d'ID commercial associée à l'espace de travail OMS qui héberge vos données Windows Analytics. Vous devez également configurer les appareils pour qu'ils envoient les données de télémétrie à un niveau approprié pour les solutions que vous souhaitez utiliser.

**Configurer les paramètres client Windows Analytics**

Pour configurer Windows Analytics, dans la console Configuration Manager, choisissez **Administration** > **Paramètres client**, double-cliquez sur **Créer des paramètres client d'appareil personnalisés par défaut**, puis cochez **Windows Analytics**.

Accédez à l'onglet des paramètres **Windows Analytics**, puis configurez les éléments suivants :

- **Clé d'ID commercial**
  La clé d'ID commercial mappe les informations des appareils que vous gérez à l'espace de travail OMS qui héberge les données Windows Analytics de votre organisation. Si vous avez déjà configuré une clé d'ID commercial avec Upgrade Readiness, utilisez cet ID. Si vous ne disposez pas encore d'une clé ID commercial, consultez Générer une clé d'ID commercial.

- **Niveau de télémétrie pour les appareils Windows 10**
  Pour plus d'informations sur chaque niveau de télémétrie Windows 10, consultez Configurer la télémétrie Windows dans votre organisation.

> **NOTE**
> Avec la mise à jour 1710, vous pouvez définir la collecte de données de télémétrie dans Windows 10 sur le niveau **Avancé (limité)**. Ce paramètre vous permet d'obtenir un insight actionnable sur les périphériques de votre environnement sans que ces derniers aient à envoyer toutes les données au niveau de télémétrie **Avancé** avec Windows 10 version 1709 ou ultérieure. Le niveau de télémétrie Avancé (limité) inclut les mesures du niveau de base, ainsi qu'une partie des données collectées au niveau Avancé et pertinentes pour Windows Analytics.

- **Participer à la collecte de données commerciales sur les appareils Windows 7, 8 et 8.1**
  Pour plus d'informations, consultez Windows 7, Windows 8, and Windows 8.1 appraiser telemetry events and fields (Champs et événements de télémétrie d'évaluateur Windows 7, Windows 8 et Windows 8.1).
- **Configurer la collecte de données dans Internet Explorer**
  Sur les appareils Windows 8.1 ou antérieur, la collecte de données dans Internet Explorer permet à Upgrade Readiness de détecter les incompatibilités d'application web qui risquent d'entraver la mise à niveau vers Windows 10. La collecte des données dans Internet Explorer peut être activée pour chaque zone internet. Pour plus d'informations sur les zones internet, consultez À propos des zones de sécurité des URL.

## Utiliser Upgrade Readiness pour identifier les problèmes de compatibilité avec Windows 10

Upgrade Readiness (anciennement Upgrade Analytics) vous permet d'analyser l'état de préparation des appareils et leur compatibilité avec Windows 10. Cette évaluation permet d'optimiser les mises à niveau. Après avoir connecté Configuration Manager à Upgrade Readiness, accédez directement aux données de compatibilité de mise à niveau du client dans la console Configuration Manager. Ensuite, ciblez des appareils pour la mise à niveau ou la mise à jour dans la liste d'appareils.

Pour plus d'informations sur la configuration de la solution Upgrade Readiness et la connexion à celle-ci, consultez Upgrade Readiness.

## Utiliser Windows Analytics pour identifier les écarts dans les stratégies de Protection des informations Windows

Les appareils Windows 10 version 1703 et ultérieures configurés avec une stratégie Protection des informations Windows (WIP) envoient des données de télémétrie sur les applications qui accèdent à des données d'entreprise dans votre environnement, mais qui ne sont pas prises en compte dans les règles d'application de la stratégie WIP. Les utilisateurs peuvent avoir besoin de ces applications pour rester productifs, mais la Protection des informations Windows bloque l'accès des utilisateurs. Le fait de savoir que les utilisateurs accèdent aux données d'entreprise est utile pour la maintenance de vos stratégies de Protection des informations Windows dans Configuration Manager.

Accédez à ces données de Protection des informations Windows à l'aide de cette requête Operations Management Suite.

# Guide pratique pour surveiller les clients pour des serveurs Linux et UNIX dans System Center Configuration Manager

22/06/2018 • 4 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez afficher des informations sur les serveurs Linux et UNIX dans la console System Center Configuration Manager selon les mêmes méthodes que vous employez pour afficher des informations sur des clients Windows.

Vous pouvez notamment afficher les informations suivantes :

- Détails de l'état des clients, dans les tableaux de bord de la console Configuration Manager
- Détails sur les clients dans les rapports par défaut de Configuration Manager
- Détails de l'inventaire dans l'Explorateur de ressources

  Les sections suivantes décrivent comment obtenir ces informations à partir de l'Explorateur de ressources et des rapports.

## Utiliser l'Explorateur de ressources pour afficher l'inventaire des serveurs Linux et UNIX

Quand un client Configuration Manager envoie un inventaire matériel au site Configuration Manager, vous pouvez par la suite utiliser l'Explorateur de ressources pour consulter ces informations. Le client Configuration Manager pour Linux et UNIX n'ajoute pas de nouvelles classes ou vues d'inventaire dans l'Explorateur de ressources. Les données d'inventaire Linux et UNIX sont mappées aux classes WMI existantes. Vous pouvez afficher les détails d'inventaire de vos serveurs Linux et UNIX dans des classifications Windows à l'aide de l'Explorateur de ressources.

Par exemple, vous pouvez collecter la liste de tous les programmes installés en mode natif sur vos serveurs Linux et UNIX, tels que les programmes **.rpms** dans Linux ou **.pkgs** dans Solaris. Une fois que l'inventaire a été envoyé par un client UNIX ou Linux, vous pouvez afficher la liste de tous les programmes UNIX ou Linux installés en mode natif dans l'Explorateur de ressources de la console Configuration Manager.

Pour plus d'informations sur l'utilisation de l'Explorateur de ressources, consultez Guide pratique pour utiliser l'Explorateur de ressources pour afficher l'inventaire matériel dans System Center Configuration Manager.

## Utiliser des rapports pour afficher des informations sur les serveurs Linux et UNIX

Les rapports Configuration Manager contiennent des informations sur les serveurs Linux et UNIX, ainsi que des informations sur les ordinateurs Windows. Aucune configuration supplémentaire n'est nécessaire pour intégrer les données des serveurs Linux et UNIX dans les rapports.

Par exemple, si vous générez le rapport Nombre de versions du système d'exploitation, ce rapport affiche la liste des différents systèmes d'exploitation utilisés et le nombre de clients qui exécutent chaque système d'exploitation. Le rapport est créé sur la base des informations d'inventaire matériel envoyées par les différents clients Configuration Manager qui s'exécutent sur les différents systèmes d'exploitation.

Vous pouvez aussi créer des rapports personnalisés contenant des données propres aux serveurs Linux et UNIX. Vous pouvez utiliser la propriété **Légende** de la classe d'inventaire matériel **Système d'exploitation** pour identifier les systèmes d'exploitation spécifiques dans la demande de rapport.

Pour plus d'informations sur les rapports dans Configuration Manager, consultez Génération de rapports dans System Center Configuration Manager.

# Guide pratique pour gérer les clients dans System Center Configuration Manager

22/06/2018 • 40 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Quand le client Configuration Manager est installé sur un appareil et correctement attribué à un site, l'appareil s'affiche dans l'espace de travail **Ressources et Conformité** du nœud **Appareil**, ainsi que dans un ou plusieurs regroupements du nœud **Regroupements d'appareils**. Quand vous sélectionnez l'appareil ou un regroupement, vous pouvez effectuer des opérations de gestion. Toutefois, il existe d'autres manières de gérer le client, pouvant impliquer d'autres espaces de travail dans la console ou des tâches hors de la console.

> **NOTE**
>
> Si le client Configuration Manager est installé mais n'a pas encore été attribué à un site, il est possible qu'il ne soit pas affiché dans la console. Une fois que le client a été attribué à un site, mettez à jour l'appartenance au regroupement et actualisez l'affichage de la console.
>
> De plus, un appareil peut s'afficher dans la console quand le client Configuration Manager n'est pas installé. Ce comportement peut se produire si l'appareil est découvert mais que le client n'est pas installé et attribué.
>
> Les appareils mobiles gérés à l'aide du connecteur Exchange Server et les appareils inscrits dans Microsoft Intune n'installent pas le client Configuration Manager.
>
> Utilisez la colonne **Client** dans la console Configuration Manager pour déterminer si le client est installé afin de pouvoir être géré à partir de la console.

## Gérer les clients à partir du nœud Appareils

Selon le type de périphérique, certaines de ces options peuvent ne pas être disponibles.

1. Dans la console Configuration Manager, choisissez **Ressources et Conformité** > **Appareils**.
2. Sélectionnez un ou plusieurs appareils, puis sélectionnez une des tâches de gestion de client disponible dans le ruban ou en cliquant avec le bouton droit sur l'appareil :

   - **Gérer les informations relatives à l'affinité entre périphérique et utilisateur**

     Configurez les associations entre les utilisateurs et les appareils, ce qui vous permet de déployer efficacement des logiciels sur les utilisateurs.

     Consultez Lier des utilisateurs et des appareils avec l'affinité entre utilisateur et appareil dans System Center Configuration Manager

   - **Ajouter l'appareil à un regroupement nouveau ou existant**

     Ajoutez l'appareil à un regroupement avec une règle directe.

   - **Installer et réinstaller le client à l'aide de l'Assistant Installation poussée du client**

     Installez et réinstallez le client Configuration Manager pour le réparer ou le reconfigurer. Cette option comprend des paramètres de configuration de site et des propriétés client.msi que vous définissez pour l'installation Push du client.

> **TIP**
> Vous avez le choix entre plusieurs méthodes d'installation (et de réinstallation) du client Configuration Manager. L'Assistant Installation Push du client constitue une méthode pratique d'installation du client car elle peut être exécutée depuis la console, mais cette méthode a de nombreuses dépendances et n'est pas adaptée à tous les environnements. Pour plus d'informations sur les dépendances, consultez Configuration requise pour le déploiement de clients sur des ordinateurs Windows dans System Center Configuration Manager. Pour plus d'informations sur les autres méthodes d'installation de clients, consultez Méthodes d'installation de clients dans System Center Configuration Manager.

Consultez Comment installer des clients Configuration Manager à l'aide de l'installation poussée du client.

- **Réaffecter le site**

  Vous pouvez réaffecter un ou plusieurs clients, notamment des appareils mobiles gérés, à un autre site principal de la hiérarchie. Les clients peuvent être réattribués individuellement ou tous sélectionnés et réattribués en bloc à un nouveau site.

- **Administrer le client à distance**

  Exécutez l'Explorateur de ressources pour afficher des informations sur les inventaires matériel et logiciel à partir d'un client Windows. Administrez à distance l'appareil à l'aide du Contrôle à distance, de l'Assistance à distance ou du Bureau à distance.

  Consultez Guide pratique pour afficher l'inventaire matériel à l'aide de l'Explorateur de ressources et Guide pratique pour afficher l'inventaire logiciel à l'aide de l'Explorateur de ressources.

  Consultez Guide pratique pour administrer à distance un ordinateur client Windows.

- **Approuver un client**

  Quand le client communique avec les systèmes de site en utilisant HTTP et un certificat autosigné, vous devez approuver ces clients pour les identifier comme ordinateurs approuvés. Par défaut, la configuration du site approuve automatiquement les clients de la même forêt Active Directory et de forêts approuvées pour vous éviter d'approuver manuellement chaque client. Toutefois, vous devez approuver manuellement les ordinateurs du groupe de travail auxquels vous faites confiance et tous les ordinateurs non approuvés auxquels vous faites confiance.

  > **WARNING**
  > Certaines fonctions de gestion peuvent fonctionner pour les clients non approuvés, mais ce scénario n'est pas pris en charge pour Configuration Manager.

  Vous ne devez pas approuver les clients qui communiquent toujours avec les systèmes de site en utilisant le protocole HTTPS, ou les clients qui utilisent un certificat PKI quand ils communiquent avec les systèmes de site en utilisant le protocole HTTP. Ces clients établissent une relation de confiance en utilisant les certificats PKI.

- **Bloquer ou débloquer un client**

  Bloquez un client auquel vous ne faites plus confiance. Le blocage empêche le client de recevoir la stratégie et empêche les systèmes de site de communiquer avec le client.

> **WARNING**
> Le fait de bloquer un client empêche les communications entre le client et les systèmes de site Configuration Manager uniquement. Cela n'empêche pas les communications avec d'autres appareils. De plus, lorsque le client communique avec des systèmes de site à l'aide du protocole HTTP au lieu de HTTPS, certaines contraintes de sécurité se présentent.

Vous pouvez également débloquer un client qui est bloqué.

Consultez Déterminer si des clients doivent être bloqués dans System Center Configuration Manager.

- **Effacer un déploiement PXE requis**

  Redéployez les déploiements PXE nécessaires pour l'ordinateur.

  Consultez Utiliser PXE pour déployer Windows sur le réseau avec System Center Configuration Manager.

- **Gérer les propriétés du client**

  Vous pouvez afficher les données de découverte et les déploiements ciblés pour le client. Vous pouvez également configurer des variables qui sont utilisées par les séquences de tâches pour déployer un système d'exploitation sur l'appareil.

- **Supprimer le client**

  > **WARNING**
  > Ne supprimez pas un client si vous souhaitez désinstaller le client Configuration Manager ou le supprimer d'un regroupement.

  L'action **Supprimer** permet de supprimer manuellement l'enregistrement client de la base de données Configuration Manager. En général, cette action est utilisée dans les scénarios de résolution des problèmes. Si vous supprimez l'enregistrement de client, mais que celui-ci est toujours installé et communique avec le site, la Découverte par pulsations d'inventaire recrée l'enregistrement de client. L'enregistrement de client réapparaît dans la console Configuration Manager, mais l'historique du client et les associations précédentes sont perdus.

  > **NOTE**
  > Si vous supprimez un client d'appareil mobile inscrit par Configuration Manager, cette action révoque également le certificat PKI émis pour l'appareil mobile. Ce certificat est alors rejeté par le point de gestion, même si IIS ne vérifie pas la liste de révocation de certificats. Les certificats sur les clients hérités d'appareils mobiles ne sont pas révoqués lorsque vous supprimez ces clients.

  Pour désinstaller le client, voir Désinstaller le client Configuration Manager.

  Pour affecter le client à un nouveau site principal, consultez Comment affecter des clients à un site dans System Center Configuration Manager.

  Pour supprimer le client d'un regroupement, reconfigurez les propriétés du regroupement. Consultez Comment gérer des regroupements dans System Center Configuration Manager.

- **Réinitialiser un appareil mobile**

Vous pouvez réinitialiser les appareils mobiles qui prennent en charge la commande de réinitialisation.

Cette action supprime définitivement toutes les données sur l'appareil mobile, notamment les paramètres et données personnels. En général, cette action rétablit les paramètres par défaut de l'appareil mobile. Réinitialisez un appareil mobile quand vous ne lui faites plus confiance, par exemple s'il a été perdu ou volé.

> **TIP**
> Consultez la documentation du fabricant pour obtenir plus d'informations sur la façon dont l'appareil mobile traite les commandes de réinitialisation à distance.

L'appareil mobile reçoit souvent la commande de réinitialisation avec un certain délai :

- Si l'appareil mobile est inscrit par Configuration Manager ou Microsoft Intune, le client reçoit la commande quand il télécharge sa stratégie client.
- Si l'appareil mobile est géré par le connecteur Exchange Server, il reçoit la commande quand il se synchronise avec Exchange.

  Vous pouvez utiliser la colonne **État de réinitialisation** pour surveiller quand l'appareil reçoit la commande de réinitialisation. Vous pouvez annuler cette commande tant que l'appareil n'a pas envoyé d'accusé de réception de la réinitialisation à Configuration Manager.

- **Mettre hors service un appareil mobile**

  L'option **Mettre hors service** est prise en charge uniquement par les appareils mobiles inscrits par Microsoft Intune ou par la gestion des appareils mobiles (MDM) locale.

  Pour plus d'informations, consultez Protéger vos données à l'aide de la réinitialisation à distance, du verrouillage à distance ou de la réinitialisation du code d'accès avec System Center Configuration Manager.

- **Modifier la propriété d'un appareil**

  Si un appareil n'est pas joint à un domaine et que le client Configuration Manager n'y est pas installé, utilisez cette option pour changer la propriété d'un appareil et la définir sur **Entreprise** ou **Personnel**.

  Vous pouvez utiliser cette valeur dans les conditions des applications pour contrôler les déploiements, et pour contrôler la quantité de données d'inventaire collectées auprès des appareils des utilisateurs.

  Il peut être nécessaire d'ajouter la colonne **Propriétaire de l'appareil**à la vue en à la vue en cliquant avec le bouton droit sur n'importe quel titre de colonne et en choisissant le choisissant.

  Pour plus d'informations, consultez Gestion des appareils mobiles (MDM) hybride avec System Center Configuration Manager et Microsoft Intune.

## Gérer les clients à partir du nœud Regroupements d'appareils

Une grande partie des tâches disponibles pour les appareils du nœud **Appareils** sont également disponibles sur les regroupements. La console applique automatiquement l'opération à tous les appareils éligibles du regroupement. Cette action sur un regroupement entier génère des paquets réseau supplémentaires et augmente l'utilisation de l'UC sur le serveur de site.

Considérez les éléments suivants avant d'effectuer des tâches au niveau du regroupement. Une fois démarrée, vous ne pouvez pas arrêter la tâche à partir de la console.

- Combien y a-t-il d'appareils dans le regroupement ?
- Les appareils sont-ils connectés par des connexions réseau à faible bande passante ?
- Combien de temps faut-il pour effectuer cette tâche pour tous les appareils ?

**Pour gérer les clients à partir du nœud Regroupements de périphériques**

1. Dans la console Configuration Manager, choisissez **Ressources et Conformité** > **Regroupements d'appareils**.

2. Sélectionnez un regroupement, puis sélectionnez une des tâches de gestion du client disponibles dans le ruban ou en cliquant avec le bouton droit sur le regroupement. Ces tâches de gestion de client peuvent être réalisées *uniquement* au niveau du regroupement.

   - **Analysez les ordinateurs pour y détecter des programmes malveillants et téléchargez des fichiers de définition de logiciel anti-programme malveillant.**

     Consultez Endpoint Protection dans System Center Configuration Manager.

   - **Déployez des logiciels, des lignes de base de configuration et des séquences de tâches.**

     Consultez :

     - Déployer des mises à jour logicielles dans System Center Configuration Manager
     - Planifier et configurer les paramètres de conformité dans System Center Configuration Manager

   - **Configurez les paramètres de gestion de l'alimentation.**

     Consultez Comment créer et appliquer des modes de gestion de l'alimentation dans System Center Configuration Manager. Les modes de gestion de l'alimentation ne peuvent être utilisés qu'avec les ordinateurs qui exécutent Windows.

   - **Invitez les ordinateurs à télécharger la stratégie dès que possible.**

     Utilisez une notification de client pour inviter les clients Windows sélectionnés à télécharger la stratégie de l'ordinateur dès que possible en dehors de l'intervalle d'interrogation de stratégie du client.

     Les tâches de notification de client s'affichent dans le nœud **Opérations du client** de l'espace de travail **Surveillance** .

## Redémarrer les clients

À compter de la version 1710, vous pouvez utiliser la console Configuration Manager pour identifier les clients qui nécessitent un redémarrage. Utilisez ensuite une action de notification du client pour les redémarrer.

> **TIP**
> Vous devez également mettre à niveau les clients vers la version 1710 pour que cette fonctionnalité soit opérationnelle. Nous vous recommandons d'activer la mise à niveau automatique des clients pour tenir à jour vos clients avec une surcharge administrative minimale. Pour plus d'informations, consultez Utiliser la mise à niveau automatique du client.

Pour identifier les appareils qui sont en attente de redémarrage, accédez à l'espace de travail **Ressources et conformité** dans la console Configuration Manager et sélectionnez le nœud **Appareils**. Ensuite, affichez l'état de chaque appareil dans le volet des détails d'une nouvelle colonne nommée **Redémarrage en attente**.

Chaque appareil a une ou plusieurs des valeurs suivantes :

- **Non** : il n'existe aucun redémarrage en attente
- **Configuration Manager**: cette valeur provient du composant coordinateur de redémarrage du client (RebootCoordinator.log)
- **Renommage du fichier** : cette valeur vient du fait que Windows a signalé une opération de changement de nom de fichier en attente (HKLM\SYSTEM\CurrentControlSet\Control\Session Manager, PendingFileRenameOperations)
- **Windows Update**: cette valeur vient du fait que l'Agent Windows Update a signalé qu'un redémarrage en attente était nécessaire pour une ou plusieurs mises à jour (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update\RebootRequired)
- **Ajouter ou supprimer une fonctionnalité** : cette valeur vient du fait que le service basé sur les composants Windows a signalé que l'ajout ou la suppression d'une fonctionnalité de Windows nécessitait un redémarrage (HKLM\Software\Microsoft\Windows\CurrentVersion\Component Based Servicing\Reboot Pending)

**Pour créer la notification invitant le client à redémarrer un appareil :**

1. Recherchez l'appareil que vous souhaitez redémarrer dans un regroupement dans le nœud **Regroupements d'appareils** de la console.
2. Cliquez avec le bouton droit sur l'appareil, sélectionnez **Notification du client** et **Redémarrer**. Une fenêtre s'ouvre et affiche des informations concernant le redémarrage. Cliquez sur **OK** pour confirmer la demande de redémarrage.

Lorsqu'un client reçoit la notification, une fenêtre de notification **Centre logiciel** s'ouvre et pour informer l'utilisateur du redémarrage. Par défaut, le redémarrage se produit après 90 minutes. Vous pouvez modifier le délai de redémarrage en configurant les paramètres du client. Les paramètres qui définissent le comportement du redémarrage se trouvent dans l'onglet Redémarrage de l'ordinateur des paramètres par défaut.

# Configurer le cache du client pour les clients Configuration Manager

Le cache du client stocke les fichiers temporaires utilisés lors de l'installation d'applications et de programmes par les clients. Les mises à jour logicielles utilisent également le cache du client, mais elles tentent toujours de télécharger vers le cache, quel que soit le paramètre de taille. Configurez les paramètres du cache, tels que la taille et l'emplacement, quand vous installez manuellement le client, quand vous utilisez une installation Push du client, ou après l'installation.

Depuis Configuration Manager version 1606, vous pouvez spécifier la taille du dossier du cache en utilisant les paramètres client dans la console Configuration Manager.

L'emplacement par défaut pour le cache du client Configuration Manager est %*windir*%\ccmcache, et l'espace disque par défaut est de 5 120 Mo.

> **IMPORTANT**
> Ne chiffrez pas le dossier utilisé pour le cache du client. Configuration Manager ne peut pas télécharger du contenu vers un dossier chiffré.

**À propos du cache du client**

Le client Configuration Manager télécharge le contenu pour les logiciels nécessaires dès qu'il reçoit le déploiement, mais il ne l'exécute pas avant l'heure planifiée du déploiement. À l'heure planifiée, le client Configuration Manager vérifie si le contenu est disponible dans le cache. Si le contenu est dans le cache et qu'il s'agit de la version correcte, le client utilise le contenu mis en cache. Quand la version demandée du contenu change, ou si le client supprime le contenu pour faire de la place pour un autre package, le client retélécharge

le contenu dans le cache.

Si le client tente de télécharger du contenu pour un programme ou une application dont la taille est supérieure à celle du cache, le déploiement échoue en raison de la taille insuffisante du cache. Le client génère un message d'état 10050 signalant que la taille du cache est insuffisante. Si vous augmentez ultérieurement la taille du cache, le résultat est :

- Pour un programme requis : le client ne retente pas automatiquement de télécharger le contenu. Redéployez le package et le programme sur le client.
- Pour une application demandée : le client tente automatiquement de télécharger le contenu quand il télécharge sa stratégie client.

Si le client tente de télécharger un package dont la taille est inférieure à celle du cache, mais que le cache est plein, tous les déploiements demandés continuent leurs tentatives, jusqu'à ce que l'espace du cache soit disponible, jusqu'à expiration du délai de téléchargement ou jusqu'à ce que la limite du nombre de nouvelles tentatives soit atteinte. Si la taille du cache augmente ultérieurement, Configuration Manager effectue une nouvelle tentative de téléchargement du package à l'intervalle suivant. Le client tente de télécharger le contenu toutes les 4 heures jusqu'à ce qu'il atteigne 18 tentatives.

Le contenu mis en cache n'est pas automatiquement supprimé, mais reste dans le cache pendant au moins un jour après son utilisation par le client. Si vous configurez les propriétés du package avec l'option de conserver le contenu dans le cache du client, le client ne supprime pas automatiquement le contenu du package du cache. Si l'espace du cache est utilisé par des packages téléchargés au cours des dernières 24 heures et que le client doit télécharger de nouveaux packages, vous pouvez augmenter la taille du cache ou choisir l'option de suppression du contenu conservé dans le cache.

Utilisez les procédures suivantes pour configurer le cache du client lors de l'installation manuelle du client, ou après avoir installé le client.

**Pour configurer le cache du client lorsque vous installez les clients à l'aide de l'installation client manuelle**

Exécutez la commande CCMSetup.exe à partir de l'emplacement source d'installation et spécifiez les propriétés suivantes dont vous avez besoin, séparées par des espaces :

- DISABLECACHEOPT
  - SMSCACHEDIR
  - SMSCACHEFLAGS
  - SMSCACHESIZE

> **NOTE**
> Pour la version 1606, utilisez les paramètres de taille du cache disponibles dans **Paramètres client** dans la console Configuration Manager au lieu de la propriété SMSCACHESIZE. Pour plus d'informations, consultez Paramètres du cache client.

Pour plus d'informations sur la façon d'utiliser ces propriétés de ligne de commande pour CCMSetup.exe, consultez À propos des propriétés d'installation du client.

**Pour configurer le dossier du cache du client lorsque vous installez les clients à l'aide de l'installation poussée du client**

1. Dans la console Configuration Manager, choisissez **Administration** > **Configuration du site** > **Sites**.
2. Sélectionnez le site approprié et, sous l'onglet **Accueil**, dans le groupe **Paramètres**, choisissez **Paramètres d'installation du client** > **Onglet Propriétés de l'installation**.

3. Spécifiez les propriétés suivantes, séparées par des espaces :

   - DISABLECACHEOPT
   - SMSCACHEDIR
   - SMSCACHEFLAGS
   - SMSCACHESIZE

   > **NOTE**
   > Pour la version 1606, utilisez les paramètres de taille du cache disponibles dans **Paramètres client** dans la console Configuration Manager au lieu de la propriété SMSCACHESIZE. Pour plus d'informations, consultez Paramètres du cache client.

   Pour plus d'informations sur la façon d'utiliser ces propriétés de ligne de commande pour CCMSetup.exe, consultez À propos des propriétés d'installation du client.

**Pour configurer le dossier du cache du client sur l'ordinateur client**

1. Sur l'ordinateur client, accédez à **Configuration Manager** dans le Panneau de configuration et double-cliquez pour ouvrir les propriétés.
2. Sous l'onglet **Cache**, définissez les propriétés de l'espace et de l'emplacement. L'emplacement par défaut est *%windir%* \ccmcache.
3. Pour supprimer les fichiers dans le dossier du cache, choisissez **Supprimer les fichiers**.

**Pour configurer la taille du cache du client dans les paramètres client**

Ajustez la taille du cache du client sans avoir à réinstaller le client en configurant la taille du cache dans la console Configuration Manager à l'aide des Paramètres client.

1. Dans la console Configuration Manager, accédez à **Administration** > **Paramètres client**.
2. Double-cliquez sur **Paramètres client par défaut**. Vous pouvez également créer des paramètres client personnalisés pour appliquer la taille du cache de manière plus sélective. Pour plus d'informations sur les paramètres client personnalisés et par défaut, consultez Guide pratique pour configurer les paramètres client dans System Center Configuration Manager.

   a. Choisissez **Paramètres de cache du client** et choisissez **Oui** pour **Configurer la taille du cache du client**, puis utilisez le paramètre **Mo** ou **Pourcentage du disque**. La taille du cache est ajustée en fonction de la plus petite valeur.

      Le client Configuration Manager configurera la taille du cache avec ces paramètres lors du téléchargement de la stratégie client suivante.

## Désinstaller le client Configuration Manager

Vous pouvez désinstaller le client Configuration Manager d'un ordinateur Windows en exécutant **CCMSetup.exe** avec la propriété **/Uninstall**. Exécutez CCMSetup.exe sur un ordinateur individuel à partir de l'invite de commande ou déployez un package et un programme pour désinstaller le client pour un regroupement d'ordinateurs.

> **WARNING**
> Il n'est pas possible de désinstaller le client Configuration Manager depuis un appareil mobile. Si vous devez supprimer le client Configuration Manager d'un appareil mobile, vous devez le réinitialiser, ce qui supprime toutes les données présentes sur l'appareil mobile.

**Pour désinstaller le client Configuration Manager à partir de l'invite de commande**

1. Ouvrez une invite de commandes Windows et accédez à l'emplacement du fichier CCMSetup.exe.
2. Entrez **Ccmsetup.exe /uninstall**, puis appuyez sur **Entrée**.

> **NOTE**
> Le processus de désinstallation n'affiche pas de résultats à l'écran. Pour vérifier que la désinstallation du client s'est déroulée correctement, examinez le fichier journal **CCMSetup.log** dans le dossier *%windir%\ccmsetup* de l'ordinateur client.

# Gérer les enregistrements en conflit pour les clients Configuration Manager

Configuration Manager utilise l'identificateur de matériel pour tenter d'identifier les éventuels clients dupliqués et vous signale les enregistrements en conflit. Par exemple, si vous réinstallez un ordinateur, il est possible que l'identificateur de matériel soit le même, mais que le GUID utilisé par Configuration Manager soit différent.

Configuration Manager résout automatiquement les conflits en utilisant l'authentification Windows du compte d'ordinateur ou un certificat PKI émis par une source approuvée. Toutefois, quand Configuration Manager ne peut pas résoudre le conflit d'identificateurs de matériel dupliqués, un paramètre de hiérarchie détermine s'il faut fusionner automatiquement les enregistrements ou il vous permet de déterminer le comportement. Si vous décidez de gérer manuellement les enregistrements en doublon, vous devez résoudre vous-même les enregistrements en conflit dans la console Configuration Manager.

**Pour modifier le paramètre de hiérarchie pour gérer les conflits d'enregistrement**

1. Dans la console Configuration Manager, choisissez **Administration** > **Configuration du site** > **Sites** > **Paramètres de hiérarchie**.
2. Sous l'onglet **Approbation client et enregistrements en conflit**, choisissez **Résoudre automatiquement les enregistrements en conflit** ou **Résoudre manuellement les enregistrements en conflit**.

**Pour résoudre manuellement les enregistrements en conflit**

1. Dans la console Configuration Manager, choisissez **Surveillance** > **État du système** > **Enregistrements en conflit**.
2. Sélectionnez un ou plusieurs enregistrements en conflit, puis choisissez **Enregistrement en conflit**.
3. Sélectionnez l'une des options suivantes :

   - **Fusionner** : permet de combiner le nouvel enregistrement détecté avec l'enregistrement client existant.
   - **Nouveau** : permet de créer un nouvel enregistrement pour l'enregistrement de client en conflit.
   - **Bloquer** : permet de créer un nouvel enregistrement pour l'enregistrement de client en conflit, mais le marquer comme bloqué.

# Gérer les identificateurs de matériel dupliqués

Le fait de fournir une liste d'identificateurs de matériel que Configuration Manager ignore pour les besoins du démarrage PXE et de l'inscription du client vous aide à résoudre deux problèmes courants.

1. De nombreux nouveaux appareils, comme la Surface Pro 3, ne comprennent pas de port Ethernet intégré. Les techniciens utilisent une carte USB-Ethernet pour établir une connexion filaire afin de déployer le système d'exploitation. Toutefois, il s'agit souvent de cartes partagées pour des questions de coût et de facilité d'utilisation. Étant donné que l'adresse MAC de cette carte est utilisée pour identifier l'appareil, la réutilisation de cette carte nécessite l'intervention supplémentaire d'un administrateur entre chaque déploiement. Pour réutiliser la carte dans ce scénario, excluez son adresse MAC.
2. Bien que l'attribut SMBIOS doive être unique, certains appareils spécialisés ont des identificateurs dupliqués. Excluez cet identificateur dupliqué et reposez-vous sur l'adresse MAC unique de chaque appareil.

#### Pour ajouter des identificateurs de matériel que Configuration Manager doit ignorer

1. Dans la console Configuration Manager, accédez à **Administration** > **Vue d'ensemble** > **Configuration du site** > **Sites**.
2. Sous l'onglet **Accueil**, dans le groupe **Sites**, choisissez **Paramètres de hiérarchie**.
3. Sous l'onglet **Approbation client et enregistrements en conflit**, choisissez **Ajouter** dans la section **Identificateurs de matériel en doublon** pour ajouter de nouveaux identificateurs de matériel.

# Lancer une récupération de stratégie pour un client Configuration Manager

Sur Windows, un client Configuration Manager télécharge sa stratégie client selon un calendrier que vous configurez comme paramètre du client. Il se peut cependant que dans certaines situations vous souhaitiez lancer une récupération de stratégie à la demande à partir du client, par exemple à des fins de dépannage ou de test.

Vous pouvez lancer une récupération de stratégie en utilisant :

- Notification du client
- L'onglet **Actions** sur le client
- Un script

> **NOTE**
> Pour plus d'informations sur la récupération des stratégies pour les clients qui exécutent Linux et UNIX, consultez Computer policy for Linux and UNIX servers.

#### Lancer une récupération de stratégie client en utilisant une notification de client

1. Dans la console Configuration Manager, choisissez **Ressources et Conformité** > **Regroupements de périphériques**.
2. Sélectionnez le regroupement d'appareils contenant les ordinateurs dont vous voulez télécharger la stratégie. Sous l'onglet **Accueil**, dans le groupe **Regroupements**, choisissez **Notification du Client** > **Télécharger la stratégie d'ordinateur**.

> **NOTE**
> Vous pouvez également utiliser une notification de client pour lancer la récupération de la stratégie pour un ou plusieurs périphériques sélectionnés affichés dans un nœud de regroupement temporaire sous le nœud **Périphériques** .

#### Lancer manuellement la récupération de stratégie du client sous l'onglet Actions du client Configuration Manager

1. Sélectionnez **Configuration Manager** dans le panneau de configuration de l'ordinateur.
2. Sous l'onglet **Actions**, choisissez **Récupération de stratégie ordinateur et cycle d'évaluation** pour lancer la stratégie ordinateur, puis choisissez **Exécuter maintenant**.
3. Cliquez sur **OK** pour confirmer la demande.
4. Répétez les étapes 3 et 4 pour toutes les actions dont vous avez besoin, telles que **Récupération de stratégie utilisateur et cycle d'évaluation** pour les paramètres client utilisateur.

#### Lancer manuellement la récupération de stratégie du client par script

1. Ouvrez un éditeur de texte, tel que le Bloc-notes.
2. Copiez et insérez l'exemple de code Visual Basic Scripting Edition suivant dans le fichier :

```
on error resume next

dim oCPAppletMgr 'Control Applet manager object.
dim oClientAction 'Individual client action.
dim oClientActions 'A collection of client actions.

'Get the Control Panel manager object.
set  oCPAppletMgr=CreateObject("CPApplet.CPAppletMgr")
if err.number <> 0 then
    Wscript.echo "Couldn't create control panel application manager"
    WScript.Quit
end if

'Get a collection of actions.
set oClientActions=oCPAppletMgr.GetClientActions
if err.number<>0 then
    wscript.echo "Couldn't get the client actions"
    set oCPAppletMgr=nothing
    WScript.Quit
end if

'Display each client action name and perform it.
For Each oClientAction In oClientActions

    if oClientAction.Name = "Request & Evaluate Machine Policy" then
        wscript.echo "Performing action " + oClientAction.Name
        oClientAction.PerformAction
    end if
next

set oClientActions=nothing
set oCPAppletMgr=nothing
```

3. Enregistrez le fichier avec une extension .vbs.
4. Sur l'ordinateur client, exécutez le fichier à l'aide de l'une des méthodes ci-après :
   - Accédez au fichier via l'Explorateur Windows et double-cliquez sur le fichier de script.
   - Ouvrez une invite de commandes et tapez **cscript <chemin\nom_fichier.vbs>**.

5. Cliquez sur **OK** dans la boîte de dialogue **Environnement d'exécution de scripts WSH (Windows Script Host)**.

# Guide pratique pour gérer les clients pour des serveurs Linux et UNIX dans System Center Configuration Manager

22/06/2018 • 8 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Quand vous gérez des serveurs Linux et UNIX avec System Center Configuration Manager, vous pouvez configurer des regroupements, des fenêtres de maintenance et des paramètres client pour mieux gérer les serveurs. Par ailleurs, le client Configuration Manager pour Linux et UNIX n'a pas d'interface utilisateur, mais vous pouvez forcer le client à interroger manuellement la stratégie du client.

## Regroupements de serveurs Linux et UNIX

Utilisez les regroupements pour gérer des groupes de serveurs Linux et UNIX de la même façon que d'autres types de clients. Les regroupements peuvent être des regroupements avec adhésion directe ou des regroupements basés sur une requête. Les regroupements basés sur une requête identifient les systèmes d'exploitation clients, les configurations matérielles ou d'autres détails sur le client qui sont stockés dans la base de données du site. Par exemple, vous pouvez utiliser des regroupements qui incluent des serveurs Linux et UNIX pour gérer les paramètres suivants :

- Paramètres du client
- Déploiements de logiciels
- Application de fenêtres de maintenance

  Avant de pouvoir identifier un client Linux ou UNIX par son système d'exploitation ou sa distribution, vous devez collecter l'inventaire matériel du client.

  Les paramètres client par défaut pour l'inventaire matériel incluent des informations sur le système d'exploitation de l'ordinateur client. Vous pouvez utiliser la propriété **Légende** de la classe **Système d'exploitation** pour identifier le système d'exploitation d'un serveur Linux ou UNIX.

  Vous pouvez afficher des informations détaillées sur les ordinateurs qui exécutent le client Configuration Manager pour Linux et UNIX dans le nœud **Appareils** de l'espace de travail **Ressources et Conformité**, dans la console Configuration Manager. Dans l'espace de travail **Ressources et Conformité** de la console Configuration Manager, la colonne **Système d'exploitation** affiche le nom du système d'exploitation de chaque ordinateur.

  Par défaut, les serveurs Linux et UNIX sont membres du regroupement **Tous les systèmes** . Nous recommandons de créer des regroupements personnalisés qui incluent uniquement les serveurs Linux et UNIX, ou un sous-ensemble de ces serveurs. Les regroupements personnalisés vous permettent de gérer des opérations telles que le déploiement de logiciels ou l'affectation de paramètres client à des groupes d'ordinateurs similaires, et de mesurer ainsi avec précision la réussite d'un déploiement.

  Quand vous créez un regroupement personnalisé pour des serveurs Linux et UNIX, insérez des requêtes de règle d'appartenance qui incluent l'attribut Légende pour l'attribut Système d'exploitation. Pour plus d'informations sur la création de regroupements, consultez Guide pratique pour créer des regroupements dans System Center Configuration Manage.

## Fenêtres de maintenance pour les serveurs Linux et UNIX

Le client Configuration Manager pour les serveurs Linux et UNIX prend en charge l'utilisation des fenêtres de maintenance. Cette prise en charge est inchangée par rapport à celle des clients Windows.

## Paramètres client pour les serveurs Linux et UNIX

Vous pouvez configurer les paramètres client qui s'appliquent aux serveurs Linux et UNIX de la même façon que vous configurez les paramètres d'autres clients.

Par défaut, les **paramètres d'agent client par défaut** s'appliquent aux serveurs Linux et UNIX. Vous pouvez également créer des paramètres client personnalisés et les déployer dans des regroupements de clients spécifiques.

Il n'existe pas d'autres paramètres client qui s'appliquent uniquement aux clients Linux et UNIX. Toutefois, il existe des paramètres client par défaut qui ne s'appliquent pas aux clients Linux et UNIX. Le client pour Linux et UNIX applique uniquement les paramètres pour les fonctionnalités qu'il prend en charge.

Par exemple, un paramètre d'appareil client personnalisé qui active et configure les paramètres de contrôle à distance est ignoré par les serveurs Linux et UNIX, car le client pour Linux et UNIX ne prend pas en charge le contrôle à distance.

## Stratégie d'ordinateur pour les serveurs Linux et UNIX

Le client pour les serveurs Linux et UNIX interroge régulièrement la stratégie d'ordinateur de son site pour connaître les configurations demandées et rechercher les déploiements.

Vous pouvez également forcer le client sur un serveur Linux ou UNIX à interroger immédiatement la stratégie d'ordinateur. Pour cela, utilisez les informations d'identification **racine** sur le serveur pour exécuter la commande suivante : **/opt/microsoft/configmgr/bin/ccmexec -rs policy**

Des détails sur l'interrogation de la stratégie d'ordinateur sont entrés dans le fichier journal du client partagé **scxcm.log**.

> **NOTE**
> Le client Configuration Manager pour Linux et UNIX ne demande et ne traite jamais de stratégie utilisateur.

## Gérer les certificats sur le client pour Linux et UNIX

Après avoir installé le client pour Linux et UNIX, vous pouvez utiliser l'outil **certutil** pour mettre à jour le client avec un nouveau certificat PKI et importer une nouvelle liste de révocation de certificats (CRL). Quand vous installez le client pour Linux et UNIX, cet outil est placé dans **/opt/microsoft/configmgr/bin/certutil**.

Pour gérer les certificats, sur chaque client, exécutez certutil avec l'une des options suivantes :

| OPTION | PLUS D'INFORMATIONS |
| --- | --- |

| OPTION | PLUS D'INFORMATIONS |
| --- | --- |
| importPFX | Utilisez cette option pour spécifier un certificat pour remplacer le certificat actuellement utilisé par un client.<br><br>Quand vous utilisez **-importPFX**, vous devez également utiliser le paramètre de ligne de commande **-password** pour fournir le mot de passe associé au fichier PKCS#12.<br><br>Utilisez **-rootcerts** pour spécifier des exigences de certificat racine supplémentaires.<br><br>Exemple : **certutil -importPFX <chemin du certificat PKCS#12> -mot de passe <mot de passe de certificat> [-rootcerts <liste de certificats séparés par des virgules>]** |
| -importsitecert | Utilisez cette option pour mettre à jour le certificat de signature du serveur de site qui se trouve sur le serveur d'administration.<br><br>Exemple : **certutil -importsitecert <chemin du certificat DER>** |
| -importcrl | Utilisez cette option pour mettre à jour la liste de révocation de certificats sur le client avec un ou plusieurs chemins d'accès de fichiers CRL.<br><br>Exemple : **certutil -importcrl <liste de chemins de fichier CRL séparés par des virgules>** |

# Synchroniser les données de System Center Configuration Manager vers Microsoft Operations Management Suite

22/06/2018 • 15 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez utiliser l'**Assistant Services Azure** pour configurer la connexion de Configuration Manager au service cloud Operations Management Suite (OMS). À compter de la version 1706, l'Assistant remplace les flux de travail précédents pour configurer cette connexion. Pour les versions antérieures, consultez Synchroniser les données de System Center Configuration Manager vers Microsoft Operations Management Suite (1702 et antérieur).

- L'Assistant est utilisé pour configurer les services cloud pour Configuration Manager, comme OMS, Microsoft Store pour Entreprises et Azure Active Directory (Azure AD).
- Configuration Manager se connecte à OMS pour des fonctionnalités comme Log Analytics ou Upgrade Readiness.

> **NOTE**
> Par défaut, Configuration Manager n'active pas cette fonctionnalité facultative. Vous devez activer cette fonctionnalité avant de l'utiliser. Pour plus d'informations, consultez Activer les fonctionnalités facultatives des mises à jour.

## Conditions préalables pour le connecteur OMS

Les prérequis pour configurer une connexion à OMS sont identiques aux prérequis documentés pour la version de Current Branch 1702. Ces informations sont répétées ici :

- Avant d'installer le connecteur OMS dans Configuration Manager, vous devez accorder à Configuration Manager les autorisations d'accès à OMS. Plus précisément, vous devez accorder un *accès Contributeur* au *groupe de ressources* Azure qui contient l'espace de travail OMS Log Analytics. Les procédures à suivre sont documentées dans le contenu Log Analytics. Consultez la rubrique Accorder à Configuration Manager les autorisations d'accès à OMS dans la documentation OMS.
- Le connecteur OMS doit être installé sur l'ordinateur qui héberge un point de connexion de service se trouvant en mode en ligne.
- Vous devez installer un Microsoft Monitoring Agent pour OMS sur le point de connexion de service ainsi que le connecteur OMS. L'agent et le connecteur OMS doivent être configurés pour utiliser le même **espace de travail OMS**. Pour installer l'agent, consultez Télécharger et installer l'agent dans la documentation OMS.
- Après avoir installé le connecteur et l'agent, vous devez configurer OMS pour utiliser les données Configuration Manager. Pour ce faire, dans le portail OMS, importez des regroupements Configuration Manager.

## Utilisez l'assistant de services Azure pour configurer la connexion à OMS

1. Dans la console, accédez à **Administration** > **Vue d'ensemble** > **Services cloud** > **Services Azure**. Choisissez **Configurer les services Azure** sous l'onglet **Accueil** du ruban pour démarrer l'**Assistant Services Azure** .

2. Sur la page **Services Azure**, sélectionnez le service cloud Operation Management Suite. Saisissez un nom convivial comme **Nom du service Azure** ainsi qu'une description facultative, puis cliquez sur **Suivant**.

3. Sur la page **Application**, spécifiez votre environnement Azure (la version Technical Preview prend en charge uniquement le cloud public). Ensuite, cliquez sur **Parcourir** pour ouvrir la fenêtre de l'application serveur.

4. Sélectionnez une application web :

   - **Importer** : pour utiliser une application web qui existe déjà dans votre abonnement Azure, cliquez sur **Importer**. Fournissez un nom convivial pour l'application et le locataire. Spécifiez l'ID de locataire, l'ID de client et la clé secrète de l'application web Azure que Configuration Manager doit utiliser. Après avoir **vérifié** les informations, cliquez sur **OK** pour continuer.

   > **NOTE**
   > Lorsque vous configurez OMS avec cette version préliminaire, OMS ne prend en charge la fonction *Importer* pour une application web. La création d'une application web n'est pas prise en charge. De même, vous ne pouvez pas réutiliser une application existante pour OMS.

5. Si vous avez suivi toutes les autres procédures avec succès, les informations sur l'écran **Configuration de la connexion OMS** s'affichent automatiquement sur cette page. Les informations pour les paramètres de connexion devraient s'afficher pour votre **Abonnement Azure**, votre **Groupe de ressources Azure** et votre **Espace de travail Operations Management Suite**.

6. L'Assistant se connecte au service OMS en utilisant les informations que vous avez saisies. Sélectionnez les collections d'appareils que vous souhaitez synchroniser avec OMS, puis cliquez sur **Ajouter**.

7. Vérifiez vos paramètres de connexion dans l'écran **Résumé**, puis sélectionnez **Suivant**. L'écran **Progression** indique l'état de connexion, puis **Terminé**.

8. Une fois l'Assistant terminé, la console Configuration Manager indique que vous avez configuré **Operation Management Suite** comme **Type de service cloud**.

# Synchroniser les données de System Center Configuration Manager vers Microsoft Operations Management Suite (1702 et antérieur)

*S'applique à : System Center Configuration Manager (1702 et versions antérieures)*

Vous pouvez utiliser le connecteur Microsoft Operations Management Suite (OMS) pour synchroniser les données, comme vos regroupements de System Center Configuration Manager avec OMS Log Analytics dans Microsoft Azure. Le connecteur rend les données de votre déploiement Configuration Manager visibles dans OMS.

> **TIP**
> À compter de Configuration Manager 1802, le connecteur OMS n'est plus une fonctionnalité en préversion. Pour plus d'informations, consultez Utiliser des fonctionnalités de préversion des mises à jour.

Depuis la version 1702, vous pouvez utiliser le connecteur OMS pour vous connecter à un espace de travail OMS figurant sur le Microsoft Azure Government Cloud. Pour cela, vous devez modifier un fichier de configuration

avant d'installer le connecteur OMS. Consultez la section Utiliser le connecteur OMS avec Azure Government Cloud de cet article.

**Prérequis**

- Avant d'installer le connecteur OMS dans Configuration Manager, vous devez accorder à Configuration Manager les autorisations d'accès à OMS. Plus précisément, vous devez accorder un *accès Contributeur* au *groupe de ressources* Azure qui contient l'espace de travail OMS Log Analytics. Les procédures à suivre sont documentées dans le contenu Log Analytics. Consultez la rubrique Accorder à Configuration Manager les autorisations d'accès à OMS dans la documentation OMS.

- Le connecteur OMS doit être installé sur l'ordinateur qui héberge un point de connexion de service se trouvant en mode en ligne.

  Si vous avez connecté OMS à un site principal autonome et que vous prévoyez d'ajouter un site d'administration centrale à votre environnement, vous devez supprimer la connexion actuelle puis reconfigurer le connecteur sur le nouveau site d'administration centrale.

- Vous devez installer un Microsoft Monitoring Agent pour OMS sur le point de connexion de service ainsi que le connecteur OMS. L'agent et le connecteur OMS doivent être configurés pour utiliser le même **espace de travail OMS**. Pour installer l'agent, consultez Télécharger et installer l'agent dans la documentation OMS.

- Après avoir installé le connecteur et l'agent, vous devez configurer OMS pour utiliser les données Configuration Manager. Pour ce faire, dans le portail OMS, importez des regroupements Configuration Manager.

**Installer le connecteur OMS**

1. Dans la console Configuration Manager, configurez votre hiérarchie pour utiliser les fonctionnalités de la version préliminaire, puis activez l'utilisation du connecteur OMS.
   0
2. Ensuite, accédez à **Administration** > **Services de cloud** > **Connecteur OMS**. Dans le ruban, cliquez sur « Créer une connexion à Operations Management Suite ». Cette étape ouvre l'**Assistant Connexion à Operation Management Suite**. Sélectionnez **Suivant**.

3. Dans la page **Général**, vérifiez que vous disposez des informations suivantes, puis sélectionnez **Suivant**.

   - Configuration Manager inscrit en tant qu'outil de gestion « Application web et/ou API web » et présence de l'ID de client résultant de cette inscription.
   - Clé de client créée pour l'outil de gestion inscrit dans Azure Active Directory.
   - Dans le portail Azure, l'application web inscrite autorisée à accéder à OMS, comme indiqué dans Accorder à Configuration Manager les autorisations d'accès à OMS.

4. Dans la page **Azure Active Directory**, configurez vos paramètres de connexion à OMS en renseignant les champs **Locataire**, **ID Client** et **Clé secrète du client**, puis sélectionnez **Suivant**.

5. Dans la page **Configuration de la connexion OMS**, définissez vos paramètres de connexion en renseignant les champs **Abonnement Azure**, **Groupe de ressources Azure** et **Espace de travail Operations Management Suite**. L'espace de travail doit correspondre à l'espace de travail configuré pour Microsoft Management Agent installé sur le point de connexion de service.

6. Vérifiez vos paramètres de connexion dans la page **Résumé**, puis sélectionnez **Suivant**. La page **Progression** indique l'état de connexion, puis **Terminé**.

Après avoir lié Configuration Manager à OMS, vous pouvez ajouter ou supprimer des regroupements et afficher les propriétés de la connexion OMS.

**Vérifiez les propriétés du connecteur OMS**

1. Dans la console de Configuration Manager, accédez à **Administration** > **Services cloud**, puis sélectionnez **Connecteur OMS** afin d'ouvrir la page **Connexion OMS**.
2. Cette page contient deux onglets :

   - **Azure Active Directory :**

     Cet onglet affiche votre **Llcataire**, l'**ID client**, l'**expiration de la clé secrète client** et vous permet de vérifier si votre clé secrète client a expiré.

   - **Propriétés de connexion OMS :**

     Cet onglet affiche votre **Abonnement Azure**, votre **Groupe de ressources Azure**, l'**Espace de travail Operations Management Suite**, ainsi que la liste des **Regroupements d'appareils pour lesquels Operations Management Suite peut obtenir des données**. Utilisez les boutons **Ajouter** et **Supprimer** pour modifier les collections autorisées.

**Utiliser le connecteur OMS avec Azure Government Cloud**

1. Sur les ordinateurs où est installée la console Configuration Manager, modifiez le fichier de configuration suivant pour qu'il pointe vers Azure Government Cloud : ***<Chemin d'installation de Configuration Manager>\AdminConsole\bin\Microsoft.configurationManagmenet.exe.config***

   **Modifications :**

   Changez la valeur du nom de paramètre *FairFaxArmResourceID* pour qu'elle corresponde à « https://management.usgovcloudapi.net/ »

   - **Avant modification :** <setting name="FairFaxArmResourceId" serializeAs="String">
     <value></value>
     </setting>

   - **Après modification :**
     <setting name="FairFaxArmResourceId" serializeAs="String">
     <value>https://management.usgovcloudapi.net/</value>
     </setting>

   Changez la valeur du nom de paramètre *FairFaxAuthorityResource* pour qu'elle corresponde à « https://login.microsoftonline.us/ »

   - **Avant modification :** <nom de paramètre="FairFaxAuthorityResource" serializeAs="String">
     <value></value>

   - **Après modification :** <nom du paramètre="FairFaxAuthorityResource" serializeAs="String">
     <value>https://login.microsoftonline.us/</value>

2. Après avoir apporté ces deux modifications et enregistré le fichier, redémarrez la console Configuration Manager sur le même ordinateur, puis utilisez cette console pour installer le connecteur OMS. Pour installer le connecteur, utilisez les informations situées sous Synchroniser les données de System Center Configuration Manager vers Microsoft Operations Management Suite, puis sélectionnez l'**Espace de travail Operations Management Suite** qui se trouve dans Microsoft Azure Government Cloud.

3. Une fois le connecteur OMS installé, une connexion à Azure Government Cloud est disponible lorsque vous utilisez une console se connectant au site.

# Gérer les clients Mac

22/06/2018 • 11 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Voici des procédures relatives à la désinstallation de clients Mac et au renouvellement de leurs certificats.

## Désinstallation du client Mac

1. Sur un ordinateur Mac, ouvrez une fenêtre de terminal et accédez au dossier contenant **macclient.dmg**.
2. Accédez au dossier Outils, puis entrez la ligne de commande suivante :

   **./CMUninstall -c**

   > **NOTE**
   > La propriété **-c** demande au programme de désinstallation du client de supprimer aussi les fichier journaux et les journaux d'incidents du client. Nous recommandons d'utiliser cette propriété pour éviter toute confusion si vous réinstallez le client ultérieurement.

3. Si nécessaire, supprimez manuellement le certificat d'authentification de client que Configuration Manager utilisait, ou révoquez-le. CMUnistall ne supprime et ne révoque pas ce certificat.

## Renouvellement du certificat client Mac

Pour renouveler le certificat client Mac, utilisez une des méthodes suivantes :

- Assistant Renouveler le certificat
- Renouveler le certificat manuellement

**Assistant Renouveler le certificat**

1. Configurez les valeurs suivantes comme *chaînes* dans le fichier ccmclient.plist qui contrôle l'ouverture de l'Assistant Renouvellement de certificat :

   - **RenewalPeriod1** : spécifie, en secondes, la première période de renouvellement pendant laquelle les utilisateurs peuvent renouveler le certificat. La valeur par défaut correspond à 3 888 000 secondes (45 jours). Ne configurez pas de valeur inférieure à 300, sinon la période est rétablie à la valeur par défaut.

   - **RenewalPeriod2** : spécifie, en secondes, la deuxième période de renouvellement pendant laquelle les utilisateurs peuvent renouveler le certificat. La valeur par défaut correspond à 259 200 secondes (3 jours). Si cette valeur est configurée sur une valeur supérieure ou égale à 300 secondes et inférieure ou égale à **RenewalPeriod1**, la valeur configurée est utilisée. Si **RenewalPeriod1** est supérieure à 3 jours, une valeur de 3 jours sera utilisée pour **RenewalPeriod2**. Si **RenewalPeriod1** est inférieure à 3 jours, **RenewalPeriod2** est définie sur la même valeur que **RenewalPeriod1**.

   - **RenewalReminderInterval1** : spécifie, en secondes, la fréquence à laquelle l'Assistant Renouveler le certificat sera affiché pour les utilisateurs lors de la première période de renouvellement. La valeur par défaut correspond à 86 400 secondes (1 jour). Si **RenewalReminderInterval1** est supérieur à 300 secondes et inférieur à la valeur configurée pour **RenewalPeriod1**, la valeur configurée sera utilisée. Dans le cas contraire, la valeur par défaut de 1 jour sera utilisée.

- **RenewalReminderInterval2** : spécifie, en secondes, la fréquence à laquelle l'Assistant Renouveler le certificat sera affiché pour les utilisateurs lors de la deuxième période de renouvellement. La valeur par défaut correspond à 28 800 secondes (8 heures). Si **RenewalReminderInterval2** est supérieure à 300 secondes, inférieure ou égale à **RenewalReminderInterval1** et inférieure ou égale à **RenewalPeriod2**, la valeur configurée sera utilisée. Sinon, une valeur de 8 heures sera utilisée.

  **Exemple** : si les valeurs sont laissées sur leurs valeurs par défaut, 45 jours avant l'expiration du certificat, l'Assistant s'ouvre toutes les 24 heures. Dans les 3 jours de la date d'expiration du certificat, l'Assistant s'ouvre toutes les 8 heures.

  **Exemple** : utilisez la ligne de commande suivante, ou un script, pour définir la première période de renouvellement sur 20 jours.

  ```
  sudo defaults write com.microsoft.ccmclient RenewalPeriod1 1728000
  ```

2. Quand l'Assistant Renouveler le certificat s'ouvre, les champs **Nom d'utilisateur** et **Nom du serveur** sont en général déjà remplis et l'utilisateur peut simplement entrer qu'un mot de passe pour renouveler le certificat.

   > **NOTE**
   > Si l'Assistant ne s'ouvre pas ou si vous fermez l'Assistant par inadvertance, cliquez sur **Renouveler** sur la page des préférences **Configuration Manager** pour ouvrir l'Assistant.

**Renouveler le certificat manuellement**

La période de validité classique pour le certificat client Mac est de 1 an. Configuration Manager ne renouvelle pas automatiquement le certificat utilisateur demandé à l'inscription ; vous devez donc procéder comme suit pour renouveler manuellement le certificat.

> **IMPORTANT**
> Si le certificat a expiré, vous devez désinstaller, réinstaller et réinscrire le client Mac.

Cette procédure supprime l'ID SMS, qui est requis pour demander un nouveau certificat pour le même ordinateur Mac. Lorsque vous supprimez et remplacez l'ID SMS client, tout historique client stocké, tel que l'inventaire, est supprimé après la suppression du client de la console Configuration Manager.

1. Créez et remplissez un regroupement d'appareils pour les ordinateurs Mac qui doivent renouveler les certificats utilisateur.

   > **WARNING**
   > Configuration Manager ne surveille pas la période de validité du certificat qu'il inscrit pour les ordinateurs Mac. Vous devez surveiller cette validité indépendamment de Configuration Manager pour identifier les ordinateurs Mac à ajouter à ce regroupement.

2. Dans l'espace de travail **Ressources et compatibilité** , démarrez l' **Assistant Création d'élément de configuration**.

3. Sur la page **Général** , spécifiez informations suivantes :

   - **Nom :Supprimer l'ID SMS pour Mac**
   - **Type :Mac OS X**

4. Dans la page **Plateformes prises en charge**, vérifiez que toutes les versions de Mac OS X sont sélectionnées.
5. Dans la page **Paramètres**, choisissez **Nouveau**, puis dans la boîte de dialogue **Créer un paramètre**, spécifiez les informations suivantes :
   - **Nom :Supprimer l'ID SMS pour Mac**
   - **Type de paramètre :Script**
   - **Type de données :Chaîne**
6. Dans la boîte de dialogue **Créer un paramètre**, sous **Script de découverte**, choisissez **Ajouter un script** pour spécifier un script de découverte des ordinateurs Mac configurés avec un SMSID configuré.
7. Dans la boîte de dialogue **Modifier un script de découverte** , entrez le script Shell suivant :

   ```
   defaults read com.microsoft.ccmclient SMSID
   ```

8. Choisissez **OK** pour fermer la boîte de dialogue **Modifier un script de découverte**.
9. Dans la boîte de dialogue **Créer un paramètre**, sous **Script de correction (facultatif)**, choisissez **Ajouter un script** pour spécifier un script de suppression du SMSID détecté sur les ordinateurs Mac.
10. Dans la boîte de dialogue **Créer un script de correction** , entrez le script Shell suivant :

    ```
    defaults delete com.microsoft.ccmclient SMSID
    ```

11. Choisissez **OK** pour fermer la boîte de dialogue **Créer un script de correction**.
12. Sur la page **Règles de compatibilité** de l'Assistant, cliquez sur **Nouveau**, puis dans la boîte de dialogue **Créer une règle** , spécifiez les informations suivantes :
    - **Nom :Supprimer l'ID SMS pour Mac**
    - **Paramètre sélectionné :** Choisissez **Parcourir**, puis sélectionnez le script de découverte que vous avez spécifié précédemment.
    - Dans **les valeurs suivantes** , entrez **la paire domaine/par défaut (com.microsoft.ccmclient, ID SMS) n'existe pas**.
    - Activez l'option **Exécuter le script de correction spécifié lorsque ce paramètre n'est pas compatible**.
13. Effectuez toutes les étapes de l'Assistant Création d'élément de configuration.
14. Créez une ligne de base de configuration contenant l'élément de configuration que vous venez de créer et déployez-la sur le regroupement d'appareils créé à l'étape 1.

    Pour plus d'informations sur la création et le déploiement de lignes de base de configuration, consultez Comment créer des bases de référence de configuration dans System Center Configuration Manager et Comment déployer des lignes de base de configuration dans System Center Configuration Manager.
15. Sur les ordinateurs Mac sur lesquels l'ID SMS a été supprimé, exécutez la commande suivante pour installer un nouveau certificat :

    ```
    sudo ./CMEnroll -s <enrollment_proxy_server_name> -ignorecertchainvalidation -u <'user name'>
    ```

Lorsque vous y êtes invité, fournissez le mot de passe du compte de superutilisateur qui exécute la commande, puis le mot de passe du compte d'utilisateur Active Directory.

16. Pour limiter le certificat inscrit à Configuration Manager, sur l'ordinateur Mac, ouvrez une fenêtre de terminal et apportez les modifications suivantes :

    a. Entrez la commande **sudo /Applications/Utilities/Keychain\ Access.app/Contents/MacOS/Keychain\ Access**

    b. Dans la boîte de dialogue **Trousseau d'accès**, dans la zone **Trousseau**, choisissez **Système**, puis dans la zone **Catégorie**, choisissez **Clés**.

    c. Développez les clés pour afficher les certificats clients. Lorsque vous avez identifié le certificat avec une clé privée que vous venez d'installer, double-cliquez sur la clé.

    d. Sous l'onglet **Contrôle d'accès**, choisissez **Confirmer avant d'autoriser l'accès**.

    e. Accédez à **/Library/Application Support/Microsoft/CCM**, sélectionnez **CCMClient**, puis choisissez **Ajouter**.

    f. Choisissez **Enregistrer les modifications** et fermez la boîte de dialogue **Trousseau d'accès**.

17. Redémarrez l'ordinateur Mac.

# Tableau de bord des appareils Surface dans System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

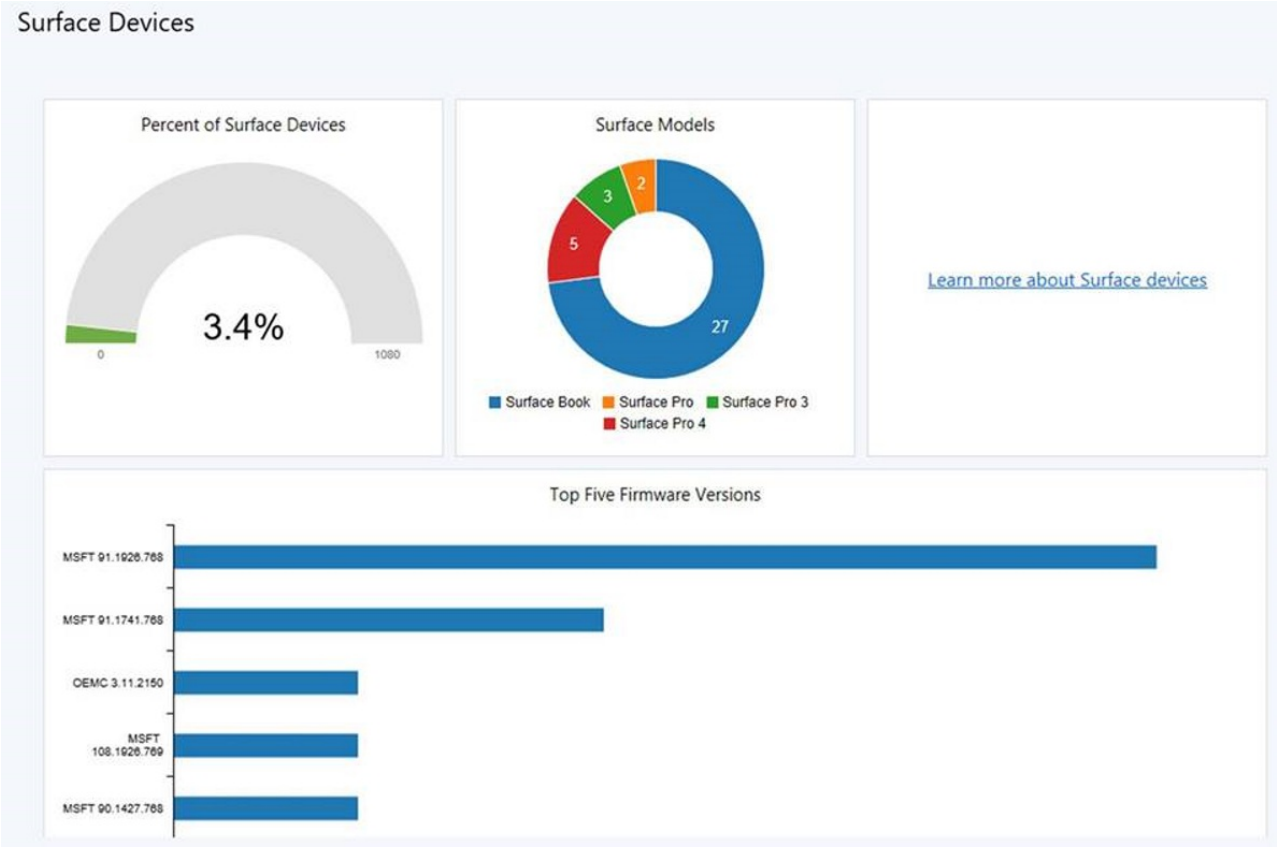
À compter de la version 1802, le tableau de bord des appareils Surface vous fournit, d'un seul coup d'œil, des informations sur les appareils Surface se trouvant dans votre environnement.

## Ouvrir le tableau de bord des appareils Surface

Pour ouvrir le tableau de bord des appareils Surface, effectuez les étapes suivantes :

1. Ouvrez la console Configuration Manager.
2. Cliquez sur le nœud **Analyse**.
3. Pour charger le tableau de bord, cliquez sur **Appareils Surface**.

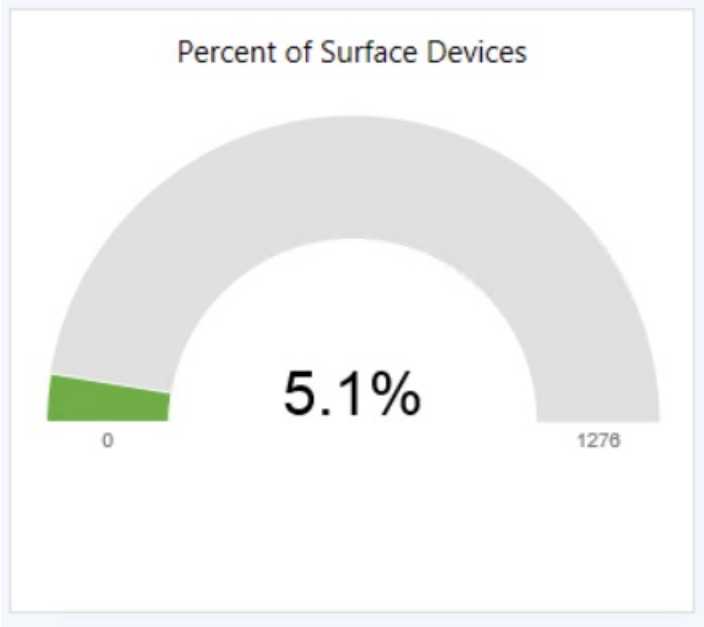
**Tableau de bord des appareils Surface**



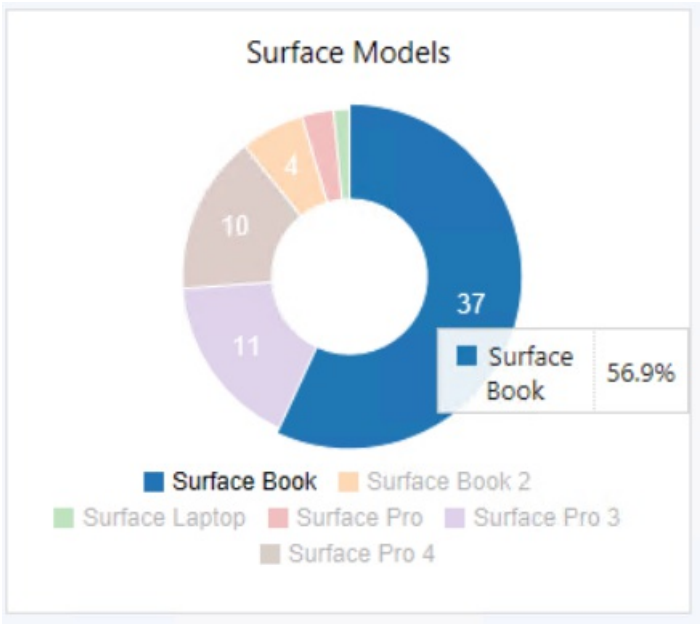

## Consultation des informations contenues dans le tableau de bord des appareils Surface

Le tableau de bord des appareils Surface présente trois graphiques pour votre environnement.

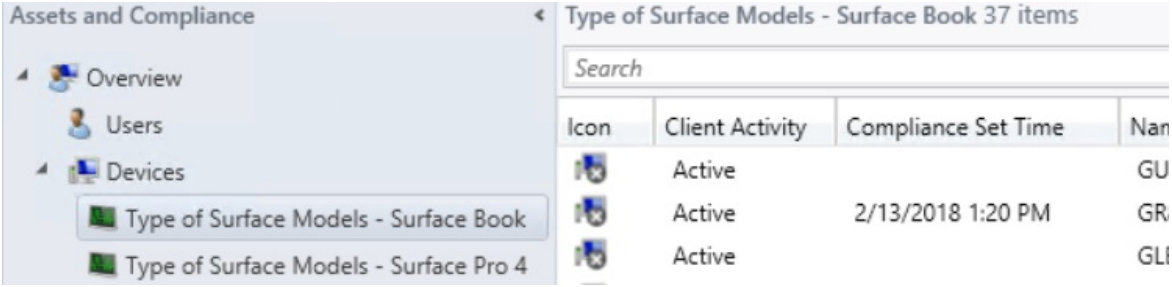
- **Pourcentage d'appareils Surface** : indique le pourcentage d'appareils Surface dans tout votre environnement.



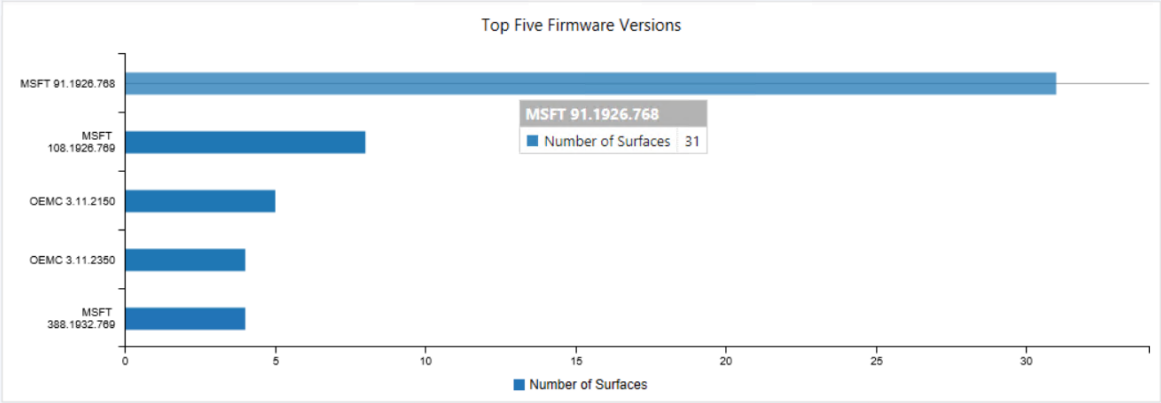

- **Modèles d'appareil Surface** : affiche le nombre d'appareils par modèle Surface.
  - Pointer sur une section du graphique vous donne le pourcentage d'appareils Surface qui sont du modèle sélectionné.




  - Cliquer sur une section du graphique vous permet d'accéder à une liste d'appareils pour le modèle.




- **Cinq principales versions de microprogramme** : affiche un graphique comprenant les cinq principaux modèles de microprogramme de votre environnement.
  - Pointer sur une section du graphique vous donne le nombre d'appareils Surface qui sont de la version de microprogramme sélectionnée.




## Plus d'informations

Pour plus d’informations sur les appareils Surface, consultez les éléments suivants :

- Le site web Surface.

Pour plus d’informations sur le déploiement des mises à jour de microprogramme Surface dans Configuration Manager, consultez :

- Comment gérer les mises à jour de pilote Surface dans Configuration Manager

# Cogestion pour les appareils Windows 10

18/06/2018 • 9 minutes to read • Edit Online

Dans les mises à jour précédentes de Windows 10, vous pouviez déjà joindre un appareil Windows 10 à Active Directory (AD) en local et à Azure AD sur le cloud (Azure AD hybride). À compter de Configuration Manager version 1710, la cogestion tire parti de cette amélioration et vous permet de gérer simultanément plusieurs appareils Windows 10 version 1709 à l'aide de Configuration Manager et d'Intune.

## Pourquoi la cogestion ?

Nombreux sont les clients qui souhaitent gérer les appareils Windows 10 comme les appareils mobiles, en recourant à une solution cloud plus simple et moins chère. Toutefois, le passage de la gestion classique à la gestion moderne peut s'avérer difficile.

## Qu'est-ce que la cogestion ?

La cogestion vous permet de gérer simultanément des appareils Windows 10 à l'aide de Configuration Manager et d'Intune. C'est une solution qui établit une passerelle entre la gestion classique et la gestion moderne tout en vous donnant la possibilité d'opérer cette transition selon une approche en plusieurs phases.

## Avantages

- Utilisation immédiate des fonctionnalités Intune
  - Actions à distance
    - Réinitialisation aux paramètres d'usine
    - Réinitialisation sélective
    - Suppression d'appareils
    - Redémarrage d'un appareil
    - Nouvelle version
  - Orchestration avec Intune pour les charges de travail suivantes :
    - Stratégies de conformité
    - Stratégies d'accès aux ressources
    - Stratégies Windows Update
    - Endpoint Protection, à compter de Configuration Manager 1802

## Comment configurer la cogestion

Il existe deux principaux parcours pour accéder à la cogestion. Le premier a trait à la cogestion provisionnée par Configuration Manager où les appareils Windows 10 gérés conjointement par Configuration Manager et Azure AD hybride sont inscrits dans Intune. Le second fait intervenir les appareils provisionnés par Intune qui sont inscrits dans Intune, puis installés avec le client Configuration Manager pour atteindre l'état de cogestion.

**Configuration Manager**

- Effectuez une mise à niveau vers Configuration Manager version 1710 ou ultérieure.

**Azure Active Directory**

- Jonction à Azure AD hybride (jonction à AD et à Azure AD).
- Activez l'inscription automatique Windows 10.

**Intune**

- Comment configurer un abonnement Intune ou Configurer Intune
- Démarrer la migration de MDM hybride vers Intune autonome

> **NOTE**
> Si vous avez un environnement MDM hybride (Intune intégré à Configuration Manager), vous ne pouvez pas activer la cogestion. Toutefois, vous pouvez commencer la migration d'utilisateurs vers Intune autonome, puis activer leurs appareils Windows 10 associés pour la cogestion. Pour plus d'informations sur la migration vers Intune autonome, consultez Démarrer la migration de MDM hybride vers Intune autonome.

**Activer la cogestion**

Dans la console Configuration Manager, accédez à **Administration** > **Vue d'ensemble** > **Services cloud** > **Cogestion**. Choisissez **Configurer la cogestion** à partir du ruban pour ouvrir l'**Assistant Intégration de la cogestion**

1. Dans la page **Abonnement**, cliquez sur **Se connecter** et connectez-vous à votre locataire Intune, puis cliquez sur **Suivant**. Vérifiez que le compte utilisé pour se connecter à votre locataire dispose d'une licence Intune. Si ce n'est pas le cas, la connexion échoue avec le message d'erreur suivant : « Utilisateur non reconnu ».
2. Dans la page **Activation**, choisissez votre paramètre **Inscription automatique dans Intune**. Copiez la ligne de commande pour les appareils déjà inscrits dans Intune, si nécessaire.
3. Dans la page **Charges de travail**, de chaque charge de travail, choisissez le groupe d'appareils concerné par la gestion avec Intune.
4. Dans la page **Mise en lots**, sélectionnez un regroupement d'appareils en tant que **regroupement pilote**. Vérifiez les informations de **résumé** et terminez l'Assistant.

**Mettre à niveau le client Windows 10**

- Effectuez une mise à niveau vers Windows 10, version 1709 (également appelée Fall Creators Update) et ultérieure.

**Configurer les charges de travail pour basculer vers Intune**

L'article intitulé Charges de travail pouvant être transférées à Intune vous explique comment basculer des charges de travail Configuration Manager spécifiques vers Intune. Cet article comprend également des instructions sur la modification des groupes d'appareils pour lesquels des charges de travail sont transférées.

- **Stratégies de conformité :** Les stratégies de conformité définissent les règles et les paramètres auxquels doit se conformer un appareil pour être considéré conforme par les stratégies d'accès conditionnel. Vous pouvez également utiliser des stratégies de conformité pour surveiller et corriger les problèmes de conformité avec les appareils indépendamment de l'accès conditionnel. Pour plus d'informations, consultez Stratégies de conformité des appareils.

- **Stratégies Windows Update :** Les stratégies Windows Update pour Entreprise vous permettent de configurer des stratégies de report pour les mises à jour de fonctionnalités Windows 10 ou les mises à jour qualité pour les appareils Windows 10 gérés directement par Windows Update pour Entreprise.Pour plus d'informations, consultez Configurer les stratégies de report Windows Update pour Entreprise.

- **Stratégies d'accès aux ressources :** Les stratégies d'accès aux ressources configurent les paramètres VPN, Wi-Fi, d'e-mail et de certificat sur les appareils. Pour plus d'informations, consultez Déployer des profils d'accès aux ressources.

- **Endpoint Protection:** À compter de Configuration Manager 1802, la charge de travail Endpoint Protection peut être transférée à Intune. Pour plus d'informations, consultez Endpoint Protection pour Microsoft Intune et Charges de travail pouvant être transférées à Intune.

**Installer le client Configuration Manager sur les appareils inscrits à Intune**

Lorsque des appareils Windows 10 sont inscrits à Intune, vous pouvez y installer le client Configuration Manager (à l'aide d'un argument de ligne de commande spécifique) pour préparer les clients à la cogestion. Ensuite, activez la cogestion à partir de la console Configuration Manager et commencez le déplacement de charges de travail spécifiques vers Intune pour des appareils Windows 10 spécifiques. Quant aux appareils Windows 10 qui ne sont pas encore inscrits à Intune, vous pouvez utiliser l'inscription automatique dans Azure pour les inscrire. Pour ce qui est des nouveaux appareils Windows 10, vous pouvez utiliser Windows AutoPilot et configurer l'expérience OOBE (Out of Box Experience) qui inclut l'inscription automatique permettant d'inscrire les appareils à Intune.

- Activez Passerelle de gestion cloud dans Configuration Manager (uniquement lorsque vous utilisez Intune pour installer le client Configuration Manager).

## Surveiller la cogestion

Le tableau de bord de cogestion vous permet d'examiner les machines qui sont cogérées dans votre environnement. Les graphes peuvent vous aider à identifier les appareils qui demandent une attention particulière.

## Étapes suivantes

Préparer les appareils Windows 10 pour la cogestion

# Préparer les appareils Windows 10 pour la cogestion

22/06/2018 • 10 minutes to read • Edit Online

Vous pouvez activer la cogestion sur les appareils Windows 10 qui sont joints à AD et à Azure AD, et inscrits auprès de Microsoft Intune et d'un client dans Configuration Manager. Pour les nouveaux appareils Windows 10 et pour ceux qui sont déjà inscrits à Intune, installez le client Configuration Manager avant de pouvoir les cogérer. Pour les appareils Windows 10 qui sont déjà des clients Configuration Manager, inscrivez-les à Intune et activez la cogestion dans la console Configuration Manager.

> **IMPORTANT**
> Les appareils mobiles Windows 10 ne prennent pas en charge la cogestion.

## Prérequis

Les prérequis suivants doivent être mis en place avant de pouvoir activer la cogestion. Il existe des prérequis généraux et des prérequis distincts pour les appareils dotés du client Configuration Manager et les appareils sur lesquels le client n'est pas installé.

### Conditions préalables

Les prérequis généraux pour activer la cogestion sont les suivants :

- Configuration Manager version 1710 ou ultérieure
- Site intégré à Azure AD pour la gestion cloud
- Licence EMS ou Intune pour tous les utilisateurs
- Inscription automatique auprès d'Azure AD activée
- Abonnement Intune (autorité MDM dans Intune définie sur **Intune**)

> **NOTE**
> Si vous avez un environnement MDM hybride (Intune intégré à Configuration Manager), vous ne pouvez pas activer la cogestion. Toutefois, vous pouvez commencer la migration d'utilisateurs vers Intune autonome, puis activer leurs appareils Windows 10 associés pour la cogestion. Pour plus d'informations sur la migration vers Intune autonome, consultez Démarrer la migration de MDM hybride vers Intune autonome.

### Prérequis supplémentaires pour les appareils dotés du client Configuration Manager

- Windows 10, version 1709 ou ultérieure
- Jonction à Azure AD hybride (jonction à AD et à Azure AD)

### Prérequis supplémentaires pour les appareils non dotés du client Configuration Manager

- Windows 10, version 1709 ou ultérieure
- Passerelle de gestion cloud dans Configuration Manager (lorsque vous utilisez Intune pour installer le client Configuration Manager)

> **IMPORTANT**
> Les appareils mobiles Windows 10 ne prennent pas en charge la cogestion.

# Ligne de commande pour installer un client Configuration Manager

Créez une application dans Intune pour les appareils Windows 10 qui ne sont pas encore des clients Configuration Manager. Lors de la création de l'application dans les sections suivantes, utilisez cette ligne de commande :

```
ccmsetup.msi CCMSETUPCMD="/mp:<URL of cloud management gateway mutual auth endpoint> CCMHOSTNAME=<URL of cloud management gateway mutual auth endpoint> SMSSiteCode=<Sitecode> SMSMP=https://<FQDN of MP> AADTENANTID=<AAD tenant ID> AADCLIENTAPPID=<Server AppID for AAD Integration> AADRESOURCEURI=https://<Resource ID>"
```

Par exemple, si vous aviez les valeurs suivantes :

- **URL du point de terminaison de l'authentification mutuelle pour la passerelle de gestion cloud** : https://contoso.cloudapp.net/CCM_Proxy_MutualAuth/72186325152220500

  > **NOTE**
  > Utilisez la valeur **MutualAuthPath** dans la vue SQL **vProxy_Roles** pour la valeur **URL du point de terminaison de l'authentification mutuelle pour la passerelle de gestion cloud**.

- **Nom de domaine complet du point de gestion** : mp1.contoso.com
- **CodeSite** : PS1
- **ID de locataire Azure AD** : 60a413f4-c606-4744-8adb-9476ae3XXXXX
- **ID d'application cliente Azure AD** : 9fb9315f-4c42-405f-8664-ae63283XXXXX
- **URI de l'ID de la ressource AAD** : ConfigMgrServer

  > **NOTE**
  > Utilisez la valeur **IdentifierUri** trouvée dans la vue SQL **vSMS_AAD_Application_Ex** pour la valeur **URI de l'ID de la ressource AAD**.

Vous utiliseriez la ligne de commande suivante :

```
ccmsetup.msi CCMSETUPCMD="/mp:https://contoso.cloudapp.net/CCM_Proxy_MutualAuth/72186325152220500 CCMHOSTNAME=contoso.cloudapp.net/CCM_Proxy_MutualAuth/72186325152220500 SMSSiteCode=PS1 SMSMP=https://mp1.contoso.com AADTENANTID=60a413f4-c606-4744-8adb-9476ae3XXXXX AADCLIENTAPPID=9fb9315f-4c42-405f-8664-ae63283XXXXX AADRESOURCEURI=https://ConfigMgrServer"
```

> **TIP**
> Pour trouver les paramètres de ligne de commande pour votre site, effectuez les étapes suivantes :
>
> 1. Dans la console Configuration Manager, accédez à **Administration** > **Vue d'ensemble** > **Services cloud** > **Cogestion**.
> 2. Sous l'onglet Accueil, dans le groupe Gérer, choisissez **Configurer la cogestion** pour ouvrir l'Assistant Intégration de la cogestion.
> 3. Dans la page Abonnement, cliquez sur **Se connecter** et connectez-vous à votre locataire Intune, puis cliquez sur **Suivant**.
> 4. Dans la page Activation, cliquez sur **Copier** dans la section **Appareils inscrits dans Intune** pour copier la ligne de commande dans le Presse-papiers et l'enregistrer ensuite pour vous en servir ultérieurement dans la procédure de création de l'application.
> 5. Cliquez sur **Annuler** pour quitter l'Assistant.

> **IMPORTANT**
> Si vous personnalisez la ligne de commande pour installer le client Configuration Manager, vérifiez qu'elle ne dépasse pas 1 024 caractères. Quand la ligne de commande fait plus de 1024 caractères, l'installation du client échoue.

## Nouveaux appareils Windows 10

Pour les nouveaux appareils Windows 10, vous pouvez utiliser le service Autopilot pour configurer le mode OOBE (Out Of Box Experience) qui inclut la jonction de l'appareil à AD et à Azure AD, ainsi que son inscription dans Intune. Ensuite, créez une application dans Intune pour déployer le client Configuration Manager.

1. Activez AutoPilot pour les nouveaux appareils Windows 10. Pour plus d'informations, consultez Présentation de Windows AutoPilot.

   > **NOTE**
   > À compter de la version 1802, utilisez Configuration Manager pour collecter et signaler les informations des appareils nécessaires à Microsoft Store pour Entreprises et Éducation. numéro de série, identificateur de produit Windows et identificateur matériel. Dans l'espace de travail **Monitoring** de la console de Configuration Manager, développez le nœud **Création de rapports**, puis **Rapports**, et sélectionnez le nœud **Matériel – Général**. Exécutez le nouveau rapport, **Informations sur les appareils Windows AutoPilot**, et affichez les résultats. Dans la visionneuse de rapports, cliquez sur l'icône **Exporter**, puis sélectionnez l'option **CSV (délimité par des virgules)**. Après avoir enregistré le fichier, chargez les données dans Microsoft Store pour Entreprises et Éducation. Pour plus d'informations, consultez la page Ajouter des appareils dans Microsoft Store pour Entreprises et Éducation.

2. Configurez l'inscription automatique dans Azure AD pour que vos appareils soient inscrits automatiquement à Intune. Pour plus d'informations, consultez Inscrire des appareils Windows pour Microsoft Intune.

3. Créez une application dans Intune avec le package du client Configuration Manager et déployez l'application sur les appareils Windows 10 que vous souhaitez gérer conjointement. Utilisez la ligne de commande pour installer un client Configuration Manager lorsque vous suivez les étapes permettant d'installer des clients à partir d'Internet avec Azure AD.

## Appareils Windows 10 non inscrits à Intune ou non-clients Configuration Manager

Pour les appareils Windows 10 qui ne sont pas inscrits à Intune ou qui n'ont pas le client Configuration Manager, vous pouvez utiliser l'inscription automatique pour les inscrire dans Intune. Ensuite, créez une application dans Intune pour déployer le client Configuration Manager.

1. Configurez l'inscription automatique dans Azure AD pour que vos appareils soient inscrits automatiquement à Intune. Pour plus d'informations, consultez Inscrire des appareils Windows pour Microsoft Intune.
2. Créez une application dans Intune avec le package du client Configuration Manager et déployez l'application sur les appareils Windows 10 que vous souhaitez gérer conjointement. Utilisez la ligne de commande pour installer un client Configuration Manager lorsque vous suivez les étapes permettant d'installer des clients à partir d'Internet avec Azure AD.

## Appareils Windows 10 inscrits à Intune

Pour les appareils Windows 10 qui sont déjà inscrits à Intune, créez une application dans Intune pour déployer le client Configuration Manager. Utilisez la ligne de commande pour installer un client Configuration Manager lorsque vous suivez les étapes permettant d'installer des clients à partir d'Internet avec Azure AD.

## Étapes suivantes

Basculer les charges de travail de Configuration Manager sur Intune

# Basculer les charges de travail de Configuration Manager sur Intune

12/06/2018 • 9 minutes to read • Edit Online

Dans Préparer les appareils Windows 10 pour la cogestion, vous avez préparé les appareils Windows 10 à la cogestion. Ces appareils sont joints à AD et à Azure AD, ils sont inscrits dans Intune et ils disposent du client Configuration Manager. Vous avez probablement encore des appareils Windows 10 joints à AD et qui ont le client Configuration Manager, mais qui ne sont pas joints à Azure AD ni inscrits à Intune. La procédure suivante présente les étapes permettant d'activer la cogestion et de préparer le reste de vos appareils Windows 10 (les clients Configuration Manager sans inscription à Intune) pour la cogestion ; elle vous sert également à lancer le basculement de charges de travail spécifiques de Configuration Manager vers Intune.

1. Dans la console Configuration Manager, accédez à **Administration** > **Vue d'ensemble** > **Services cloud** > **Cogestion**.
2. Sous l'onglet Accueil, dans le groupe Gérer, choisissez **Configurer la cogestion** pour ouvrir l'Assistant Configuration de la cogestion.
3. Dans la page Abonnement, cliquez sur **Se connecter** et connectez-vous à votre locataire Intune, puis cliquez sur **Suivant**.
4. Dans la page Activation, choisissez **Pilote** ou **Tout** pour activer l'inscription automatique dans Intune, puis cliquez sur **Suivant**. Lorsque vous choisissez **Pilote**, seuls les clients Configuration Manager membres du groupe pilote sont automatiquement inscrits à Intune. Cette option vous permet d'activer la cogestion sur un sous-ensemble de clients pour tester initialement la cogestion et la déployer au moyen d'une approche progressive. Vous pouvez utiliser la ligne de commande pour déployer le client Configuration Manager en tant qu'application dans Intune pour les appareils déjà inscrits à Intune. Pour plus d'informations, consultez Appareils Windows 10 inscrits à Intune.
5. Dans la page Charges de travail, choisissez de basculer ou non les charges de travail Configuration Manager devant être gérées par Intune pilote ou Intune, puis cliquez sur **Suivant**. Le paramètre **Intune pilote** bascule la charge de travail associée uniquement pour les appareils inclus dans le groupe pilote. Le paramètre **Intune** bascule la charge de travail associée pour tous les appareils Windows 10 cogérés.

   > **IMPORTANT**
   > Avant de basculer toutes les charges de travail, vérifiez que la charge de travail correspondante dans Intune a été correctement configurée et déployée. Ainsi, vous garantissez que les charges de travail sont toujours gérées par l'un des outils de gestion de vos appareils.

6. Dans la page Préparation, configurez les paramètres suivants et cliquez sur **Suivant** :
   - **Pilote** : le groupe pilote contient un ou plusieurs regroupements que vous sélectionnez. Utilisez ce groupe dans le cadre de votre déploiement progressif de la cogestion. Vous pouvez commencer par un regroupement test peu volumineux, puis ajouter d'autres regroupements à ce groupe pilote au fur et à mesure que vous déployez la cogestion pour d'autres utilisateurs et appareils. À tout moment, vous pouvez modifier les regroupements dans le groupe pilote à partir des propriétés de cogestion.
   - **Production** : configurez le **groupe d'exclusions** avec un ou plusieurs regroupements. Les appareils membres d'une des collections de ce groupe sont exclus de l'utilisation de la cogestion.
7. Pour activer la cogestion, terminez l'Assistant.

## Modifier les paramètres de cogestion

Après avoir activé la cogestion à l'aide de l'Assistant, vous pouvez modifier les paramètres dans les propriétés de cogestion.

- Dans la console Configuration Manager, accédez à **Administration** > **Vue d'ensemble** > **Services cloud** > **Cogestion**.
  Sélectionnez l'objet de cogestion, cliquez sur l'onglet Accueil, puis sur **Propriétés**.

## Charges de travail pouvant être transférées à Intune

Certaines charges de travail sont disponibles pour être basculées sur Intune. La liste suivante est mise à jour dès que des charges de travail sont disponibles pour être transférées :

1. Stratégies de conformité des appareils
2. Stratégies d'accès aux ressources : Les stratégies d'accès aux ressources configurent les paramètres VPN, Wi-Fi, d'e-mail et de certificat sur les appareils. Pour plus d'informations, consultez Déployer des profils d'accès aux ressources.
   - Profil de messagerie
   - Profil Wi-Fi
   - Profil VPN
   - Profil de certificat
3. Stratégies Windows Update
4. Endpoint Protection (à compter de Configuration Manager version 1802)
   - Windows Defender Application Guard
   - Pare-feu Windows Defender
   - Windows Defender SmartScreen
   - Chiffrement Windows
   - Windows Defender Exploit Guard
   - Windows Defender Application Control
   - Centre de sécurité Windows Defender
   - Windows Defender - Protection avancée contre les menaces
   - Protection des informations Windows

## Surveiller la cogestion

Après avoir activé la cogestion, vous pouvez surveiller les appareils de cogestion à l'aide des méthodes suivantes :

- Tableau de bord de cogestion
- **Vue SQL et classe WMI** : vous pouvez interroger la vue SQL **v_ClientCoManagementState** dans la base de données du site Configuration Manager ou la classe WMI **SMS_Client_ComanagementState**. Avec les informations contenues dans la classe WMI, vous pouvez créer des regroupements personnalisés dans Configuration Manager pour vous aider à déterminer l'état du déploiement de la cogestion. Pour plus d'informations, consultez Guide pratique pour créer des regroupements. Les champs suivants sont disponibles dans la vue SQL et la classe WMI :
  - **MachineID** : spécifie un ID d'appareil unique pour le client Configuration Manager.
  - **MDMEnrolled** : spécifie si l'appareil est inscrit à la gestion des appareils mobiles.
  - **Authority** : spécifie l'autorité pour laquelle l'appareil est inscrit.
  - **ComgmtPolicyPresent** : spécifie si la stratégie de cogestion Configuration Manager existe sur le client. Si la valeur **MDMEnrolled** est **0**, l'appareil n'est pas cogéré, que la stratégie de cogestion existe sur le client ou non.

> **NOTE**
> Un appareil est cogéré quand les champs **MDMEnrolled** et **ComgmtPolicyPresent** ont tous les deux la valeur **1**.

- **Stratégies de déploiement** : Il existe deux stratégies créées dans **Surveillance** > **Déploiements** : une stratégie pour le groupe pilote et une stratégie pour la production. Ces stratégies signalent uniquement le nombre d'appareils auxquels Configuration Manager a appliqué la stratégie. Elles ne considèrent pas le nombre d'appareils inscrits dans Intune, ce qui est obligatoire pour pouvoir cogérer des appareils.

## Vérifier la conformité des appareils cogérés

Les utilisateurs peuvent utiliser le Centre logiciel pour vérifier la conformité de leurs appareils Windows 10 cogérés, que l'accès conditionnel soit géré par Configuration Manager ou par Intune. Ils peuvent également vérifier la conformité à l'aide de l'application Portail d'entreprise quand l'accès conditionnel est géré par Intune.

## Étapes suivantes

Utilisez les ressources suivantes pour vous aider à gérer les charges de travail que vous basculez vers Intune :

- Stratégies de conformité des appareils
- Stratégies d'accès aux ressources
- Stratégies Windows Update pour Entreprise
- Endpoint Protection pour Microsoft Intune

# Tableau de bord de cogestion dans System Center Configuration Manager

22/06/2018 • 3 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

À compter de la version 1802, vous pouvez consulter un tableau de bord contenant des informations sur la cogestion. Le tableau de bord vous permet d'examiner les machines qui sont cogérées dans votre environnement. Les graphiques peuvent vous aider à identifier les appareils qui demandent une attention particulière.

## Ouvrir le tableau de bord de cogestion

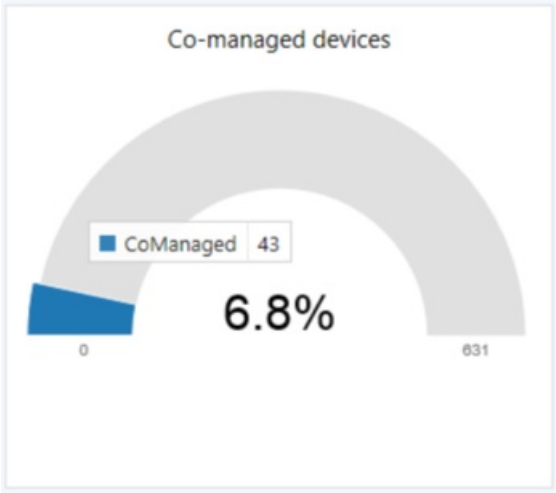
Pour ouvrir le tableau de bord de cogestion, effectuez les étapes suivantes :

1. Ouvrez la console Configuration Manager.
2. Cliquez sur le nœud **Analyse**.
3. Pour charger le tableau de bord, cliquez sur **Cogestion**.

## Consultation des informations contenues dans le tableau de bord de cogestion

Le tableau de bord de cogestion présente quatre graphiques pour votre environnement.

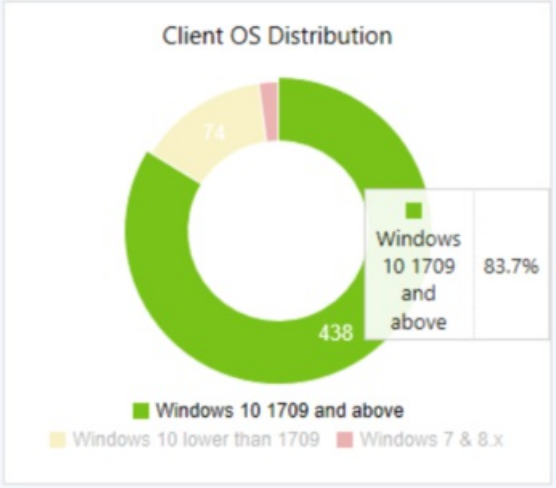
- **Appareils cogérés** : indique le pourcentage d'appareils cogérés dans tout votre environnement.




- **Distribution de système d'exploitation client** : affiche le nombre d'appareils clients par système d'exploitation et par version. Les regroupements suivants sont utilisés :
  - Windows 7 et 8.x
  - Windows 10 antérieur à 1709
  - Windows 10 1709 et ultérieur

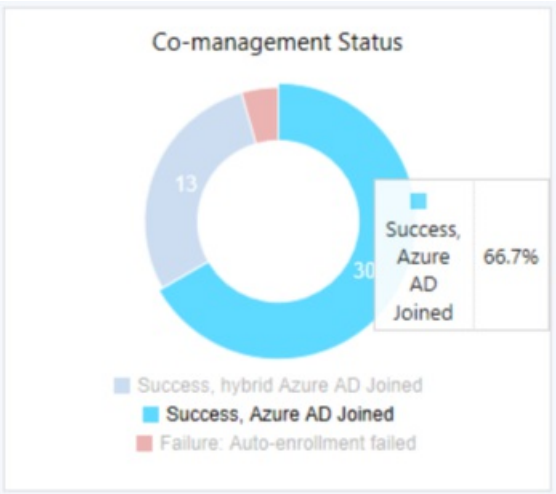
> **NOTE**
> Windows 10, version 1709 et ultérieures, est un prérequis pour la cogestion.

Pointer sur une section du graphique vous donne le pourcentage d'appareils du regroupement de systèmes d'exploitation sélectionné.

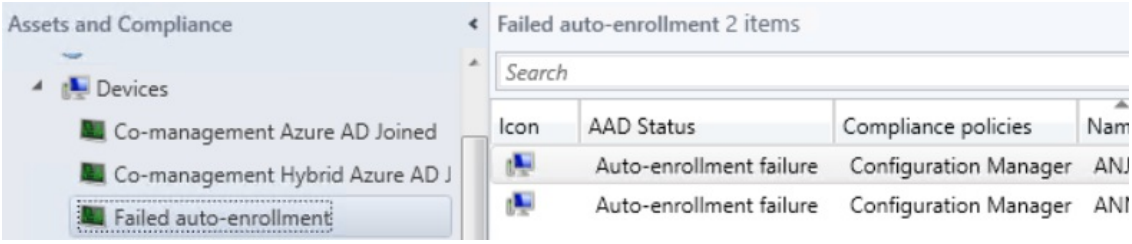



- **État de la cogestion** : répartition des réussites et des échecs des appareils selon les catégories suivantes :
  - Réussite, Joint à une version hybride d'Azure AD
  - Réussite, Joint à Azure AD
  - Échec : Échec de l'inscription automatique

  Pointer sur une section du graphique vous donne le pourcentage d'appareils dans la catégorie.

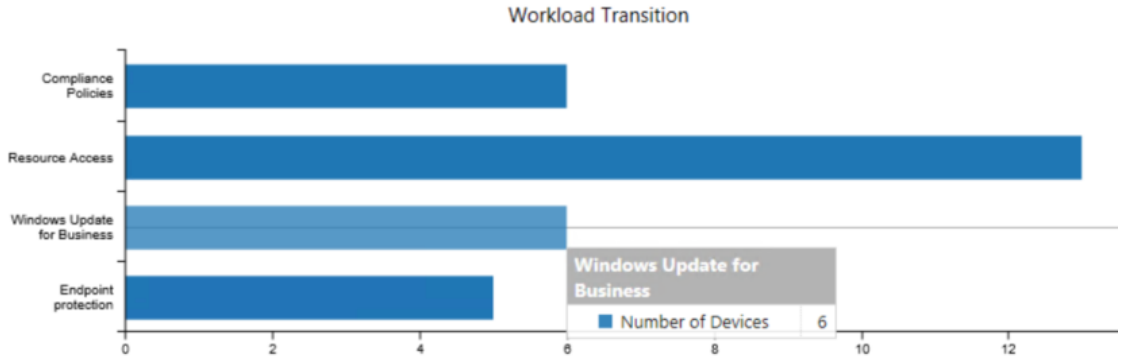



  Cliquer sur une section du graphique vous permet d'accéder à une liste d'appareils pour la catégorie.




- **Transition des charges de travail** : affiche un graphique à barres indiquant le nombre d'appareils que vous avez fait passer à Microsoft Intune pour les quatre charges de travail disponibles :
  - Stratégies de conformité
  - Accès aux ressources
  - Windows Update for Business
  - Endpoint Protection

Pointer sur une section du graphique vous donne le nombre d'appareils transférés pour la charge de travail.




## Étapes suivantes

Pour plus d'informations sur la cogestion, consultez :

- Cogestion pour les appareils Windows 10
- Préparer les appareils Windows 10 pour la cogestion

# Gérer les clients sur Internet avec Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

En général, dans Configuration Manager, la plupart des ordinateurs et serveurs gérés se trouvent physiquement sur le même réseau interne que les serveurs de système de site qui exécutent des fonctions de gestion. Toutefois, vous pouvez gérer les clients en dehors de votre réseau interne quand ils sont connectés à Internet. Cette possibilité ne nécessite pas que les clients se connectent via VPN pour atteindre les serveurs de système de site.

Configuration Manager fournit deux façons de gérer les clients connectés à Internet :

- Passerelle de gestion cloud
- Gestion des clients basés sur Internet

## Passerelle de gestion cloud

La passerelle de gestion cloud permet de gérer les clients Internet. Elle utilise une combinaison d'un service cloud Microsoft Azure et d'un nouveau rôle de système de site qui communique avec ce service. Les clients Internet utilisent le service cloud pour communiquer avec Configuration Manager local.

**Avantages**

- Aucun investissement n'est nécessaire pour l'infrastructure supplémentaire.
- L'infrastructure locale n'est pas exposée sur Internet.
- Les machines virtuelles du cloud qui exécutent le service sont entièrement gérées par Azure et ne nécessitent aucune maintenance.
- Installation et configuration faciles dans la console Configuration Manager.

**Inconvénients**

- Coût de l'abonnement au cloud.
- Données de gestion envoyées via le service cloud.

Pour plus d'informations, consultez Planifier la passerelle de gestion cloud.

## Gestion des clients basés sur Internet

Cette méthode s'appuie sur les serveurs de système de site accessibles sur Internet avec lesquels les clients communiquent à des fins de gestion. Elle nécessite que les clients et serveurs de système de site soient configurés pour une gestion basée sur Internet.

**Avantages**

- Aucune dépendance du service cloud.
- Aucun coût supplémentaire associé à un abonnement au cloud.
- Contrôle total des serveurs et rôles assurant le service.

**Inconvénients**

- Un investissement est nécessaire pour l'infrastructure supplémentaire.

- Frais généraux et coût opérationnel de l’infrastructure supplémentaire.
- L’infrastructure doit être exposée sur Internet.

Pour plus d’informations, consultez Planifier la gestion des clients basés sur Internet.

# Planifier la passerelle de gestion cloud dans Configuration Manager

22/06/2018 • 37 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

La passerelle de gestion cloud fournit un moyen simple de gérer les clients Configuration Manager sur Internet. En déployant la passerelle de gestion cloud comme un service cloud dans Microsoft Azure, vous pouvez gérer les clients traditionnels qui sont itinérants sur Internet sans infrastructure supplémentaire. De même, vous n'avez pas besoin d'exposer votre infrastructure locale sur Internet.

**TIP**

Cette fonctionnalité a été introduite dans la version 1610 en tant que fonctionnalité en préversion. À compter de la version 1802, cette fonctionnalité n'est plus en préversion.

**NOTE**

Par défaut, Configuration Manager n'active pas cette fonctionnalité facultative. Vous devez activer cette fonctionnalité avant de l'utiliser. Pour plus d'informations, consultez Activer les fonctionnalités facultatives des mises à jour.

Une fois les prérequis établis, la création de la passerelle de gestion cloud se fait via les trois étapes suivantes dans la console Configuration Manager :

1. Déployer le service cloud de la passerelle de gestion cloud sur Azure.
2. Ajouter le rôle de point de connexion de passerelle de gestion cloud.
3. Configurer le site et les rôles de site pour le service. Une fois déployés et configurés, les clients accèdent sans problème aux rôles de site locaux, qu'ils soient sur l'intranet ou sur Internet.

Cet article fournit les connaissances de base permettant de découvrir la passerelle de gestion cloud, comment elle s'intègre dans votre environnement, et de planifier l'implémentation.

## Scénarios

La passerelle de gestion cloud présente des avantages dans plusieurs scénarios. Voici quelques-uns des scénarios les plus courants :

- Gérer des clients Windows traditionnels avec une identité jointe à un domaine Active Directory. Ces clients incluent Windows 7, Windows 8.1 et Windows 10. Elle utilise des certificats d'infrastructure à clé publique pour sécuriser le canal de communication. Les activités de gestion sont les suivantes :
  - Mises à jour logicielles et protection des points de terminaison
  - État du parc et des clients
  - Paramètres de conformité
  - Distribution de logiciels à l'appareil
  - Séquence de tâches de mise à niveau sur place de Windows 10 (à partir de la version 1802)
- Gérer les clients Windows 10 traditionnels avec une identité moderne, hybride ou cloud pure et jointe au domaine avec Azure Active Directory (Azure AD). Les clients utilisent Azure AD pour s'authentifier, au lieu

de certificats d'infrastructure à clé publique. L'utilisation d'Azure AD demande une installation, une configuration et une gestion plus simples que pour les systèmes plus complexes des infrastructures à clé publique. Les activités de gestion sont les mêmes que pour le premier scénario, ainsi que :

  - Distribution de logiciels à l'utilisateur
- Installation du client Configuration Manager sur les appareils Windows 10 via Internet. L'utilisation d'Azure AD permet à l'appareil de s'authentifier auprès de la passerelle de gestion cloud pour l'inscription et l'affectation du client. Vous pouvez installer le client manuellement ou via une autre méthode de distribution de logiciels, comme Microsoft Intune.

- Nouveau provisionnement des appareils avec la cogestion. La passerelle de gestion cloud n'est pas obligatoire pour la cogestion. Elle permet de réaliser un scénario de bout en bout pour les nouveaux appareils impliquant Windows AutoPilot, Azure AD, Microsoft Intune et Configuration Manager.

**Cas d'usage spécifiques**

Dans ces scénarios, les cas d'usage d'appareils spécifiques suivants peuvent s'appliquer :

- Appareils itinérants, comme les ordinateurs portables

- Appareils distants ou dans les filiales, dont la gestion est moins coûteuse et plus efficace via Internet que via un réseau WAN ou un VPN.

- Fusions et acquisitions, où il peut être plus facile de joindre des appareils à Azure AD et de les gérer via une passerelle de gestion cloud.

> **IMPORTANT**
> Par défaut, tous les clients reçoivent une stratégie pour une passerelle de gestion cloud et commencent à l'utiliser quand ils sont basés sur Internet. Selon le scénario et le cas d'usage qui s'appliquent à votre organisation, il peut être nécessaire de délimiter l'utilisation de la passerelle de gestion cloud. Pour plus d'informations, consultez le paramètre client Autoriser les clients à utiliser une passerelle de gestion cloud.

# Conception de la topologie

**Composants de la passerelle de gestion cloud**

Le déploiement et le fonctionnement de la passerelle de gestion cloud incluent les composants suivants :

- Le **service cloud de passerelle de gestion cloud** dans Azure authentifie et transfère les demandes des clients Configuration Manager au point de connexion de la passerelle de gestion cloud.

- Le rôle de système de site **Point de connexion de passerelle de gestion cloud** permet une connexion cohérente et hautes performances entre le réseau local et le service de passerelle de gestion cloud dans Azure. Il publie également les paramètres sur la passerelle de gestion cloud, notamment les informations de connexion et les paramètres de sécurité. Le point de connexion de la passerelle de gestion cloud transfère les demandes des clients de la passerelle de gestion cloud vers les rôles locaux en fonction des mappages d'URL.

- Le rôle de système de site **Point de connexion de service** exécute le composant du gestionnaire de service cloud, qui gère toutes les tâches de déploiement de la passerelle de gestion cloud. En outre, il surveille et transmet les informations d'intégrité du service et de journalisation à partir d'Azure AD. Vérifiez que votre point de connexion de service est en mode en ligne.

- Le rôle de système de site **Point de gestion** traite normalement les demandes des clients des services.

- Le rôle de système de site **Point de mise à jour logicielle** traite normalement les demandes des clients des services.

- **Les clients Internet** se connectent à la passerelle de gestion cloud pour accéder aux composants de Configuration Manager local.
- La passerelle de gestion cloud utilise un service web **HTTPS basé sur un certificat** pour sécuriser la communication réseau avec les clients.
- Les clients Internet utilisent **des certificats d'infrastructure à clé publique ou Azure AD** pour l'identité et l'authentification.
- Un **point de distribution cloud** fournit du contenu aux clients Internet selon les besoins.

### Azure Resource Manager

Depuis la version 1802, vous pouvez créer la passerelle de gestion cloud en utilisant un **déploiement Azure Resource Manager**. Azure Resource Manager est une plateforme moderne permettant de gérer l'ensemble des ressources de la solution comme une seule entité, nommée groupe de ressources. Lors du déploiement d'une Passerelle CMG avec Azure Resource Manager, le site utilise Azure Active Directory (Azure AD) pour authentifier et créer les ressources cloud nécessaires. Le certificat de gestion Azure classique n'est pas nécessaire pour ce déploiement modernisé.

L'Assistant CMG propose toujours l'option de **déploiement de service classique** à l'aide d'un certificat de gestion Azure. Pour simplifier le déploiement et la gestion des ressources, l'utilisation du modèle de déploiement Azure Resource Manager est recommandé pour toutes les nouvelles instances de passerelle de gestion cloud. Si possible, redéployez les instances CMG existantes avec Resource Manager. Pour plus d'informations, consultez Modifier une passerelle de gestion cloud.

> **IMPORTANT**
> Cette fonctionnalité ne permet pas la prise en charge des fournisseurs de services cloud Azure. Le déploiement CMG avec Azure Resource Manager continue d'utiliser le service cloud classique, que ne prend pas en charge le fournisseur de services cloud. Pour plus d'informations, consultez les services Azure disponibles auprès du fournisseur de services cloud Azure.

### Conception de hiérarchie

Créez la passerelle de gestion cloud sur le site de plus haut niveau de votre hiérarchie. S'il s'agit d'un site d'administration centrale, créez des points de connexion de passerelle de gestion cloud sur les sites principaux enfants. Le composant du gestionnaire de service cloud se trouve sur le point de connexion du service, qui est également sur le site d'administration centrale. Cette conception permet si nécessaire de partager le service entre différents sites principaux.

Vous pouvez créer plusieurs services de passerelle de gestion cloud dans Azure et plusieurs points de connexion de passerelle de gestion cloud. Des points de connexion de passerelle de gestion cloud multiples permettent l'équilibrage de charge du trafic client depuis la passerelle de gestion cloud vers les rôles locaux. Pour réduire la latence du réseau, affectez la passerelle de gestion cloud associée à la même région géographique que le site principal.

> **NOTE**
> Les clients Internet et la passerelle de gestion cloud ne sont dans aucun groupe de limites.

D'autres facteurs, comme le nombre de clients à gérer, impactent également votre conception de la passerelle de gestion cloud. Pour plus d'informations, consultez Performances et échelle.

#### Exemple 1 : Site principal autonome

Contoso a un site principal autonome dans un centre de données local à son siège social de New York.

- Le département informatique crée une passerelle de gestion cloud dans la région Azure États-Unis de l'Est pour

réduire la latence du réseau.

- Il crée deux points de connexion de passerelle de gestion cloud, les deux étant liés au même service de passerelle de gestion cloud.

Quand les clients se déplacent et utilisent Internet, ils communiquent avec la passerelle de gestion cloud dans la région Azure États-Unis de l'Est. La passerelle de gestion cloud transfère cette communication via les deux points de connexion de passerelle de gestion cloud.

**Exemple 2 : Hiérarchie avec une passerelle de gestion cloud spécifique au site**

Fourth Coffee a un site d'administration centrale dans un centre de données local à son siège social de Seattle. Un site principal se trouve dans le même centre de données, et l'autre site principal se trouve dans son bureau européen principal à Paris.

- Sur le site d'administration centrale, le département informatique crée deux services de passerelle de gestion cloud :
  - Une passerelle de gestion cloud dans la région Azure États-Unis de l'Ouest.
  - Une passerelle de gestion cloud dans la région Azure Europe de l'Ouest.
- Sur le site principal de Seattle, il crée un point de connexion de passerelle de gestion cloud lié à la passerelle de gestion cloud États-Unis de l'Ouest.
- Sur le site principal de Paris, il crée un point de connexion de passerelle de gestion cloud lié à la passerelle de gestion cloud Europe de l'Ouest.

Quand les clients basés à Seattle se déplacent et utilisent Internet, ils communiquent avec la passerelle de gestion cloud dans la région Azure États-Unis de l'Ouest. La passerelle de gestion cloud transfère cette communication au point de connexion de passerelle de gestion cloud basé à Seattle.

De même, quand les clients basés à Paris se déplacent et utilisent Internet, ils communiquent avec la passerelle de gestion cloud dans la région Azure Europe de l'Ouest. La passerelle de gestion cloud transfère cette communication au point de connexion de passerelle de gestion cloud basé à Paris. Quand des utilisateurs basés à Paris se déplacent au siège de la société à Seattle, leurs ordinateurs continuent de communiquer avec la passerelle de gestion cloud dans la région Azure Europe de l'Ouest.

> **NOTE**
>
> Fourth Coffee a envisagé la création d'un autre point de connexion de passerelle de gestion cloud sur le site principal de Paris lié à la passerelle de gestion cloud États-Unis de l'Ouest. Les clients basés à Paris utiliseraient alors les deux passerelles de gestion cloud, quel que soit l'endroit où ils se trouvent. Si cette configuration permet d'équilibrer le trafic et offre une redondance du service, elle peut également entraîner des délais quand des clients basés à Paris communiquent avec la passerelle de gestion cloud basée aux États-Unis. Les clients Configuration Manager ne sont pas informés de leur région géographique et ne cherchent donc pas à préférer une passerelle de gestion cloud qui est géographiquement plus proche. Les clients utilisent de façon aléatoire une passerelle de gestion cloud disponible.

## spécifications

- Un **abonnement Azure** pour héberger la passerelle de gestion cloud.
  - Un **administrateur Azure** doit participer à la création initiale de certains composants, en fonction de votre conception. Cette personne n'a pas besoin d'autorisations dans Configuration Manager.
- Au moins un serveur Windows local pour héberger le **point de connexion de passerelle de gestion cloud**. Vous pouvez colocaliser ce rôle avec d'autres rôles de système de site Configuration Manager.
- Le **point de connexion de service** doit être en mode en ligne.
- Un **certificat d'authentification serveur** pour la passerelle de gestion cloud.

- Si vous utilisez la méthode de déploiement classique Azure, vous devez utiliser un **certificat de gestion Azure**.

  > **TIP**
  > À compter de Configuration Manager version 1802, l'utilisation du modèle de déploiement **Azure Resource Manager** est recommandé. Il ne nécessite pas ce certificat de gestion.

- **D'autres certificats** peuvent être nécessaires, en fonction de la version du système d'exploitation et du modèle d'authentification de votre client. Pour plus d'informations, consultez Certificats de passerelle de gestion cloud.
  - À compter de la version 1802, vous devez configurer tous les **points de gestion activés pour la passerelle de gestion cloud afin d'utiliser le protocole HTTPS**.
- L'intégration à **Azure AD** peut être nécessaire pour les clients Windows 10. Pour plus d'informations, consultez Configurer des services Azure.
- Les clients doivent utiliser **IPv4**.

## Spécifications

- Toutes les versions de Windows listées dans Systèmes d'exploitation pris en charge pour les clients et les appareils sont prises en charge pour la passerelle de gestion cloud.
- La passerelle de gestion cloud prend en charge les rôles Point de gestion et Point de mise à jour logicielle.
- La passerelle de gestion cloud ne prend pas en charge les clients qui communiquent seulement avec des adresses IPv6.
- Les points de mise à jour logicielle utilisant un équilibreur de charge réseau ne fonctionnent pas avec la passerelle de gestion cloud.
- À compter de la version 1802, les déploiements de passerelle de gestion cloud avec le modèle Azure Resource manager ne permettent pas la prise en charge des fournisseurs de services cloud Azure. Le déploiement CMG avec Azure Resource Manager continue d'utiliser le service cloud classique, que ne prend pas en charge le fournisseur de services cloud. Pour plus d'informations, consultez les services Azure disponibles dans les fournisseurs de services cloud Azure.

**Prise en charge des fonctionnalités de Configuration Manager**

Le tableau suivant détaille la prise en charge par la passerelle de gestion cloud des fonctionnalités de Configuration Manager :

| FONCTIONNALITÉ | ASSISTANCE |
|---|---|
| Mises à jour logicielles | ✓ |
| Endpoint Protection | ✓ |
| Inventaire matériel et logiciel | ✓ |
| État du client et notifications | ✓ |
| Exécuter les scripts | ✓ |

| FONCTIONNALITÉ | ASSISTANCE |
| --- | --- |
| Paramètres de conformité | ✅ |
| Installation du client<br>(avec intégration d'Azure AD) | ✅ (1706) |
| Distribution de logiciels (ciblée sur des appareils) | ✅ |
| Distribution de logiciels (ciblée sur des utilisateurs, obligatoires)<br>(avec intégration d'Azure AD) | ✅ (1710) |
| Distribution de logiciels (ciblée sur des utilisateurs, disponibles)<br>(toutes les exigences) | ✅ (1802) |
| Séquence de tâches de mise à niveau sur place de Windows 10 | ✅ (1802) |
| Tous les autres scénarios de séquence de tâches | ❌ |
| Installation Push du client | ❌ |
| Attribution automatique du site | ❌ |
| Catalogue d'applications | ❌ |
| Demandes d'approbation de logiciel | ❌ |
| Console Configuration Manager | ❌ |
| outils de contrôle à distance. | ❌ |
| Site web de création de rapports | ❌ |
| Éveil par appel réseau | ❌ |
| Clients Mac, Linux et UNIX | ❌ |
| Cache d'homologue | ❌ |
| Gestion des appareils mobiles locale | ❌ |

| CLÉ |
| --- |
| ✅ = Cette fonctionnalité est prise en charge avec la passerelle de gestion cloud par toutes les versions prises en charge de Configuration Manager |
| ✅ (*AAMM*) = cette fonctionnalité est prise en charge avec la passerelle de gestion cloud depuis la version *AAMM* de Configuration Manager |

| CLÉ |
| --- |
| ❌ = Cette fonctionnalité n'est pas prise en charge avec la passerelle de gestion cloud. |

# Coût

> **IMPORTANT**
> Les informations suivantes sur les coûts sont données à titre d'estimation seulement. Votre environnement peut avoir d'autres variables qui affectent le coût total d'utilisation de la passerelle de gestion cloud.

La passerelle de gestion cloud utilise les composants Azure suivants, qui impliquent des frais pour le compte de l'abonnement Azure :

**Machine virtuelle**

- La passerelle de gestion cloud utilise les services cloud Azure comme PaaS (plateforme en tant que service). Ce service utilise des machines virtuelles qui génèrent des coûts de calcul.
- Dans Configuration Manager version 1706, la passerelle de gestion cloud utilise une machine virtuelle Standard A2.
- À compter de Configuration Manager version 1710, la passerelle de gestion cloud utilise une machine virtuelle Standard A2 V2.
- Vous choisissez le nombre d'instances de machine virtuelle qui prennent en charge la passerelle de gestion cloud. La valeur par défaut est 1 et 16 est le maximum. Ce nombre est défini lors de la création de la passerelle de gestion cloud et il peut être changé ultérieurement pour faire évoluer le service en fonction des besoins.
- Pour plus d'informations sur le nombre de machines virtuelles dont vous avez besoin pour prendre en charge vos clients, consultez Performances et évolutivité.
- Pour vous aider à déterminer les coûts potentiels, consultez la calculatrice de prix Azure.

  > **NOTE**
  > Les coûts des machines virtuelles varient selon la région.

**Transfert de données sortantes**

- Les frais sont calculés d'après les données qui sortent d'Azure (sortie ou téléchargement). Les flux de données entrant dans Azure sont gratuits (entrée ou chargement). Les flux de données de la passerelle de gestion cloud sortant d'Azure incluent la stratégie pour le client, les notifications au client et les réponses au client transférées au site par la passerelle de gestion cloud. Ces réponses incluent les rapports d'inventaire, les messages d'état et l'état de conformité.
- Même si aucun client ne communique avec une passerelle de gestion cloud, certaines communications d'arrière-plan engendrent du trafic réseau entre la passerelle de gestion cloud et le site local.
- Consultez le **Transfert de données sortantes (Go)** dans la console Configuration Manager. Pour plus d'informations, consultez Surveiller les clients sur une passerelle de gestion cloud.
- Pour vous aider à déterminer les coûts potentiels, consultez les détails de la tarification de la bande passante. La tarification pour le transfert de données est à plusieurs niveaux. Plus votre utilisation augmente, moins vous payez par gigaoctet.

- *À titre d'estimation seulement*, prévoyez environ 100 à 300 Mo par client par mois pour les clients Internet. L'estimation la plus basse est pour une configuration de client par défaut. L'estimation la plus haute est pour une configuration de client plus active. Votre utilisation réelle peut varier en fonction de la façon dont vous configurez les paramètres du client.

  > **NOTE**
  > La réalisation d'autres actions, comme le déploiement de mises à jour logicielles ou d'applications, fait augmenter la quantité de données sortantes transférées depuis Azure.

**Stockage de contenu**

- Les clients Internet obtiennent gratuitement le contenu des mises à jour de logiciels Microsoft auprès de Windows Update. Ne distribuez pas des packages de mises à jour avec du contenu de mise à jour Microsoft sur un point de distribution cloud, sinon des frais de stockage et de sortie de données vous sont facturés.
- Pour tout autre contenu nécessaire, comme des applications ou des mises à jour de logiciels tiers, vous devez distribuer sur un point de distribution cloud. Actuellement, la passerelle de gestion cloud prend en charge le point de distribution cloud seulement pour l'envoi de contenu à des clients.
- Pour plus d'informations, reportez-vous au coût d'utilisation de la distribution cloud.

**Autres coûts**

- Chaque service cloud a une adresse IP dynamique. Chaque passerelle de gestion cloud distincte utilise une nouvelle adresse IP dynamique. L'ajout de machines virtuelles supplémentaires par passerelle de gestion cloud n'augmente pas le nombre de ces adresses.

## Performances et évolutivité

Pour plus d'informations sur l'évolutivité de la passerelle de gestion cloud, consultez Taille et échelle en chiffres.

Les recommandations suivantes peuvent vous aider à améliorer les performances de la passerelle de gestion cloud :

- Si possible, configurez la passerelle CMG, le point de connexion CMG et le serveur de site Configuration Manager dans la même région pour réduire la latence du réseau.
- Actuellement, la connexion entre le client Configuration Manager et la passerelle CMG ne tient pas compte de la région.
- Pour un service à haute disponibilité, créez au moins deux services de passerelle de gestion cloud et deux points de connexion de passerelle de gestion cloud par site.
- Faites évoluer la passerelle de gestion cloud pour prendre en charge plus de clients en ajoutant d'autres instances de machine virtuelle. L'équilibrage de charge Azure contrôle les connexions des clients au service.
- Créez plusieurs points de connexion CMG pour répartir la charge entre ces points. La passerelle de gestion cloud distribue le trafic à ses points de connexion de passerelle de gestion cloud via un tourniquet (round-robin).
- Quand la passerelle de gestion cloud subit une charge élevée en raison d'un dépassement du nombre de clients pris en charge, elle gère néanmoins les demandes, mais des délais sont possibles.

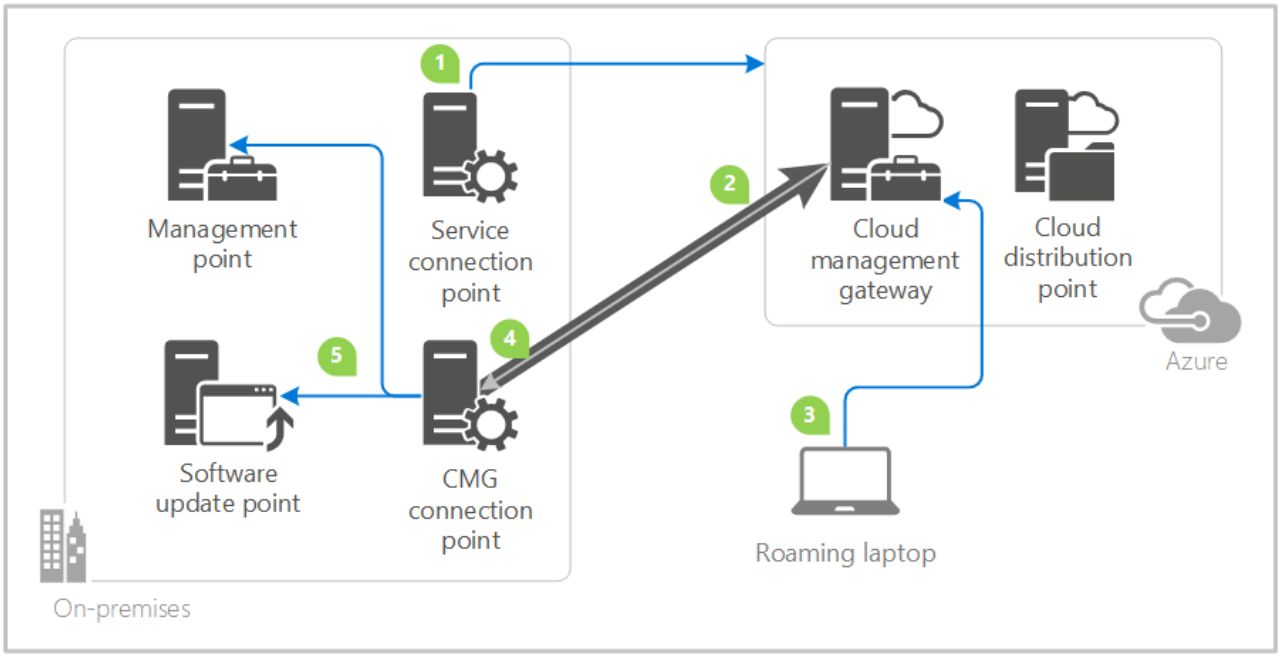
**NOTE**

Si Configuration Manager n'a aucune limite matérielle quant au nombre de clients pour un point de connexion de passerelle de gestion cloud, Windows Server a une plage de ports dynamiques TCP maximale par défaut de 16 384. Si un site Configuration Manager gère plus de 16 384 clients avec un seul point de connexion de passerelle de gestion cloud, vous devez augmenter la limite de Windows Server. Tous les clients gèrent un canal pour les notifications des clients, qui détient un port ouvert sur le point de connexion de la passerelle de gestion cloud. Pour plus d'informations sur l'utilisation de la commande netsh pour augmenter cette limite, consultez Article du Support Microsoft 929851.

## Ports et flux de données

Vous n'avez pas besoin d'ouvrir des ports entrants sur votre réseau local. Le point de connexion du service et le point de connexion de la passerelle de gestion cloud lancent toutes les communications avec Azure et la passerelle de gestion cloud. Ces deux rôles de système de site doivent être en mesure de créer des connexions sortantes vers le cloud Microsoft. Le point de connexion du service déploie et surveille le service dans Azure : il doit donc être en mode en ligne. Le point de connexion de la passerelle de gestion cloud se connecte à la passerelle de gestion cloud pour gérer les communications entre la passerelle et les rôles de système de site locaux.

Le diagramme suivant est un flux de données conceptuel de base pour la passerelle de gestion cloud :




1. Le point de connexion du service se connecte à Azure via le port HTTPS 443. Il s'authentifie avec Azure AD ou avec le certificat de gestion Azure. Le point de connexion du service déploie la passerelle de gestion cloud dans Azure. La passerelle de gestion cloud crée le service cloud HTTPS en utilisant le certificat d'authentification serveur.

2. Le point de connexion de la passerelle de gestion cloud se connecte à la passerelle dans Azure via TCP-TLS ou HTTPS. Il laisse la connexion ouverte et crée le canal pour la communication bidirectionnelle à venir.

3. Le client se connecte à la passerelle de gestion cloud sur le port HTTPS 443. Il s'authentifie avec Azure AD ou avec le certificat d'authentification client.

4. La passerelle de gestion cloud transfère la communication client via la connexion existante au point de connexion de la passerelle de gestion cloud. Vous n'avez pas besoin d'ouvrir des ports de pare-feu entrants.

5. Le point de connexion de la passerelle de gestion cloud transfère la communication client au point de gestion local et au point de mise à jour logicielle.

**Ports nécessaires**

Ce tableau répertorie les ports et les protocoles réseau nécessaires. Le *client* est l'appareil qui lance la connexion, qui nécessite un port sortant. Le *serveur* est l'appareil qui accepte la connexion, qui nécessite un port entrant.

| CLIENT | PROTOCOLE | PORT | SERVEUR | DESCRIPTION |
|---|---|---|---|---|
| point de connexion de service | HTTPS | 443 | Azure | Déploiement CMG |
| Point de connexion CMG | TCP-TLS | 10140-10155 | Service de passerelle de gestion cloud | Protocole préféré pour créer le canal de passerelle de gestion cloud[1] |
| Point de connexion CMG | HTTPS | 443 | Service de passerelle de gestion cloud | Alternative de secours pour créer le canal de passerelle de gestion cloud pour une seule instance de machine virtuelle[2] |
| Point de connexion CMG | HTTPS | 10124-10139 | Service de passerelle de gestion cloud | Alternative de secours pour créer le canal de passerelle de gestion cloud pour plusieurs instances de machine virtuelle[3] |
| Client | HTTPS | 443 | CMG | Communication client générale |
| Point de connexion CMG | HTTPS ou HTTP | 443 ou 80 | Point de gestion (version 1706 ou 1710) | Trafic local, le port dépend de la configuration du point de gestion |
| Point de connexion CMG | HTTPS | 443 | Point de gestion (version 1802) | Le trafic de local doit être sur HTTPS |
| Point de connexion CMG | HTTPS ou HTTP | 443 ou 80 | Point de mise à jour logicielle | Trafic local, le port dépend de la configuration du point de mise à jour logicielle |

[1] Le point de connexion de la passerelle de gestion cloud tente d'abord d'établir une connexion TCP-TLS à long terme avec chaque instance de machine virtuelle de la passerelle. Il se connecte à la première instance de machine virtuelle sur le port 10140. La deuxième instance de machine virtuelle utilise le port 10141, jusqu'à la seizième sur le port 10155. Une connexion TCP-TLS offre les meilleures performances, mais elle ne prend pas en charge le proxy Internet. Si le point de connexion de la passerelle de gestion cloud ne peut pas se connecter via TCP-TLS, elle passe à l'alternative de secours HTTPS[2].

[2] Si le point de connexion de la passerelle de gestion cloud ne peut pas se connecter à la passerelle via TCP-TLS[1], il se connecte à l'équilibreur de charge réseau Azure via HTTPS 443 pour une seule instance de machine virtuelle.

[3] S'il existe plusieurs instances de machine virtuelle, le point de connexion de la passerelle de gestion cloud utilise le protocole HTTPS 10124 avec première instance de machine virtuelle, et non pas HTTPS 443. Il se connecte à la deuxième instance de machine virtuelle via HTTPS 10125, jusqu'à la seizième sur le port HTTPS 10139.

**Conditions requises pour l'accès Internet**

Le système de site du point de connexion de la passerelle de gestion cloud prend en charge l'utilisation d'un proxy web. Pour plus d'informations sur la configuration de ce rôle pour un proxy, consultez Prise en charge d'un serveur proxy. Le point de connexion de la passerelle de gestion cloud nécessite une connexion aux points de terminaison suivants :

- Les points de terminaison Azure spécifiques sont différents pour chaque environnement, en fonction de la configuration. Configuration Manager stocke ces points de terminaison dans la base de données du site. Pour obtenir la liste des points de terminaison Azure, interrogez la table **AzureEnvironments** dans SQL Server.
- ServiceManagementEndpoint (https://management.core.windows.net/)
- StorageEndpoint (core.windows.net)
- Pour la récupération du jeton Azure AD par la console Configuration Manager et le client : ActiveDirectoryEndpoint ()https://login.microsoftonline.com/)
- Pour la découverte des utilisateurs Azure AD : point de terminaison du graphe AAD (https://graph.windows.net/)

## Étapes suivantes

- Certificats pour la passerelle de gestion cloud
- Sécurité et confidentialité de la passerelle de gestion cloud
- Taille et scalabilité de la passerelle de gestion cloud en chiffres
- Questions fréquentes (FAQ) sur la passerelle de gestion cloud
- Configurer la passerelle de gestion cloud

# Sécurité et confidentialité de la passerelle de gestion cloud

22/06/2018 • 8 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cet article inclut des informations sur la sécurité et la confidentialité pour la passerelle de gestion cloud (CMG) Configuration Manager. Pour plus d'informations, consultez Planifier la passerelle de gestion cloud.

## Informations sur la sécurité de la passerelle de gestion cloud (CMG)

- La passerelle de gestion cloud accepte et gère les connexions à partir de points de connexion CMG. Elle utilise l'authentification mutuelle SSL à l'aide de certificats et d'ID de connexion.
- La passerelle de gestion cloud accepte et transfère les requêtes client à l'aide des méthodes suivantes :
  - Authentifie au préalable les connexions à l'aide d'un protocole SSL mutuel avec le certificat d'authentification client basé sur une infrastructure à clé publique (PKI) ou Azure AD.
    - IIS sur les instances de machine virtuelle de la passerelle de gestion cloud vérifie que le chemin du certificat basé sur les certificats racines approuvés est chargé sur la passerelle de gestion cloud.
    - IIS sur les instances de machine virtuelle vérifie également la révocation des certificats clients, si elle est activée. Pour plus d'informations, consultez Publication de la liste de révocation de certificats.
  - La liste de certificats de confiance vérifie la racine du certificat d'authentification client. Elle effectue également la même validation que le point de gestion pour le client. Pour plus d'informations, consultez Examiner les entrées de la liste de certificats de confiance du site.
  - Valide et filtre les requêtes client (URL) pour vérifier si un point de connexion CMG peut traiter la requête.
  - Vérifie la longueur du contenu pour chaque point de terminaison de publication.
  - Utilise le comportement de tourniquet (round robin) pour équilibrer la charge des points de connexion CMG sur le même site.
- Le point de connexion CMG utilise les méthodes suivantes :
  - Crée des connexions HTTPS/TCP cohérentes pour toutes les instances de machine virtuelle à la passerelle de gestion cloud. Il vérifie et gère ces connexions toutes les minutes.
  - Utilise l'authentification mutuelle SSL avec la passerelle de gestion cloud à l'aide de certificats.
  - Transfère les requêtes client basées sur des mappages d'URL.
  - Indique l'état de la connexion pour afficher l'état d'intégrité du service dans la console.
  - Indique le trafic par point de terminaison toutes les cinq minutes.

**Rôles Configuration Manager utilisés par le client**

Le point de gestion et le point de mise à jour logicielle hébergent des points de terminaison dans IIS pour traiter les requêtes client. La passerelle de gestion cloud n'expose pas tous les points de terminaison internes. Chaque point de terminaison publié sur la passerelle CMG comporte un mappage d'URL.

- L'URL externe est celle que le client utilise pour communiquer avec la passerelle CMG.
- L'URL interne est le point de connexion CMG utilisé pour transférer les demandes vers le serveur interne.

**Exemple de mappage d'URL**

Quand vous activez le trafic CMG sur un point de gestion, Configuration Manager crée un ensemble interne de mappages d'URL pour chaque serveur de point de gestion. Par exemple : ccm_system, ccm_incoming et sms_mp.

L'URL externe du point de terminaison ccm_system du point de gestion peut se présenter ainsi :

```
https://<CMG service name>/CCM_Proxy_MutualAuth/<MP Role ID>/CCM_System
```

L'URL est unique pour chaque point de gestion. Le client Configuration Manager place ensuite le nom du point de gestion activé pour la passerelle de gestion cloud dans sa liste de points de gestion Internet. Ce nom se présente comme suit :

```
<CMG service name>/CCM_Proxy_MutualAuth/<MP Role ID>
```

Le site charge automatiquement toutes les URL externes publiées sur la passerelle de gestion cloud. Ce comportement permet à la passerelle de gestion cloud d'effectuer un filtrage des URL. Tous les mappages d'URL sont répliqués sur le point de connexion CMG. Il transfère ensuite la communication vers les serveurs internes en fonction de l'URL externe à partir de la requête client.

## Conseils en matière de sécurité pour la passerelle de gestion cloud

**Publication de la liste de révocation de certificats**

Publiez la liste de révocation de certificats de votre infrastructure à clé publique (PKI) pour permettre l'accès des clients Internet. Quand vous déployez une passerelle de gestion cloud à l'aide de l'infrastructure à clé publique, configurez le service sur **Vérifier la révocation des certificats clients** sous l'onglet Paramètres. Ce paramètre configure le service pour qu'il utilise une liste de révocation de certificats publiée. Pour plus d'informations, consultez Planifier la révocation de certificats PKI.

**Examiner les entrées de la liste de certificats de confiance du site**

Chaque site Configuration Manager inclut une liste d'autorités de certification racines de confiance, la liste de certificats de confiance (CTL, Certificate Trust List). Pour consulter et modifier cette liste, accédez à l'espace de travail Administration, développez Configuration du site, puis sélectionnez Sites. Sélectionnez un site, puis cliquez sur Propriétés dans le ruban. Basculez vers l'onglet Communication de l'ordinateur client, puis cliquez sur **Définir** sous Autorités de certification racines de confiance.

Utilisez une liste de certificats de confiance plus restrictive pour un site avec une passerelle de gestion cloud à l'aide de l'authentification client PKI. Sinon, les clients disposant de certificats d'authentification client émis par toute racine de confiance qui existe déjà sur le point de gestion sont automatiquement acceptés pour l'inscription du client.

Ce sous-ensemble confère aux administrateurs un contrôle accru de la sécurité. La liste de certificats de confiance limite le serveur à accepter uniquement les certificats clients émis par les autorités de certification figurant dans cette liste. Par exemple, Windows est fourni avec différents certificats d'autorités de certification tierces renommées, telles que VeriSign et Thawte. Par défaut, l'ordinateur qui exécute les services Internet (IIS) approuve les certificats liés à ces autorités de certification connues. Sans configuration d'IIS avec une liste de certificats de confiance, tout ordinateur avec un certificat client publié par ces autorités de certification est accepté comme client Configuration Manager valide. Si vous configurez IIS avec une liste de certificats de confiance qui ne comprend pas ces autorités de certification, les connexions clientes sont rejetées si le certificat était lié à ces autorités de certification.

## Étapes suivantes

- Planifier la passerelle de gestion cloud
- Configurer la passerelle de gestion cloud
- Questions fréquentes (FAQ) sur la passerelle de gestion cloud
- Certificats pour la passerelle de gestion cloud

# Questions fréquentes (FAQ) sur la passerelle de gestion cloud

22/06/2018 • 3 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cet article répond aux questions que vous vous posez fréquemment concernant la passerelle de gestion cloud (CMG, Cloud Management Gateway). Pour plus d'informations, consultez Planifier la passerelle de gestion cloud.

## Forum aux questions

**De quels certificats ai-je besoin ?**

Pour des informations plus détaillées, consultez Certificats pour la passerelle de gestion cloud.

**Ai-je besoin d'Azure ExpressRoute ?**

Azure ExpressRoute vous permet d'étendre votre réseau local dans Microsoft Cloud. ExpressRoute, ou d'autres connexions de réseau virtuel du même type, ne sont pas exigés pour la passerelle de gestion cloud Configuration Manager. La conception de la passerelle de gestion cloud permet aux clients Internet de communiquer via le service Azure avec des systèmes de site locaux sans aucune configuration réseau supplémentaire. Pour plus d'informations, consultez Planifier la passerelle de gestion cloud.

Si votre organisation utilise ExpressRoute, une bonne pratique de sécurité consiste à isoler l'abonnement Azure pour la passerelle de gestion cloud. Cette configuration garantit que le service de passerelle de gestion cloud n'est pas connecté par inadvertance de cette manière. Pour plus d'informations, consultez Sécurité et confidentialité de la passerelle de gestion cloud.

**Ai-je besoin d'assurer la maintenance des machines virtuelles Azure ?**

Aucune maintenance n'est nécessaire. La conception de la passerelle de gestion cloud utilise Azure PaaS (Platform as a Service). Configuration Manager utilise l'abonnement que vous fournissez pour créer les machines virtuelles, le stockage et le réseau nécessaires. Azure sécurise et met à jour les machines virtuelles. Ces machines virtuelles ne font pas partie de votre environnement local, comme c'est le cas avec IaaS (Infrastructure as a Service). La passerelle de gestion cloud est un service PaaS qui étend votre environnement Configuration Manager dans le cloud.

**J'utilise déjà la gestion du client basée sur Internet (IBCM, Internet-Based Client Management). Si j'ajoute la passerelle de gestion cloud (CMG), comment se comportent les clients ?**

Si vous avez déjà déployé la gestion du client basée sur Internet (IBCM), vous pouvez également déployer la passerelle de gestion cloud. Les clients reçoivent la stratégie pour les deux services. Quand ils se déplacent et utilisent Internet, ils sélectionnent et utilisent de façon aléatoire l'un de ces services Internet.

## Étapes suivantes

- Planifier la passerelle de gestion cloud
- Configurer la passerelle de gestion cloud
- Certificats pour la passerelle de gestion cloud
- Sécurité et confidentialité de la passerelle de gestion cloud
- Taille et scalabilité de la passerelle de gestion cloud en chiffres

# Certificats pour la passerelle de gestion cloud

18/06/2018 • 15 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Selon le scénario que vous utilisez pour gérer des clients sur Internet avec la passerelle de gestion cloud, vous avez besoin d'un ou de plusieurs certificats numériques. Pour plus d'informations sur les différents scénarios, consultez Planifier la passerelle de gestion cloud.

## Certificat d'authentification serveur de passerelle de gestion cloud

*Ce certificat est obligatoire dans tous les scénarios.*

Vous fournissez ce certificat lors de la création de la passerelle de gestion cloud dans la console Configuration Manager.

La passerelle de gestion cloud crée un service HTTPS auquel les clients Internet se connectent. Le serveur nécessite un certificat d'authentification serveur pour créer le canal sécurisé. Achetez un certificat à cet effet auprès d'un fournisseur public ou émettez-le à partir de votre infrastructure à clé publique. Pour plus d'informations, consultez Certificat racine approuvé de passerelle de gestion cloud pour les clients.

> **TIP**
> Ce certificat nécessite un nom global unique pour identifier le service dans Azure. Avant de demander un certificat, vérifiez que le nom de domaine Azure souhaité est unique. Par exemple, *GraniteFalls.CloudApp.Net*. Connectez-vous au portail Microsoft Azure. Cliquez sur **Créer une ressource**, sélectionnez la catégorie **Calcul**, puis cliquez sur **Service cloud**. Dans le champ **Nom DNS**, tapez le préfixe souhaité, par exemple *GraniteFalls*. L'interface indique si le nom de domaine est disponible ou déjà utilisé par un autre service. Ne créez pas le service dans le portail ; utilisez ce processus seulement pour vérifier la disponibilité du nom.

> **NOTE**
> À compter de la version 1802, le certificat d'authentification du serveur de passerelle de gestion cloud prend en charge les caractères génériques. Certaines autorités de certification émettent des certificats en utilisant un caractère générique pour le nom d'hôte. Par exemple, ***.contoso.com**. Certaines organisations utilisent des certificats génériques pour simplifier leur infrastructure à clé publique et réduire les coûts de maintenance.

### Certificat racine approuvé de passerelle de gestion cloud pour les clients

Les clients doivent approuver le certificat d'authentification serveur de la passerelle de gestion cloud. Deux méthodes existent pour effectuer cette approbation :

- Utiliser un certificat provenant d'un fournisseur de certificats public et approuvés globalement. Par exemple, DigiCert, Thawte ou VeriSign (liste non limitative). Les clients Windows incluent des autorités de certification racine approuvées provenant de ces fournisseurs. Si vous utilisez un certificat d'authentification serveur émis par un de ces fournisseurs, vos clients l'approuvent automatiquement.
- Utiliser un certificat émis par une autorité de certification d'entreprise depuis votre infrastructure à clé publique. La plupart des implémentations d'infrastructure à clé publique d'entreprise ajoutent les autorités de certification racine de confiance aux clients Windows. Par exemple, dans le cas d'une utilisation des services de certificats Active Directory avec la stratégie de groupe. Si vous émettez le certificat d'authentification serveur de passerelle de gestion cloud depuis une autorité de certification que vos clients n'approuvent pas automatiquement, vous

devez ajouter le certificat racine approuvé de l'autorité de certification aux clients Internet.
    - Vous pouvez également utiliser des profils de certificat Configuration Manager pour provisionner des certificats sur les clients. Pour plus d'informations, consultez Présentation des profils de certificat.

**Certificat d'authentification serveur émis par le fournisseur public**

Quand vous utilisez cette méthode, les clients approuvent automatiquement le certificat, et vous n'avez pas besoin de créer vous-même un certificat personnalisé. Configuration Manager crée le service dans Azure avec le domaine cloudapp.net. Un fournisseur de certificat public ne peut pas émettre pour vous un certificat portant ce nom. Pour créer un alias DNS, procédez comme suit :

1. Créez un enregistrement de nom canonique (CNAME) dans le DNS public de votre organisation. Cet enregistrement crée un alias pour la passerelle de gestion cloud avec un nom convivial que vous utilisez dans le certificat public. Par exemple, Contoso nomme sa passerelle de gestion cloud **GraniteFalls**, qui devient **GraniteFalls.CloudApp.Net** dans Azure. Dans l'espace de noms contoso.com du DNS public de Contoso, l'administrateur DNS crée un enregistrement CNAME pour **GraniteFalls.Contoso.com** pour le nom d'hôte réel, **GraniteFalls.CloudApp.net**.
2. Demandez à un fournisseur public un certificat d'authentification serveur en utilisant le nom commun (CN) de l'alias CNAME. Par exemple, Contoso utilise **GraniteFalls.Contoso.com** comme nom commun du certificat.
3. Créez la passerelle de gestion cloud dans la console Configuration Manager avec ce certificat. Dans la page **Paramètres** de l'Assistant Création d'une passerelle de gestion cloud :
    - Quand vous ajoutez le certificat de serveur pour ce service cloud (depuis le **fichier de certificat**), l'Assistant extrait le nom d'hôte du certificat CN comme nom du service.
    - Il ajoute ensuite ce nom d'hôte à **cloudapp.net** ou à **usgovcloudapp.net** pour le cloud Azure US Government, comme nom de domaine complet du service pour créer le service dans Azure.
    - Par exemple, quand Contoso crée la passerelle de gestion cloud, Configuration Manager extrait le nom d'hôte **GraniteFalls** du nom commun du certificat. Azure crée le service proprement dit sous le nom **GraniteFalls.CloudApp.net**.

**Certificat d'authentification serveur émis par l'infrastructure à clé publique d'entreprise**

Créez un certificat SSL personnalisé pour la passerelle de gestion cloud de la même façon que pour un point de distribution cloud. Suivez les instructions pour le déploiement du certificat de service pour les points de distribution cloud, mais procédez différemment pour ce qui suit :

- Lors de la demande du certificat de serveur web personnalisé, fournissez un nom de domaine complet pour le nom commun du certificat. Pour utiliser la passerelle de gestion cloud sur le cloud public Azure, utilisez un nom qui se termine par **cloudapp.net** ou par **usgovcloudapp.net** pour le cloud Azure US Government.

## Certificat de gestion Azure

*Ce certificat est obligatoire pour les déploiements de services classiques. Par contre, il ne l'est pas pour les déploiements Azure Resource Manager.*

Vous fournissez ce certificat dans le portail Azure, lors de la création de la passerelle de gestion cloud dans la console Configuration Manager.

Pour créer la passerelle de gestion cloud dans Azure, le point de connexion du service Configuration Manager doit d'abord s'authentifier auprès de votre abonnement Azure. Lors de l'utilisation d'un déploiement de service classique, il utilise le certificat de gestion Azure pour cette authentification. Un administrateur Azure charge ce certificat sur votre abonnement. Quand vous créez la passerelle de gestion cloud dans la console Configuration Manager, fournissez ce certificat.

Pour plus d'informations et des instructions sur la manière de charger un certificat de gestion, consultez les articles suivants dans la documentation Azure :

- Services cloud et certificats de gestion

- Charger un certificat de gestion de service Azure

> **IMPORTANT**
> Veillez à copier l'ID d'abonnement associé au certificat de gestion. Vous l'utilisez pour la création de la passerelle de gestion cloud dans la console Configuration Manager.

## Certificat d'authentification client

*Ce certificat est obligatoire pour les clients Internet exécutant Windows 7 ou Windows 8.1, et pour les appareils Windows 10 non joints à Azure Active Directory (Azure AD). Il est également obligatoire sur le point de connexion de passerelle de gestion cloud. Il n'est pas nécessaire pour les clients Windows 10 joints à Azure AD.*

Les clients utilisent ce certificat pour s'authentifier auprès de la passerelle de gestion cloud. Les appareils Windows 10 qui sont hybrides ou joints à un domaine cloud ne nécessitent pas ce certificat, car ils utilisent Azure AD pour s'authentifier.

Provisionnez ce certificat en dehors du contexte de Configuration Manager. Par exemple, utilisez les services de certificats Active Directory et la stratégie de groupe pour émettre des certificats d'authentification clients. Pour plus d'informations, consultez Déploiement du certificat client pour les ordinateurs Windows.

**Certificat racine approuvé de client pour la passerelle de gestion cloud**

*Ce certificat est obligatoire lors de l'utilisation de certificats d'authentification clients. Quand tous les clients utilisent Azure AD pour l'authentification, ce certificat n'est pas nécessaire.*

Vous fournissez ce certificat lors de la création de la passerelle de gestion cloud dans la console Configuration Manager.

La passerelle de gestion cloud doit approuver les certificats d'authentification clients. Pour effectuer cette approbation, fournissez la chaîne de certificats racines approuvés. Vous pouvez spécifier deux autorités de certification racines de confiance et quatre autorités de certification (subordonnées) intermédiaires.

#### Exporter la racine de confiance du certificat client

Après avoir émis un certificat d'authentification client pour un ordinateur, utilisez ce processus sur cet ordinateur pour exporter la racine de confiance.

1. Ouvrez le menu Démarrer. Tapez « run » pour ouvrir la fenêtre Exécuter. Ouvrez **mmc**.
2. Dans le menu Fichier, choisissez **Ajouter/supprimer un composant logiciel enfichable**.
3. Dans la boîte de dialogue Ajouter ou supprimer des composants logiciels enfichables, sélectionnez **Certificats**, puis cliquez sur **Ajouter**. a. Dans la boîte de dialogue Composant logiciel enfichable Certificats, sélectionnez **Compte d'ordinateur**, puis cliquez sur **Suivant**. b. Dans la boîte de dialogue Sélectionner un ordinateur, sélectionnez **Ordinateur local**, puis cliquez sur **Terminer**. c. Dans la boîte de dialogue Ajouter ou supprimer des composants logiciels enfichables, cliquez sur **OK**.
4. Développez **Certificats**, développez **Personnel**, puis sélectionnez **Certificats**.
5. Sélectionnez un certificat dont le rôle prévu est **Authentification client**. a. Dans le menu Action, sélectionnez **Ouvrir**. b. Passez à l'onglet **Chemin d'accès de certification**. Sélectionnez le certificat suivant plus haut dans la chaîne, puis cliquez sur **Afficher le certificat**.
6. Dans cette boîte de dialogue Nouveau certificat, passez à l'onglet **Détails**. Cliquez sur **Copier dans un fichier...**.
7. Effectuez l'Assistant Exportation de certificat en utilisant le format de certificat par défaut, **X.509 binaire encodé DER (*.cer)**. Notez le nom et l'emplacement du certificat exporté.

8. Exportez tous les certificats dans le chemin de certification du certificat d'authentification client d'origine. Notez quels certificats exportés sont des autorités de certification intermédiaires, et lesquels sont des autorités de certification racines de confiance.

## Activer le point de gestion pour HTTPS

*Spécifications pour les certificats*

- Dans les versions 1706 ou 1710, lors de la gestion de clients traditionnels avec des identités locales en utilisant un certificat d'authentification client, ce certificat est recommandé mais pas obligatoire.
- Dans la version 1710, lors de la gestion de clients Windows 10 joints à Azure AD, ce certificat est obligatoire pour les points de gestion.
- À compter de la version 1802, ce certificat est obligatoire dans tous les scénarios. Seuls les points de gestion que vous activez pour la passerelle de gestion cloud doivent être HTTPS. Ce changement de comportement offre une meilleure prise en charge de l'authentification basée sur un jeton Azure AD.

Provisionnez ce certificat en dehors du contexte de Configuration Manager. Par exemple, utilisez les services de certificats Active Directory et la stratégie de groupe pour émettre un certificat de serveur web. Pour plus d'informations, consultez Spécifications pour les certificats d'infrastructure à clé publique et Déployer le certificat de serveur web pour les systèmes de site qui exécutent IIS.

## Étapes suivantes

- Configurer la passerelle de gestion cloud
- Questions fréquentes (FAQ) sur la passerelle de gestion cloud
- Sécurité et confidentialité de la passerelle de gestion cloud

# Configurer la passerelle de gestion cloud pour Configuration Manager

22/06/2018 • 22 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Ce processus comprend les étapes nécessaires pour configurer une passerelle de gestion cloud (CMG).

> **TIP**
> Cette fonctionnalité a été introduite dans la version 1610 en tant que fonctionnalité en préversion. À compter de la version 1802, cette fonctionnalité n'est plus en préversion.

## Avant de commencer

Commencez par lire l'article Planifier la passerelle de gestion cloud. Utilisez cet article pour déterminer votre conception de la passerelle de gestion cloud.

Utilisez la liste de vérification suivante pour vous assurer que vous disposez des informations nécessaires et des prérequis pour créer une passerelle de gestion cloud :

- L'environnement Azure à utiliser. Par exemple, le cloud public Azure ou le cloud Azure US Government.
- Vous avez besoin d'un ou de plusieurs certificats pour la passerelle de gestion cloud, en fonction de votre conception. Pour plus d'informations, consultez Certificats pour la passerelle de gestion cloud.
- À compter de la version 1802, choisissez si vous utilisez le **déploiement Azure Resource Manager** ou un **déploiement de service classique**. Pour plus d'informations, consultez Azure Resource Manager. Vous devez respecter les exigences suivantes pour un déploiement Azure Resource Manager de la passerelle de gestion cloud :
  - Intégration à Azure AD pour la **gestion cloud**. Découverte d'utilisateurs Azure AD non requise.
  - Un administrateur des abonnements doit se connecter.
- Vous devez respecter les exigences suivantes pour un déploiement de service classique de la passerelle de gestion cloud :
  - ID d'abonnement Azure
  - Certificat de gestion Azure
- Un nom global unique pour le service. Ce nom provient du certificat d'authentification serveur de la passerelle de gestion cloud.
- La région Azure pour le déploiement de cette passerelle de gestion cloud.
- Nombre d'instances de machine virtuelle dont vous avez besoin pour la mise à l'échelle et la redondance.

## Configurer une passerelle de gestion cloud

Effectuez cette procédure sur le site de niveau supérieur. Ce site est soit un site principal autonome, soit le site d'administration centrale.

1. Dans la console Configuration Manager, accédez à l'espace de travail **Administration**, développez **Services cloud**, puis sélectionnez **Passerelle de gestion cloud**.
2. Cliquez sur **Créer une Passerelle de gestion cloud** dans le ruban.
3. À compter de la version 1802, dans la page Général de l'Assistant, choisissez d'abord la méthode de déploiement CMG : **Déploiement d'Azure Resource Manager** ou **Déploiement de service Classic**.
   a. Pour le **déploiement Azure Resource Manager** : cliquez sur **Se connecter** pour vous authentifier avec un compte d'administrateur d'abonnements Azure. L'Assistant remplit automatiquement les champs restants à partir des informations stockées dans les prérequis de l'intégration d'Azure AD. Si vous possédez plusieurs abonnements, sélectionnez l'**ID de l'abonnement** que vous voulez utiliser.
   b. Pour le **déploiement de service classique** *et les versions 1706 et 1710 de Configuration Manager* : entrez votre **ID d'abonnement** Azure. Cliquez ensuite sur **Parcourir**, puis sélectionnez le fichier .PFX du certificat de gestion Azure.
4. Spécifiez l'**environnement Azure** pour cette passerelle de gestion cloud. Les options disponibles dans la liste déroulante peuvent varier en fonction de la méthode de déploiement.
5. Cliquez sur **Suivant**. Attendez que le site teste la connexion à Azure.
6. Dans la page Paramètres de l'Assistant, cliquez d'abord sur **Parcourir**, puis sélectionnez le fichier .PFX correspondant au certificat d'authentification serveur de la passerelle de gestion cloud. Le nom de ce certificat remplit les champs **Nom de domaine complet du service** et **Nom du service**.

   > **NOTE**
   > À compter de la version 1802, le certificat d'authentification serveur de la passerelle de gestion cloud prend en charge les caractères génériques. Si vous utilisez un certificat générique, remplacez l'astérisque (*) dans le champ **Nom de domaine complet du service** par le nom d'hôte souhaité pour la passerelle de gestion cloud.

7. Cliquez sur la liste déroulante **Région** pour choisir la région Azure pour cette passerelle de gestion cloud.
8. Dans la version 1802 et si vous utilisez un déploiement Azure Resource Manager, sélectionnez une option**Groupe de ressources**.
   a. Si vous choisissez **Utiliser le fichier existant**, sélectionnez un groupe de ressources existant dans la liste déroulante.
   b. Si vous choisissez **Créer**, entrez le nom du nouveau groupe de ressources.
9. Dans le champ **Instance de machine virtuelle**, entrez le nombre de machines virtuelles pour ce service. La valeur par défaut est 1, mais vous pouvez définir jusqu'à 16 machines virtuelles par passerelle de gestion cloud.
10. Cliquez sur **Certificats** pour ajouter des certificats racines approuvés de client. Ajoutez jusqu'à deux autorités de certification racines de confiance et quatre autorités de certification (subordonnées) intermédiaires.
11. Par défaut, l'Assistant active l'option permettant de **Vérifier la révocation des certificats clients**. Une liste de révocation de certificats doit être publiée publiquement pour que cette vérification fonctionne. Si vous ne publiez pas de liste de révocation de certificats, décochez cette option.
12. Cliquez sur **Suivant**.
13. Pour surveiller le trafic de la passerelle de gestion cloud avec un seuil de 14 jours, cochez la case pour activer l'alerte de seuil. Ensuite, spécifiez le seuil et le pourcentage auquel déclencher les différents niveaux d'alerte. Choisissez **Suivant** quand vous avez terminé.

14. Vérifiez les paramètres, puis choisissez **Suivant**. Configuration Manager commence à configurer le service. Une fois l'Assistant fermé, 5 à 15 minutes sont nécessaires pour provisionner complètement le service dans Azure. Vérifiez la colonne **État** de la nouvelle passerelle de gestion cloud pour déterminer quand le service est prêt.

> **NOTE**
> Pour résoudre les problèmes de déploiement de passerelle de gestion cloud, utilisez **CloudMgr.log** et **CMGSetup.log**. Pour plus d'informations, consultez Fichiers journaux.

## Configurer le site principal pour l'authentification de certification client

Si vous utilisez des certificats d'authentification client pour que les clients s'authentifient auprès de la passerelle de gestion cloud, suivez la procédure suivante pour configurer chaque site principal.

1. Dans la console Configuration Manager, accédez à l'espace de travail **Administration**, développez **Configuration du site**, puis sélectionnez **Sites**.
2. Sélectionnez le site principal auquel vos clients Internet sont affectés, puis choisissez **Propriétés**.
3. Passer à l'onglet **Communications des ordinateurs clients** de la feuille de propriétés du site principal, puis cochez la case **Utiliser le certificat client PKI (fonctionnalité d'authentification du client) lorsqu'il est disponible**.
4. Si vous ne publiez pas de liste de révocation de certificats, désactivez l'option **Les clients vérifient la liste de révocation des certificats (CRL) pour les systèmes de site**.

## Ajouter le point de connexion CMG

Le point de connexion CMG est le rôle de système de site permettant de communiquer avec la passerelle de gestion cloud. Pour ajouter le point de connexion CMG, suivez les instructions générales fournies pour installer des rôles de système de site. Dans la page Sélection du rôle système de l'Assistant Ajout des rôles de système de site, sélectionnez **Point de connexion de la passerelle de gestion cloud**. Sélectionnez ensuite le **Nom de la passerelle de gestion cloud** à laquelle ce serveur se connecte. L'Assistant affiche la région pour la passerelle de gestion cloud sélectionnée.

> **IMPORTANT**
> Dans certains cas, le point de connexion CMG doit avoir un certificat d'authentification client.

> **NOTE**
> Pour résoudre les problèmes liés à l'intégrité du service de passerelle de gestion cloud, utilisez **CMGService.log** et **SMS_Cloud_ProxyConnector.log**. Pour plus d'informations, consultez Fichiers journaux.

## Configurer les utilisés par le client pour le trafic de la passerelle de gestion cloud

Configurez les systèmes de site de point de gestion et de point de mise à jour logicielle pour accepter le trafic de la passerelle de gestion cloud. Effectuez cette procédure sur le site principal, pour tous les points de gestion et tous les points de mise à jour logicielle qui gèrent des clients Internet.

1. Dans la console Configuration Manager, accédez à l'espace de travail **Administration**, développez

**Configuration du site**, cliquez avec le bouton droit sur **Serveurs et rôles de système de site**, puis sélectionnez **Point de gestion** dans la liste.

2. Sélectionnez le serveur de système de site que vous souhaitez configurer pour le trafic de la passerelle de gestion cloud. Sélectionnez le rôle **Point de gestion** dans le volet d'informations, puis cliquez sur **Propriétés** dans le ruban.

3. Dans la feuille des propriétés Point de gestion, sous Connexions client, cochez la case située en regard de l'option **Autoriser le trafic de la passerelle de gestion cloud de Configuration Manager**.

   - En fonction de votre conception de la passerelle de gestion cloud et de la version de Configuration Manager, vous devrez peut-être activer l'option **HTTPS**. Pour plus d'informations, consultez Activer le point de gestion pour HTTPS.

4. Cliquez sur **OK**.

Répétez ces étapes pour les points de gestion supplémentaires si nécessaire, et pour tous les points de mise à jour logicielle.

## Configurer des clients pour la passerelle de gestion cloud

Une fois que la passerelle de gestion cloud et les rôles de système de site sont en cours d'exécution, les clients obtiennent automatiquement l'emplacement du service de passerelle de gestion cloud à la prochaine demande d'emplacement. Les clients doivent se trouver sur l'intranet pour recevoir l'emplacement du service de passerelle de gestion cloud, sauf si vous installez et attribuez des clients Windows 10 à l'aide d'Azure AD à des fins d'authentification. Le cycle d'interrogation pour les demandes d'emplacement est de 24 heures. Si vous ne souhaitez pas attendre la demande d'emplacement normalement planifiée, vous pouvez forcer la demande en redémarrant le service hôte de l'agent SMS (ccmexec.exe) sur l'ordinateur.

> **NOTE**
> Par défaut, tous les clients reçoivent une stratégie de passerelle de gestion cloud. Contrôlez ce paramètre à l'aide du paramètre client Autoriser les clients à utiliser une passerelle de gestion cloud.

Le client Configuration Manager détermine automatiquement s'il est sur l'intranet ou sur Internet. Si le client peut contacter un contrôleur de domaine ou un point de gestion local, il définit son type de connexion sur **Intranet actuellement**. Sinon, il passe à **Internet actuellement** et utilise l'emplacement du service de passerelle de gestion cloud pour communiquer avec le site.

> **NOTE**
> Vous pouvez forcer le client à toujours utiliser la passerelle de gestion cloud, qu'il se trouve sur l'intranet ou sur Internet. Cette configuration est utile à des fins de test, ou pour les clients se trouvant dans des bureaux distants et que vous voulez forcer à utiliser la passerelle de gestion cloud. Définissez la clé de Registre suivante sur le client :
>
> `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CCM\Security, ClientAlwaysOnInternet = 1`
>
> Vous pouvez également spécifier ce paramètre pendant l'installation du client à l'aide de la propriété CCMALWAYSINF.

Pour vérifier que les clients disposent de la stratégie spécifiant la passerelle de gestion cloud, ouvrez une invite de commandes Windows PowerShell en tant qu'administrateur sur l'ordinateur client, puis exécutez la commande suivante :

```
Get-WmiObject -Namespace Root\Ccm\LocationServices -Class SMS_ActiveMPCandidate | Where-Object {$_.Type -eq "Internet"}
```

Cette commande affiche tous les points de gestion Internet que le client connaît. Quand la passerelle de gestion cloud n'est pas techniquement un point de gestion Internet, elle s'affiche comme telle aux clients.

> **NOTE**
>
> Pour résoudre les problèmes liés au trafic client de passerelle de gestion cloud, utilisez **CMGHttpHandler.log**, **CMGService.log** et **SMS_Cloud_ProxyConnector.log**. Pour plus d'informations, consultez Fichiers journaux.

## Modifier une passerelle de gestion cloud

Après avoir créé une passerelle de gestion cloud, vous pouvez modifier certains de ses paramètres. Sélectionnez la passerelle de gestion cloud dans la console Configuration Manager, puis cliquez sur **Propriétés**. Les paramètres suivants sont configurables :

- **Général**
  - **Certificat de gestion Azure** : changez le certificat de gestion Azure pour la passerelle de gestion cloud. Cette option est utile lors de la mise à jour du certificat avant son expiration.
- **Paramètres**
  - **Fichier de certificat** : changez le certificat d'authentification serveur pour la passerelle de gestion cloud. Cette option est utile lors de la mise à jour du certificat avant son expiration.
  - **Instance de machine virtuelle** : changez le nombre de machines virtuelles que le service utilise dans Azure. Ce paramètre vous permet de faire monter ou descendre en puissance le service de façon dynamique en fonction de considérations relatives à l'utilisation ou au coût.
  - **Certificats** : ajoutez ou supprimez des certificats d'autorité de certification intermédiaires ou racines de confiance. Cette option est utile lors de l'ajout de nouvelles autorités de certification ou du retrait de certificats expirés.
  - **Vérifier la révocation des certificats clients** : si vous n'avez pas activé ce paramètre initialement lors de la création de la passerelle de gestion cloud, vous pouvez l'activer ultérieurement une fois que vous publiez la liste de révocation de certificats.
- **Alertes** : vous pouvez reconfigurer les alertes à tout moment après avoir créé la passerelle de gestion cloud.

Les changements plus importants, tels que les configurations suivantes, exigent de redéployer le service :

- Méthode de déploiement classique sur Azure Resource Manager
- Abonnement
- Nom du service
- De PKI privée à PKI publique
- Région

Conservez toujours au moins une passerelle de gestion cloud active pour que les clients Internet reçoivent la stratégie mise à jour. Les clients Internet ne peuvent pas communiquer avec une passerelle de gestion cloud supprimée. Les clients n'ont pas connaissance de l'existence d'une nouvelle passerelle tant qu'ils ne se reconnectent pas à l'intranet. Quand vous créez une deuxième instance de passerelle de gestion cloud afin de supprimer la première, créez également un autre point de connexion CMG.

Étant donné que les clients actualisent la stratégie par défaut toutes les 24 heures, attendez au moins un jour après avoir créé une passerelle de gestion cloud pour supprimer l'ancienne. Si les clients sont désactivés ou sans connexion Internet, vous devrez peut-être attendre plus longtemps.

À compter de la version 1802, si vous avez une passerelle de gestion cloud existante sur la méthode de déploiement classique, vous devez déployer une nouvelle passerelle de gestion cloud pour utiliser la méthode de déploiement Azure Resource Manager. Il existe deux options :

- Si vous voulez réutiliser le même nom de service :
  1. Supprimez d'abord la passerelle de gestion cloud classique, en respectant le conseil de toujours avoir au moins une passerelle de gestion cloud active pour les clients Internet.
  2. Créez une passerelle de gestion cloud à l'aide d'un déploiement Resource Manager. Réutilisez le même certificat d'authentification serveur.
  3. Reconfigurez le point de connexion CMG pour utiliser la nouvelle instance de passerelle de gestion cloud.
- Si vous voulez utiliser un nouveau nom de service :
  1. Créez une passerelle de gestion cloud à l'aide d'un déploiement Resource Manager. Utilisez un nouveau certificat d'authentification serveur.
  2. Créez un point de connexion CMG et un lien avec la nouvelle passerelle de gestion cloud.
  3. Attendez au moins un jour que les clients Internet reçoivent la stratégie sur la nouvelle passerelle de gestion cloud.
  4. Supprimez la passerelle de gestion cloud classique.

Modifiez la passerelle de gestion cloud uniquement à partir de la console Configuration Manager. Apporter des modifications au service ou à des machines virtuelles sous-jacentes directement dans Azure n'est pas pris en charge. Tous les changements apportés peuvent être perdus sans préavis. Comme avec n'importe quel service PaaS, le service peut regénérer les machines virtuelles à tout moment. Ces régénérations peuvent se produire pour la maintenance du matériel principal, ou pour appliquer des mises à jour au système d'exploitation des machines virtuelles.

Si vous devez supprimer la passerelle de gestion cloud, effectuez-le également à partir de la console Configuration Manager. La suppression manuelle de tout composant dans Azure entraîne l'incohérence du système. Cet état conserve des informations orphelines, et des comportements inattendus peuvent se produire.

## Étapes suivantes

- Surveiller les clients pour la passerelle de gestion cloud
- Questions fréquentes (FAQ) sur la passerelle de gestion cloud

# Surveiller la passerelle de gestion cloud dans Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Une fois que la passerelle de gestion cloud est en cours d'exécution et que les clients se connectent par son intermédiaire, vous pouvez surveiller les clients et le trafic réseau pour vérifier que le service fonctionne comme vous pensez qu'il fonctionne.

## Surveiller les clients

Les clients connectés via la passerelle de gestion cloud s'affichent dans la console Configuration Manager de la même façon que les clients locaux. Pour plus d'informations, consultez Guide pratique pour surveiller des clients.

## Surveiller le trafic dans la console

Surveillez le trafic sur la passerelle de gestion cloud à l'aide de la console Configuration Manager :

1. Accédez à **Administration > Services cloud > Passerelle de gestion cloud**.
2. Sélectionnez la passerelle de gestion cloud dans le volet Liste.
3. Affichez les informations de trafic dans le volet Détails pour le point de connexion de la passerelle de gestion cloud et les rôles de système de site auxquels il se connecte.

## Configurer des alertes de trafic sortant

Les alertes de trafic sortant vous permettent de savoir quand le trafic réseau est proche d'un niveau de seuil de 14 jours. Quand vous créez la passerelle de gestion cloud, vous pouvez définir des alertes de trafic. Si vous avez ignoré cette partie, vous pouvez toujours configurer les alertes une fois que le service est en cours d'exécution. Réglez les paramètres d'alerte à tout moment.

1. Accédez à **Administration > Services cloud > Passerelle de gestion cloud**.
2. Cliquez avec le bouton droit sur la passerelle de gestion cloud dans le volet Liste, puis choisissez **Propriétés**.
3. Cliquez sur l'onglet **Alertes**. Activez le seuil et les alertes. Spécifiez le seuil de données de 14 jours en gigaoctets (Go). Spécifiez également le seuil en pourcentage auquel déclencher les différents niveaux d'alerte.
4. Cliquez sur **OK** quand vous avez terminé.

## Surveiller les journaux

La passerelle de gestion cloud génère des entrées dans plusieurs fichiers journaux. Pour plus d'informations, consultez Fichiers journaux dans System Center Configuration Manager.

# Planifier la gestion des clients basée sur Internet dans System Center Configuration Manager

22/06/2018 • 21 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

La gestion des clients basée sur Internet (ou IBCM, Internet-Based Client Management) vous permet de gérer les clients System Center Configuration Manager quand ils ne sont pas connectés à votre réseau d'entreprise, mais qu'ils disposent d'une connexion Internet standard. Cette configuration offre plusieurs avantages, notamment la réduction des coûts, car il n'est plus nécessaire d'utiliser des réseaux privés virtuels (VPN) et la possibilité de déployer les mises à jour logicielles au moment opportun.

En raison des exigences de sécurité plus élevées liées à la gestion des ordinateurs clients sur un réseau public, la gestion de clients basés sur Internet nécessite que les clients et les serveurs de système de site auxquels les clients se connectent utilisent des certificats PKI. Cela garantit l'authentification des connexions par une autorité indépendante et le chiffrement des données vers et depuis ces systèmes de site à l'aide du protocole SSL (Secure Sockets Layer).

Utilisez les sections suivantes pour vous aider à planifier la gestion des clients basés sur Internet.

## Fonctionnalités non prises en charge sur Internet

Toutes les fonctionnalités de gestion des clients ne sont pas adaptées à Internet. Par conséquent, elles ne sont pas pris en charge lorsque les clients sont gérés sur Internet. Les fonctionnalités qui ne sont pas prises en charge pour la gestion d'Internet reposent généralement sur les services de domaine Active Directory ou ne conviennent pas à un réseau public, comme par exemple la découverte de réseau et Wake-on-LAN (WOL).

Les fonctions ci-dessous ne sont pas prises en charge lorsque les clients sont gérés sur Internet :

- Le déploiement de client sur Internet, comme par exemple l'installation poussée du client et le déploiement de client basé sur des mises à jour. Utilisez plutôt l'installation manuelle du client.
- Attribution automatique du site.
- Wake-on-LAN.
- Le déploiement de système d'exploitation. Toutefois, vous pouvez déployer des séquences de tâches qui ne déploient pas un système d'exploitation. Par exemple, des séquences de tâches qui exécutent des scripts et des tâches de maintenance sur les clients.
- Le contrôle à distance.
- Le déploiement de logiciels vers des utilisateurs, sauf si le point de gestion basé sur Internet peut authentifier l'utilisateur dans les services de domaine Active Directory à l'aide de l'authentification Windows (Kerberos ou NTLM). Cela est possible lorsque le point de gestion basé sur Internet approuve la forêt dans laquelle réside le compte d'utilisateur.

  En outre, la gestion des clients sur Internet ne prend pas en charge l'itinérance. L'itinérance permet aux clients de toujours trouver les points de distribution les plus proches pour télécharger du contenu. Les clients qui ne sont pas gérés sur Internet communiquent avec des systèmes de site à partir du site qui leur est affecté lorsque ces systèmes de site sont configurés pour utiliser un nom de domaine complet Internet et les rôles de système de site autorisent les connexions client à partir d'Internet. Les clients sélectionnent de manière non déterministique l'un des systèmes de site basés sur Internet, indépendamment de la bande

passante ou de l'emplacement physique.

Lorsque vous disposez d'un point de mise à jour logicielle qui est configuré pour accepter les connexions à partir d'Internet, les clients Configuration Manager basés sur Internet qui se trouvent sur Internet effectuent toujours une analyse par rapport à ce point de mise à jour logicielle afin de déterminer quelles mises à jour logicielles sont requises. Toutefois, lorsque ces clients se trouvent sur Internet, ils commencent par essayer de télécharger les mises à jour logicielles à partir de Microsoft Update, plutôt qu'à partir d'un point de distribution basé sur Internet. Uniquement en cas d'échec, ils tenteront de télécharger les mises à jour logicielles requises à partir d'un point de distribution basé sur Internet. Les clients qui ne sont pas configurés pour la gestion des clients basés sur Internet n'essaient jamais de télécharger les mises à jour logicielles auprès de Microsoft Update, mais utilisent toujours des points de distribution Configuration Manager.

## Éléments à prendre en considération pour les communications client à partir d'Internet ou d'une forêt non approuvée

Les rôles de système de site suivants installés sur les sites principaux prennent en charge les connexions de clients qui se trouvent dans des emplacements non approuvés, tels qu'Internet ou une forêt non approuvée (les sites secondaires ne prennent pas en charge les connexions client à partir d'emplacements non approuvés) :

- Point du site web du catalogue des applications
- Module de stratégie de Configuration Manager
- Point de distribution (HTTPS est requis par les points de distribution cloud)
- Point proxy d'inscription
- Point d'état de secours
- Point de gestion
- Point de mise à jour logicielle

**À propos des systèmes de site accessibles sur Internet :**
Même s'il n'est pas nécessaire de disposer d'une relation de confiance entre la forêt d'un client et celle d'un serveur de système de site, quand la forêt qui contient un système de site accessible sur Internet approuve la forêt qui contient les comptes d'utilisateurs, cette configuration prend en charge les stratégies utilisateur pour les appareils sur Internet quand vous activez le paramètre client **Autoriser les demandes de stratégie utilisateur depuis des clients Internet** de la **Stratégie client**.

Par exemple, les configurations suivantes illustrent la prise en charge par la gestion des clients basés sur Internet des stratégies utilisateur pour les appareils situés sur Internet :

- Le point de gestion basé sur Internet est le réseau de périmètre sur lequel réside un contrôleur de domaine en lecture seule pour authentifier l'utilisateur et un pare-feu qui intervient autorise les paquets Active Directory.
- Le compte d'utilisateur se trouve dans la forêt A (Intranet) et le point de gestion basé sur Internet dans la forêt B (le réseau de périmètre). La forêt B approuve la forêt A et un pare-feu qui intervient autorise les paquets d'authentification.
- Le compte d'utilisateur et le point de gestion basé sur Internet sont dans la forêt A (Intranet). Le point de gestion est publié sur Internet à l'aide d'un serveur proxy web (comme Forefront Threat Management Gateway).

> **NOTE**
> Si l'authentification Kerberos échoue, l'authentification NTLM est ensuite automatiquement utilisée.

Comme l'indique l'exemple précédent, vous pouvez placer des systèmes de site basés sur Internet dans l'Intranet lorsqu'ils sont publiés sur Internet à l'aide d'un serveur proxy Web, tel que ISA Server et Forefront Threat Management Gateway. Ces systèmes de site peuvent être configurés pour la connexion client à partir d'Internet uniquement ou les connexions client à partir d'Internet et Intranet. Lorsque vous utilisez un serveur proxy Web, vous pouvez le configurer pour le pontage SSL (Secure Sockets Layer) vers SSL (plus sécurisé) ou le tunnel SSL :

- **Pontage SSL vers SSL :**
  La configuration recommandée quand vous utilisez des serveurs web proxy pour la gestion de clients sur Internet est le pontage SSL vers SSL, qui utilise une terminaison SSL avec authentification. Les ordinateurs clients doivent être authentifiés à l'aide de l'authentification de l'ordinateur et les clients hérités de l'appareil mobile sont authentifiés à l'aide de l'authentification utilisateur. Les appareils mobiles inscrits par Configuration Manager ne prennent pas en charge le pontage SSL.

  La terminaison SSL au niveau du serveur Web proxy présente l'avantage que les paquets provenant d'Internet sont inspectés avant d'être transférés au réseau interne. Le serveur Web proxy authentifie la connexion du client, l'arrête, puis ouvre une nouvelle connexion authentifiée vers les systèmes de site basés sur Internet. Quand les clients Configuration Manager utilisent un serveur web proxy, leur identité (GUID client) est contenue en toute sécurité dans la charge utile du paquet pour éviter que le point de gestion prenne le serveur web proxy pour le client. Le pontage n'est pas pris en charge dans Configuration Manager de HTTP vers HTTPS ou de HTTPS vers HTTP.

- **Tunneling** :
  Si votre serveur web proxy ne peut pas prendre en charge la configuration requise pour le pontage SSL, ou si vous souhaitez configurer la prise en charge Internet pour les appareils mobiles inscrits par Configuration Manager, le tunneling SSL est aussi pris en charge. Il s'agit d'une option moins sûre car les paquets SSL d'Internet sont transférés aux systèmes de site sans terminaison SSL et ne peuvent donc pas être inspectés à la recherche de contenu malveillant. Lors de l'utilisation du tunnel SSL, aucune configuration n'est requise pour les certificats pour le serveur Web proxy.

## Planification des clients basés sur Internet

Vous devez décider si les ordinateurs clients qui seront gérés sur Internet seront configurés pour la gestion sur l'Intranet et Internet ou pour la gestion des clients sur Internet uniquement. Vous pouvez uniquement configurer l'option de gestion du client pendant l'installation d'un ordinateur client. Si vous changez d'avis ultérieurement, vous devez réinstaller le client.

> **NOTE**
> Si vous configurez un point de gestion compatible Internet, les clients qui s'y connectent deviennent compatibles Internet dès qu'ils actualisent leur liste de points de gestion disponibles.

> **TIP**
> Vous n'avez pas à limiter la configuration de la gestion des clients sur Internet uniquement à Internet et vous pouvez également l'utiliser sur l'Intranet.

Les clients qui sont configurés pour la gestion des clients sur Internet uniquement ne communiquent qu'avec les systèmes de site qui sont configurés pour les connexions client à partir d'Internet. Cette configuration serait

appropriée pour les ordinateurs qui ne se connectent jamais à l'Intranet de votre société, par exemple, des ordinateurs de point de vente dans des emplacements distants. Elle peut aussi convenir quand vous voulez limiter les communications client au protocole HTTPS uniquement (par exemple, pour prendre en charge un pare-feu et des stratégies de sécurité limitées) et quand vous installez des systèmes de site basés sur Internet dans un réseau de périmètre et que vous voulez gérer ces serveurs à l'aide du client Configuration Manager.

Lorsque vous souhaitez gérer des clients du groupe de travail sur Internet, vous devez les installer en tant qu'Internet uniquement.

> **NOTE**
> Les clients d'appareil mobile sont automatiquement configurés en tant qu'Internet uniquement lorsqu'ils sont configurés pour utiliser un point de gestion basé sur Internet.

D'autres ordinateurs clients peuvent être configurés pour une gestion des clients sur Internet et Intranet. Ils peuvent basculer automatiquement entre la gestion des clients basés sur Internet et la gestion des clients Intranet client lorsqu'ils détectent un changement de réseau. Si ces clients peuvent trouver et se connecter à un point de gestion qui est configuré pour les connexions client sur l'intranet, ces clients sont gérés en tant que clients intranet qui possèdent la fonctionnalité de gestion Configuration Manager complète. Si ces clients ne peuvent pas trouver ou se connecter à un point de gestion qui est configuré pour les connexions client sur l'Intranet, ils tentent de se connecter à un point de gestion basé sur Internet, et en cas de succès, ces clients sont ensuite gérés par les systèmes de site basés sur Internet et le site qui leur est affecté.

L'avantage de pouvoir basculer automatiquement entre la gestion des clients basée sur Internet et la gestion des clients intranet est que les ordinateurs clients peuvent utiliser automatiquement toutes les fonctionnalités de Configuration Manager chaque fois qu'ils sont connectés à l'intranet et continuer d'être gérés pour les fonctions de gestion essentielles quand ils sont sur Internet. En outre, un téléchargement commencé sur Internet peut reprendre sans interruption sur le réseau Intranet, et inversement.

## Configuration requise pour la gestion des clients Internet

Dans Configuration, la gestion du client basée sur Internet Manager présente les dépendances externes suivantes :

- Les clients qui seront gérés sur Internet doivent être dotés d'une connexion Internet.

  Configuration Manager utilise les connexions du fournisseur de services Internet (ISP), qu'elles soient permanentes ou temporaires. Les appareils mobiles clients doivent disposer d'une connexion directe à Internet, alors que les ordinateurs clients peuvent se connecter à Internet directement ou par le biais d'un serveur Web proxy.

- Les systèmes de site qui prennent en charge la gestion des clients basés sur Internet doivent être connectés à Internet et se trouver dans un domaine Active Directory.

  Les systèmes de site basés sur Internet n'exigent aucune relation d'approbation avec la forêt Active Directory du serveur de site. Toutefois, lorsque le point de gestion basé sur Internet peut authentifier l'utilisateur à l'aide de l'authentification Windows, les stratégies utilisateur sont prises en charge. En cas d'échec de l'authentification Windows, seules les stratégies d'ordinateur sont prises en charge.

  > **NOTE**
  > Pour prendre en charge des stratégies utilisateur, vous devez également définir sur **Vrai** les deux paramètres client **Stratégie client** :
  >
  > - **Activer l'interrogation de la stratégie utilisateur sur les clients**
  >   - **Autoriser les demandes de stratégie utilisateur depuis des clients Internet**

Un point de site Web du catalogue des applications basé sur Internet nécessite également l'authentification Windows pour authentifier les utilisateurs lorsque leur ordinateur est sur Internet. Cette exigence est indépendante des stratégies utilisateur.

- Vous devez posséder une infrastructure à clé publique (PKI) annexe capable de déployer et gérer les certificats requis par les clients et gérés sur Internet et les serveurs de système de site basés sur Internet.

  Pour plus d'informations sur les certificats PKI, consultez Configuration requise des certificats PKI pour System Center Configuration Manager.

- Le nom de domaine complet (FQDN) Internet des systèmes de site prenant en charge la gestion des clients Internet doit être enregistré sous la forme d'entrées hôtes sur les serveurs DNS publics.

- Les pare-feu ou serveurs proxy qui interviennent doivent autoriser les communications client associées aux systèmes de site basés sur Internet.

  Configuration requise des communications client :

  - Prise en charge du protocole HTTP 1.1
  - Autorisation du type de contenu HTTP de pièces jointes MIME fractionnées (fractionné/mixte et application/flux d'octets)
  - Autorisation des verbes suivants pour le point de gestion Internet :
    - HEAD
    - CCM_POST
    - BITS_POST
    - GET
    - PROPFIND
  - Autorisation des verbes suivants pour le point de distribution Internet :
    - HEAD
    - GET
    - PROPFIND
  - Autorisation des verbes suivants pour le point d'état de secours Internet :
    - POST
  - Autoriser les verbes suivants pour le point du site Web du catalogue des applications basé sur Internet :
    - POST
    - GET
  - Autorisation des en-têtes HTTP suivants pour le point de gestion Internet :
    - Range:
    - CCMClientID:
    - CCMClientIDSignature:
    - CCMClientTimestamp:
    - CCMClientTimestampsSignature:

- Autorisation de l'en-tête HTTP suivant pour le point de distribution Internet :
  - Range:

  Pour obtenir des informations de configuration afin de prendre en charge cette configuration requise, reportez-vous à la documentation de votre serveur proxy ou de votre pare-feu.

  Pour obtenir des configurations de communication similaires lorsque vous utilisez le point de mise à jour logicielle pour les connexions client à partir d'Internet, consultez la documentation de WSUS (Windows Server Update Services). Par exemple, dans le cas de WSUS sous Windows Server 2003, voir Annexe D : paramètres de sécurité, l'annexe de déploiement pour les paramètres de sécurité.

# Présentation des regroupements dans System Center Configuration Manager

22/06/2018 • 7 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les regroupements vous permettent d'organiser les ressources en unités gérables. Vous pouvez créer des regroupements pour répondre à vos besoins de gestion des clients et pour effectuer des opérations sur plusieurs ressources à la fois.

La plupart des tâches de gestion reposent sur ou nécessitent l'utilisation d'un ou plusieurs regroupements. Même si vous pouvez utiliser le regroupement prédéfini Tous les systèmes, son utilisation pour des tâches de gestion n'est pas une bonne pratique. Créez des regroupements personnalisés pour identifier de façon plus spécifique les appareils ou les utilisateurs pour une tâche.

Les regroupements intégrés et personnalisés figurent dans les nœuds **Regroupements d'utilisateurs** et **Regroupements de périphériques** dans l'espace de travail **Ressources et Conformité** de la console Configuration Manager.

Les derniers regroupements visualisés apparaissent dans le nœud **Utilisateurs** et dans le nœud **Appareils** de l'espace de travail **Biens et conformité**.

Voici quelques exemples d'utilisation de regroupements :

| OPÉRATION | EXEMPLE |
|---|---|
| Regroupement des ressources | Vous pouvez créer des regroupements qui rassemblent des ressources en fonction de la hiérarchie de votre organisation.<br><br>Par exemple, vous pouvez créer un regroupement de tous les ordinateurs de l'unité d'organisation Active Directory « Siège social de Londres ». Pour plus d'informations sur la création de ce type de regroupement, consultez Guide pratique pour créer des regroupements dans System Center Configuration Manager.<br><br>Vous pouvez utiliser ce regroupement pour des opérations comme la configuration des paramètres Endpoint Protection, la configuration des paramètres de gestion de l'alimentation des appareils ou l'installation du client Configuration Manager. |
| [Déploiement d'applications] | Vous pouvez créer un regroupement de tous les ordinateurs où Microsoft Office 2013 n'est pas installé, puis le déployer sur tous les ordinateurs de ce regroupement.<br><br>Vous pouvez également utiliser des données de configuration requise pour l'application pour effectuer cette tâche. Pour plus d'informations, consultez Comment créer des applications avec System Center Configuration Manager. |

| OPÉRATION | EXEMPLE |
| --- | --- |
| Gestion des paramètres client | Bien que les paramètres client par défaut dans Configuration Manager s'appliquent à tous les appareils et à tous les utilisateurs, vous pouvez créer des paramètres client personnalisés qui s'appliquent à un regroupement d'appareils ou d'utilisateurs.<br><br>Par exemple, si vous voulez que le contrôle à distance soit disponible sur tous les appareils excepté quelques-uns, configurez les paramètres client par défaut pour autoriser le contrôle à distance, puis configurez les paramètres client personnalisés qui interdisent le contrôle à distance et déployez-les sur le regroupement des clients qui font l'objet de cette exception. |
| Gestion de l'alimentation | Vous pouvez configurer des paramètres d'alimentation spécifiques par regroupement. |
| Administration basée sur des rôles | Utiliser des regroupements pour contrôler quels groupes d'utilisateurs ont accès à différentes fonctionnalités dans la console Configuration Manager. |
| Fenêtres de maintenance | Avec des fenêtres de maintenance, vous pouvez définir une période de temps pendant laquelle différentes opérations Configuration Manager peuvent être effectuées sur les membres d'un regroupement d'appareils. |

# Types de regroupements dans Configuration Manager

Configuration Manager a des regroupements prédéfinis pour les opérations courantes, et vous pouvez aussi créer des regroupements personnalisés.

### Regroupements intégrés

Par défaut, Configuration Manager contient les regroupements suivants qui ne peuvent pas être modifiés.

| NOM DU REGROUPEMENT | DESCRIPTION |
| --- | --- |
| **Tous les groupes d'utilisateurs** | Contient les groupes d'utilisateurs qui sont découverts à l'aide de la découverte de groupes de sécurité Active Directory. |
| **Tous les utilisateurs** | Contient les utilisateurs qui sont découverts à l'aide de la découverte d'utilisateurs Active Directory. |
| **Tous les utilisateurs et groupes d'utilisateurs** | Contient tous les utilisateurs et tous les regroupements de groupes d'utilisateurs. Ce regroupement contient la plus grande étendue de ressources utilisateur et groupe d'utilisateurs. |
| **Tous les clients bureau et serveur** | Contient les appareils serveurs et de bureau qui disposent du client Configuration Manager. L'appartenance est maintenue par découverte par pulsations d'inventaire. |

| NOM DU REGROUPEMENT | DESCRIPTION |
| --- | --- |
| **Tous les appareils mobiles** | Contient les appareils mobiles qui sont gérés par Configuration Manager. L'appartenance est limitée à ces appareils mobiles qui sont affectés à un site avec succès ou découverts par le connecteur Exchange Server. |
| **Tous les systèmes** | Contient les regroupements Tous les clients poste de travail et serveur, Tous les appareils mobiles et Tous les ordinateurs inconnus, ainsi que tous les appareils mobiles qui sont inscrits par Microsoft Intune. Ce regroupement contient la plus grande étendue de ressources d'appareil. |
| **Tous les ordinateurs inconnus** | Contient des enregistrements d'ordinateur générique pour plusieurs plates-formes informatiques. Vous pouvez utiliser ce regroupement pour déployer un système d'exploitation à l'aide d'une séquence de tâches et d'un démarrage PXE, d'un média de démarrage ou d'un média préparé. |

### Regroupements personnalisés

Quand vous créez un regroupement personnalisé dans Configuration Manager, l'appartenance de ce regroupement est déterminée par une ou plusieurs règles de regroupement, comme décrit dans Guide pratique pour créer des regroupements dans System Center Configuration Manager.

# Conditions préalables pour les regroupements dans System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Dans System Center Configuration Manager, les regroupements contiennent uniquement des dépendances à l'intérieur du produit.

## Dépendances de Configuration Manager

| DÉPENDANCE | PLUS D'INFORMATIONS |
|---|---|
| Point de Reporting Services | Le rôle de système de site du point de Reporting Services doit être installé pour pouvoir exécuter des rapports pour les regroupements. Pour plus d'informations, consultez Génération de rapports dans System Center Configuration Manager. |
| Des autorisations de sécurité spécifiques doivent avoir été accordées pour gérer les regroupements | Vous devez disposer des autorisations de sécurité suivantes pour gérer les paramètres de compatibilité :<br><br>- Pour créer et gérer des regroupements : **Créer**, **Supprimer**, **Modifier**, **Modifier un dossier**, **Déplacer un objet**, **Lecture** et **Lire la ressource** pour l'objet **Regroupement**.<br><br>- Pour gérer les paramètres de regroupement : **Modifier les paramètres de regroupement** pour l'objet **Regroupement**.<br><br>L'autorisation **Modifier un dossier** est nécessaire pour tous les dossiers de regroupement, y compris le dossier racine. |

# Pratiques recommandées pour les regroupements dans System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez les bonnes pratiques suivantes pour les regroupements dans System Center Configuration Manager.

## N'utilisez pas de mises à jour incrémentielles pour un grand nombre de regroupements.

Lorsque vous activez l'option **Utiliser des mises à jour incrémentielles pour ce regroupement** , cette configuration peut entraîner des retards d'évaluation si vous l'activez pour de nombreux regroupements. Le seuil s'élève à environ 200 regroupements dans votre hiérarchie. Le nombre exact dépend des facteurs suivants :

- Nombre total de regroupements
- Fréquence d'ajout et de modification de ressources dans la hiérarchie
- Nombre de clients dans la hiérarchie
- Complexité des règles d'appartenance de regroupement dans la hiérarchie

## Assurez-vous que les fenêtres de maintenance sont assez grandes pour déployer des mises à jour logicielles critiques

Vous pouvez configurer des fenêtres de maintenance pour les regroupements d'appareils afin de limiter les périodes où Configuration Manager peut installer des logiciels sur ces appareils. Si vous configurez une fenêtre de maintenance trop petite, le client peut ne pas installer les mises à jour logicielles critiques et se retrouver vulnérable à l'attaque qui aurait été contrée par la mise à jour logicielle.

# Guide pratique pour créer des regroupements dans System Center Configuration Manager

22/06/2018 • 19 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les regroupements sont des groupes d'utilisateurs ou d'appareils. Utilisez les regroupements pour effectuer des tâches comme la gestion d'applications, le déploiement de paramètres de compatibilité ou l'installation de mises à jour logicielles. Vous pouvez également utiliser des regroupements pour gérer des groupes de paramètres client ou les utiliser avec l'administration basée sur les rôles pour définir les ressources auxquelles un utilisateur administratif peut accéder. Configuration Manager contient plusieurs regroupements intégrés. Pour plus d'informations, consultez Présentation des regroupements dans System Center Configuration Manager.

> **NOTE**
> Un regroupement peut contenir des utilisateurs ou des appareils, mais pas les deux.

Le tableau suivant répertorie les règles que vous pouvez utiliser pour configurer les membres d'un regroupement dans Configuration Manager.

| TYPE DE RÈGLE D'APPARTENANCE | PLUS D'INFORMATIONS |
|---|---|
| Règle directe | Utilisez les règles directes pour choisir les utilisateurs ou les ordinateurs à ajouter à un regroupement. Cette appartenance ne change pas, à moins qu'une ressource soit supprimée de Configuration Manager. Configuration Manager doit avoir découvert les ressources ou vous devez les avoir importées pour pouvoir les ajouter à un regroupement à règle directe. Les regroupements avec règle directe ont une surcharge administrative plus élevée que celle des regroupements avec règle de requête, car ils nécessitent des modifications manuelles. |
| Règle de requête | Les règles de requête mettent à jour dynamiquement l'appartenance à un regroupement en fonction d'une requête que Configuration Manager exécute selon une planification. Par exemple, vous pouvez créer un regroupement d'utilisateurs membres de l'unité d'organisation Ressources Humaines dans les services de domaine Active Directory. Ce regroupement est automatiquement mis à jour quand de nouveaux utilisateurs sont ajoutés ou supprimés dans l'unité d'organisation Ressources Humaines.<br><br>Pour examiner des exemples de requêtes que vous pouvez utiliser pour créer des regroupements, consultez Guide pratique pour créer des requêtes dans System Center Configuration Manager. |

| TYPE DE RÈGLE D'APPARTENANCE | PLUS D'INFORMATIONS |
| --- | --- |
| Règle Inclure des regroupements | Cette règle inclut les membres d'un autre regroupement dans un regroupement Configuration Manager. L'appartenance au regroupement actif est mise à jour selon une planification si le regroupement inclus est modifié.<br><br>Vous pouvez ajouter plusieurs règles d'inclusion de regroupement à un regroupement. |
| Règle Exclure des regroupements | La règle Exclure des regroupements permet d'exclure les membres d'un autre regroupement d'un regroupement Configuration Manager. L'appartenance du regroupement actuel est mise à jour selon une planification si le regroupement exclu est modifié.<br><br>Vous pouvez ajouter plusieurs règles d'exclusion de regroupement à un regroupement. Si un regroupement inclut des règles d'inclusion et d'exclusion de regroupement et qu'il existe un conflit, la règle d'exclusion de regroupement est prioritaire.<br>**Exemple :** vous créez un regroupement qui comporte une seule règle d'inclusion de regroupement et une seule règle d'exclusion de regroupement. La règle d'inclusion concerne un regroupement d'ordinateurs de bureau Dell. La règle d'exclusion concerne un regroupement d'ordinateurs qui possèdent moins de 4 Go de RAM. Le nouveau regroupement contient les ordinateurs de bureau Dell qui ont au moins 4 Go de RAM. |

Utilisez les procédures suivantes pour créer des regroupements dans Configuration Manager. Vous pouvez aussi importer des regroupements créés sur ce site ou sur un autre site Configuration Manager. Pour plus d'informations sur l'exportation et l'importation des regroupements, consultez Guide pratique pour gérer des regroupements dans System Center Configuration Manager.

Pour plus d'informations sur la création de regroupements pour des ordinateurs qui exécutent Linux et UNIX, consultez Guide pratique pour gérer les clients pour des serveurs Linux et UNIX dans System Center Configuration Manager.

## Pour créer un regroupement d'appareils

1. Dans la console Configuration Manager, choisissez **Ressources et Conformité** > **Regroupements de périphériques**.
2. Sous l'onglet **Accueil**, dans le groupe **Créer**, choisissez **Créer un regroupement de périphériques**.
3. Dans la page **Général**, fournissez un **Nom** et un **Commentaire**. Ensuite, dans **Limitation au regroupement**, choisissez **Parcourir** pour sélectionner un regroupement de limitation. Le regroupement contiendra uniquement les membres du regroupement de limitation.
4. Dans la page **Règles d'adhésion** de l'**Assistant Création d'un regroupement de périphériques**, dans la liste **Ajouter une règle**, sélectionnez le type de règle d'adhésion que vous voulez utiliser pour le regroupement. Vous pouvez configurer plusieurs règles pour chaque regroupement.

#### Pour configurer une règle directe

1. Sur la page **Rechercher des ressources** de l' **Assistant Création d'une règle d'adhésion directe**, spécifiez les informations suivantes :

- **Classe de ressource** : Sélectionnez le type de ressource à rechercher et ajouter au regroupement. Sélectionnez dans les valeurs **Ressource Système** pour rechercher des données d'inventaire renvoyées

par les ordinateurs clients ou **Ordinateur inconnu** pour sélectionner dans les valeurs renvoyées par les ordinateurs inconnus.

- **Nom d'attribut** : Sélectionnez l'attribut associé à la classe de ressource sélectionnée que vous voulez rechercher. Par exemple, si vous souhaitez sélectionner des ordinateurs par leur nom NetBIOS, sélectionnez **Ressource Système** dans la liste **Classe de ressource** et **NetBIOS nom** dans la liste **Nom d'attribut** .
- **Exclure les ressources signalées comme obsolètes** : si un ordinateur client est signalé comme obsolète, n'incluez pas cette valeur dans les résultats de recherche.
- **Exclure les ressources sur lesquelles le client Configuration Manager n'est pas installé** : Elles ne seront pas affichées dans les résultats de recherche.
- **Valeur :** entrez une valeur pour laquelle vous voulez rechercher le nom d'attribut sélectionné. Vous pouvez utiliser le caractère de pourcentage ( **%** ) comme caractère générique. Par exemple, pour rechercher les ordinateurs dont le nom NetBIOS commence par « M », entrez **M%** dans ce champ.

1. Dans la page **Sélectionner les ressources**, sélectionnez les ressources à ajouter au regroupement dans la liste **Ressources**, puis choisissez **Suivant**.

#### Pour configurer une règle de requête

1. Dans la boîte de dialogue **Propriétés de la règle de requête** , définissez les options suivantes :

- **Nom** : Spécifiez un nom unique.
- **Importer l'instruction de requête** : Ouvre la boîte de dialogue **Parcourir la requête** dans laquelle vous pouvez sélectionner une requête Configuration Manager à utiliser comme règle de requête pour le regroupement.
- **Classe de ressource :** Sélectionnez le type de ressource à rechercher et ajouter au regroupement. Sélectionnez dans les valeurs **Ressource système** pour rechercher des données d'inventaire renvoyées par les ordinateurs clients ou **Ordinateur inconnu** pour sélectionner dans les valeurs renvoyées par les ordinateurs inconnus.
- **Modifier l'instruction de requête** : ouvre la boîte de dialogue **Propriétés de l'instruction de requête** dans laquelle vous pouvez créer une requête à utiliser comme règle pour le regroupement. Pour plus d'informations sur les requêtes, consultez Informations techniques de référence sur les requêtes pour System Center Configuration Manager.

#### Pour configurer une règle d'inclusion de regroupements

Dans la boîte de dialogue **Sélectionner des regroupements**, sélectionnez les regroupements à inclure dans le nouveau regroupement, puis choisissez **OK**.

#### Pour configurer une règle d'exclusion de regroupements

Dans la boîte de dialogue **Sélectionner des regroupements**, sélectionnez les regroupements à inclure dans le nouveau regroupement, puis choisissez **OK**.

- **Utiliser des mises à jour incrémentielles pour ce regroupement** : Sélectionnez cette option pour rechercher et mettre à jour régulièrement uniquement les ressources nouvelles ou modifiées dans l'évaluation de regroupement précédente, indépendamment d'une évaluation de regroupement complète. Les mises à jour incrémentielles ont lieu toutes les 10 minutes.

**IMPORTANT**

Les regroupements configurés à l'aide de règles de requête qui utilisent les classes suivantes ne prennent pas en charge les mises à jour incrémentielles :

- SMS_G_System_CollectedFile
- SMS_G_System_LastSoftwareScan
- SMS_G_System_AppClientState
- SMS_G_System_DCMDeploymentState
- SMS_G_System_DCMDeploymentErrorAssetDetails
- SMS_G_System_DCMDeploymentCompliantAssetDetails
- SMS_G_System_DCMDeploymentNonCompliantAssetDetails
- SMS_G_User_DCMDeploymentCompliantAssetDetails (pour les regroupements d'utilisateurs uniquement)
- SMS_G_User_DCMDeploymentNonCompliantAssetDetails (pour les regroupements d'utilisateurs uniquement)
- SMS_G_System_SoftwareUsageData
- SMS_G_System_CI_ComplianceState
- SMS_G_System_EndpointProtectionStatus
- SMS_GH_System_*
- SMS_GEH_System_*

- **Planifier une mise à jour complète sur ce regroupement** : Planifiez une évaluation complète régulière de l'appartenance au regroupement.

1. Terminez l'Assistant pour créer le regroupement. Le nouveau regroupement figure dans le nœud **Regroupements de périphériques** de l'espace de travail **Ressources et conformité**.

**NOTE**

Vous devez actualiser ou recharger la console Configuration Manager pour voir les membres du regroupement. Toutefois, les membres n'apparaissent pas dans le regroupement tant que la première mise à jour planifiée n'est pas effectuée ou que vous ne sélectionnez pas manuellement **Mettre à jour l'appartenance** pour le regroupement. La mise à jour d'un regroupement peut prendre quelques minutes.

## Pour créer un regroupement d'utilisateurs

1. Dans la console Configuration Manager, choisissez **Ressources et Conformité** > **Regroupements d'utilisateurs**.
2. Sous l'onglet **Accueil**, dans le groupe **Créer**, choisissez **Créer un regroupement d'utilisateurs**.
3. Dans la page **Général** de l'Assistant, fournissez un **Nom** et un **Commentaire**. Ensuite, dans **Limitation au regroupement**, choisissez **Parcourir** pour sélectionner un regroupement de limitation. Le regroupement contiendra uniquement les membres du regroupement de limitation.
4. Dans la page **Règles d'adhésion**, spécifiez ce qui suit :
   - dans la liste **Ajouter une règle** , sélectionnez le type de règle d'adhésion à utiliser pour le regroupement. Vous pouvez configurer plusieurs règles pour chaque regroupement.

#### Pour configurer une règle directe

1. Dans la page **Rechercher des ressources** de l'**Assistant Création d'une règle d'adhésion directe**, spécifiez les informations suivantes :

- **Classe de ressource** : Sélectionnez le type de ressource à rechercher et ajouter au regroupement. Sélectionnez des valeurs **Ressource utilisateur** pour rechercher les informations utilisateur collectées

par Configuration Manager ou **Ressource groupe d'utilisateurs** pour rechercher les informations sur les groupes d'utilisateurs collectées par Configuration Manager.

- **Nom d'attribut** : Sélectionnez l'attribut associé à la classe de ressource que vous voulez rechercher. Par exemple, si vous voulez sélectionner des utilisateurs par leur nom d'unité d'organisation (UO), sélectionnez **Ressource utilisateur** dans la liste **Classe de ressource** et **Nom de l'unité d'organisation utilisateur** dans la liste **Nom d'attribut** .

- **Valeur :** Entrez une valeur à rechercher. Vous pouvez utiliser le caractère de pourcentage ( **%** ) comme caractère générique. Par exemple, pour rechercher des utilisateurs dans l'unité d'organisation Contoso, entrez **Contoso** dans ce champ.

1. Dans la page **Sélectionner les ressources**, sélectionnez les ressources à ajouter au regroupement dans la liste **Ressources**.

#### Pour configurer une règle de requête

1. Dans la boîte de dialogue **Propriétés de la règle de requête**, fournissez les informations suivantes :

- **Nom** : Un nom unique.

- **Importer l'instruction de requête** : Ouvre la boîte de dialogue **Parcourir la requête** dans laquelle vous pouvez sélectionner une requête Configuration Manager à utiliser comme règle de requête pour le regroupement.

- **Classe de ressource** : Sélectionnez le type de ressource à rechercher et ajouter au regroupement. Sélectionnez des valeurs **Ressource utilisateur** pour rechercher les informations utilisateur collectées par Configuration Manager ou **Ressource groupe d'utilisateurs** pour rechercher les informations sur les groupes d'utilisateurs collectées par Configuration Manager.

- **Modifier l'instruction de requête** : Ouvre la boîte de dialogue **Propriétés de l'instruction de requête** dans laquelle vous pouvez créer une requête à utiliser comme règle pour le regroupement.

#### Pour configurer une règle d'inclusion de regroupements

Dans la boîte de dialogue **Sélectionner des regroupements**, sélectionnez les regroupements à inclure dans le nouveau regroupement, puis choisissez **OK**.

#### Pour configurer une règle d'exclusion de regroupements

Dans la boîte de dialogue **Sélectionner des regroupements**, sélectionnez les regroupements à inclure dans le nouveau regroupement, puis choisissez **OK**.

- **Utiliser des mises à jour incrémentielles pour ce regroupement** : Sélectionnez cette option pour rechercher et mettre à jour régulièrement uniquement les ressources nouvelles ou modifiées dans l'évaluation de regroupement précédente, indépendamment d'une évaluation de regroupement complète. Les mises à jour incrémentielles ont lieu toutes les 10 minutes.

**IMPORTANT**

Les regroupements configurés à l'aide de règles de requête qui utilisent les classes suivantes ne prennent pas en charge les mises à jour incrémentielles :

- SMS_G_System_CollectedFile
- SMS_G_System_LastSoftwareScan
- SMS_G_System_AppClientState
- SMS_G_System_DCMDeploymentState
- SMS_G_System_DCMDeploymentErrorAssetDetails
- SMS_G_System_DCMDeploymentCompliantAssetDetails
- SMS_G_System_DCMDeploymentNonCompliantAssetDetails
- SMS_G_User_DCMDeploymentCompliantAssetDetails (pour les regroupements d'utilisateurs uniquement)
- SMS_G_User_DCMDeploymentNonCompliantAssetDetails (pour les regroupements d'utilisateurs uniquement)
- SMS_G_System_SoftwareUsageData
- SMS_G_System_CI_ComplianceState
- SMS_G_System_EndpointProtectionStatus
- SMS_GH_System_*
- SMS_GEH_System_*

- **Planifier une mise à jour complète sur ce regroupement** : Planifiez une évaluation complète régulière de l'appartenance au regroupement.

1. Effectuez toutes les étapes de l'Assistant. Le nouveau regroupement figure dans le nœud **Regroupements d'utilisateurs** de l'espace de travail **Ressources et conformité**.

**NOTE**

Vous devez actualiser ou recharger la console Configuration Manager pour voir les membres du regroupement. Toutefois, les membres n'apparaissent pas dans le regroupement tant que la première mise à jour planifiée n'est pas effectuée ou que vous ne sélectionnez pas manuellement **Mettre à jour l'adhésion** pour le regroupement. La mise à jour d'un regroupement peut prendre quelques minutes.

## Pour importer un regroupement

1. Dans la console Configuration Manager, choisissez **Ressources et Conformité** > **Regroupements d'utilisateurs** ou **Regroupements d'appareils**.
2. Sous l'onglet **Accueil**, dans le groupe **Créer**, choisissez **Importer des regroupements**.
3. Dans la page **Général** de l'**Assistant Importation de regroupements**, choisissez **Suivant**.
4. Dans la page **Nom du fichier MOF**, cliquez sur **Parcourir**, puis accédez au fichier MOF qui contient les informations de regroupement à importer.

   **NOTE**

   Le fichier à importer doit avoir été exporté à partir d'un site exécutant la même version de Configuration Manager que celui-ci. Pour plus d'informations sur l'exportation de regroupements, consultez Guide pratique pour gérer des regroupements dans System Center Configuration Manager.

5. Terminez l'Assistant pour importer le regroupement. Le nouveau regroupement figure dans le nœud **Regroupements d'utilisateurs** ou **Regroupements de périphériques** de l'espace de travail

**Ressources et Conformité** . Actualisez ou rechargez la console Configuration Manager pour afficher les membres du regroupement récemment importé.

# Guide pratique pour gérer des regroupements dans System Center Configuration Manager

22/06/2018 • 17 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Aidez-vous des informations générales de cette rubrique pour effectuer les tâches de gestion des regroupements dans System Center Configuration Manager.

> **NOTE**
> Pour plus d'informations sur la création de regroupements dans Configuration Manager, consultez Guide pratique pour créer des regroupements dans System Center Configuration Manager.

## Comment gérer des regroupements de périphériques

Dans l'espace de travail **Biens et conformité** , sélectionnez **Regroupements de périphériques**, puis le regroupement à gérer, et enfin sélectionnez une tâche de gestion.

Utilisez le tableau suivant pour obtenir plus d'informations sur les tâches de gestion qui pourraient nécessiter certaines informations avant de les sélectionner.

| TÂCHE DE GESTION | DÉTAILS | PLUS D'INFORMATIONS |
|---|---|---|
| **Afficher les membres** | Affiche toutes les ressources qui sont membres du regroupement sélectionné dans un nœud temporaire sous le nœud **Périphériques** . | Aucune information supplémentaire. |

| TÂCHE DE GESTION | DÉTAILS | PLUS D'INFORMATIONS |
| --- | --- | --- |
| **Ajouter les éléments sélectionnés** | Fournit les options suivantes pour exécuter l'une des actions suivantes :<br><br>- **Ajouter des éléments sélectionnés à un regroupement d'appareils existant** : ouvre la boîte de dialogue **Sélectionner un regroupement**, où vous pouvez sélectionner le regroupement auquel vous souhaitez ajouter les membres du regroupement sélectionné. Le regroupement sélectionné est inclus dans ce regroupement grâce à la règle d'adhésion **Inclure des regroupements** .<br><br>- **Ajouter des éléments sélectionnés au nouveau regroupement d'appareils** : ouvre l'**Assistant Création d'un regroupement de périphériques** à partir duquel vous pouvez créer un nouveau regroupement. Le regroupement sélectionné est inclus dans ce regroupement grâce à la règle d'adhésion **Inclure des regroupements** . | Guide pratique pour créer des regroupements dans System Center Configuration Manager |
| **Installer le client** | Ouvre l'**Assistant Installation du client** qui utilise la méthode d'installation push du client pour installer un client Configuration Manager sur tous les ordinateurs du regroupement sélectionné. | Guide pratique pour déployer des clients sur des ordinateurs Windows |
| **Gérer les demandes d'affinité** | Ouvre la boîte de dialogue **Gérer les demandes d'affinité entre périphérique et utilisateur** où vous pouvez approuver ou rejeter les demandes en attente pour établir des affinités des périphériques d'utilisateur pour les périphériques du regroupement sélectionné. | Lier des utilisateurs et des appareils avec l'affinité entre utilisateur et appareil dans System Center Configuration Manager |
| **Effacer les déploiements PXE requis** | Efface tous les déploiements de démarrage PXE requis à partir de tous les membres du regroupement sélectionné. | Introduction au déploiement de systèmes d'exploitation |

| TÂCHE DE GESTION | DÉTAILS | PLUS D'INFORMATIONS |
| --- | --- | --- |
| **Mettre à jour l'adhésion** | Évalue l'adhésion pour le regroupement sélectionné. Pour les regroupements comportant de nombreux membres, l'exécution de cette mise à jour peut durer un certain temps. Utilisez l'action **Actualiser** pour mettre à jour l'affichage avec les nouveaux membres des regroupements une fois la mise à jour terminée. | Aucune information supplémentaire. |
| **Ajouter des ressources** | Ouvre la boîte de dialogue **Ajouter des ressources au regroupement** dans laquelle vous pouvez rechercher de nouvelles ressources à ajouter au regroupement sélectionné.<br><br>L'icône du regroupement sélectionné affiche un symbole de sablier pendant l'exécution de la mise à jour. | Aucune information supplémentaire. |
| **Notification du client** | Ordonne à tous les clients figurant dans le regroupement de périphériques sélectionné de télécharger la stratégie d'ordinateur ou utilisateur. | Aucune information supplémentaire. |
| **Endpoint Protection** | Effectue une analyse rapide ou complète des logiciels anti-programme malveillant ou télécharge les dernières définitions de logiciels anti-programme malveillant sur les ordinateurs du regroupement sélectionné. | Endpoint Protection dans System Center Configuration Manager |
| **Exporter** | Ouvre l'**Assistant Exportation de regroupements** qui vous aide à exporter ce regroupement dans un fichier MOF (Managed Object Format) qui peut ensuite être archivé ou utilisé sur un autre site Configuration Manager.<br><br>Lorsque vous exportez un regroupement, les regroupements qui sont référencés par le regroupement sélectionné à l'aide d'une règle **Inclure** ou **Exclure** ne sont pas exportés. | Aucune information supplémentaire. |
| **Copier** | Crée une copie du regroupement sélectionné. Le nouveau regroupement utilise le regroupement sélectionné comme limitation au regroupement. | Aucune information supplémentaire. |

| TÂCHE DE GESTION | DÉTAILS | PLUS D'INFORMATIONS |
| --- | --- | --- |
| **Supprimer** | Supprime le regroupement sélectionné. Vous pouvez également supprimer toutes les ressources du regroupement à partir de la base de données du site.<br><br>Vous ne pouvez pas supprimer les regroupements qui sont intégrés à Configuration Manager. | Pour obtenir la liste des regroupements intégrés, consultez Présentation des regroupements dans System Center Configuration Manager. |
| **Simuler un déploiement** | Ouvre l' **Assistant Simuler un déploiement d'application** , qui vous permet de tester les résultats du déploiement d'une application sans installer ou désinstaller l'application. | Comment simuler des déploiements d'applications avec System Center Configuration Manager |
| **Déployer** | Affiche les options suivantes :<br><br>- **Application** : ouvre l'**Assistant Déploiement logiciel**, où vous pouvez sélectionner et configurer le déploiement d'une application vers le regroupement sélectionné.<br><br>- **Programme** : ouvre l' **Assistant Déploiement logiciel** , où vous pouvez sélectionner et configurer le déploiement d'un package et d'un programme vers le regroupement sélectionné.<br><br>- **Ligne de base de configuration** : ouvre la boîte de dialogue **Déployer des lignes de base de configuration**, dans laquelle vous pouvez configurer le déploiement d'une ou de plusieurs bases de référence de configuration vers le regroupement sélectionné.<br><br>- **Séquence de tâches** : ouvre l' **Assistant Déploiement logiciel** , où vous pouvez sélectionner et configurer le déploiement d'une séquence de tâches vers le regroupement sélectionné.<br><br>- **Mises à jour logicielles** : ouvre l'**Assistant Déploiement des mises à jour logicielles** où vous pouvez configurer le déploiement de mises à jour logicielles vers les ressources du regroupement sélectionné. | Déployer des applications avec System Center Configuration Manager<br><br>Packages et programmes dans System Center Configuration Manager<br><br>Comment déployer des bases de référence de configuration dans System Center Configuration Manager<br><br>Gérer les séquences de tâches pour automatiser des tâches dans System Center Configuration Manager<br><br>Gérer les mises à jour logicielles dans System Center Configuration Manager |

## Comment gérer des regroupements d'utilisateurs

Dans l'espace de travail **Biens et conformité** , sélectionnez **Regroupements d'utilisateurs**, puis le

regroupement à gérer, et enfin sélectionnez une tâche de gestion.

Utilisez le tableau suivant pour obtenir plus d'informations sur les tâches de gestion qui pourraient nécessiter certaines informations avant de les sélectionner.

| TÂCHE DE GESTION | DÉTAILS | PLUS D'INFORMATIONS |
|---|---|---|
| **Afficher les membres** | Affiche toutes les ressources qui sont membres du regroupement sélectionné dans un nœud temporaire sous le nœud **Utilisateurs** . | Aucune information supplémentaire. |
| **Ajouter les éléments sélectionnés** | Cette option vous permet d'exécuter l'une des actions suivantes :<br><br>- **Ajouter des éléments sélectionnés à un regroupement d'utilisateurs existant** : ouvre la boîte de dialogue **Sélectionner un regroupement**, où vous pouvez sélectionner le regroupement auquel vous souhaitez ajouter les membres du regroupement sélectionné. Le regroupement sélectionné est inclus dans ce regroupement grâce à la règle d'adhésion **Inclure des regroupements** .<br><br>- **Ajouter des éléments sélectionnés au nouveau regroupement d'utilisateurs** : ouvre l'**Assistant Création d'un regroupement d'utilisateurs** à partir duquel vous pouvez créer un nouveau regroupement. Le regroupement sélectionné est inclus dans ce regroupement grâce à la règle d'adhésion **Inclure des regroupements** . | Guide pratique pour créer des regroupements dans System Center Configuration Manager |
| **Gérer les demandes d'affinité** | Ouvre la boîte de dialogue **Gérer les demandes d'affinité entre périphérique et utilisateur** où vous pouvez approuver ou rejeter les demandes en attente pour établir des affinités des périphériques d'utilisateur pour les utilisateurs du regroupement sélectionné. | Lier des utilisateurs et des appareils avec l'affinité entre utilisateur et appareil dans System Center Configuration Manager |

| TÂCHE DE GESTION | DÉTAILS | PLUS D'INFORMATIONS |
| --- | --- | --- |
| **Mettre à jour l'adhésion** | Évalue l'adhésion pour le regroupement sélectionné. Pour les regroupements comportant de nombreux membres, l'exécution de cette mise à jour peut durer un certain temps. Utilisez l'action **Actualiser** pour mettre à jour l'affichage avec les nouveaux membres des regroupements une fois la mise à jour terminée.<br><br>L'icône du regroupement sélectionné affiche un symbole de sablier pendant l'exécution de la mise à jour. | Aucune information supplémentaire. |
| **Ajouter des ressources** | Ouvre la boîte de dialogue **Ajouter des ressources au regroupement** dans laquelle vous pouvez rechercher de nouvelles ressources à ajouter au regroupement sélectionné. | Aucune information supplémentaire. |
| **Exporterer** | Ouvre l'**Assistant Exportation de regroupements** qui vous aide à exporter ce regroupement dans un fichier MOF (Managed Object Format) qui peut ensuite être archivé ou utilisé sur un autre site Configuration Manager.<br><br>Lorsque vous exportez un regroupement, les regroupements qui sont référencés par le regroupement sélectionné à l'aide d'une règle **Inclure** ou **Exclure** ne sont pas exportés. | Aucune information supplémentaire. |
| **Copier** | Crée une copie du regroupement sélectionné. Le nouveau regroupement utilise le regroupement sélectionné comme limitation au regroupement. | Aucune information supplémentaire. |
| **Supprimer** | Supprime le regroupement sélectionné. Vous pouvez également supprimer toutes les ressources du regroupement à partir de la base de données du site.<br><br>Vous ne pouvez pas supprimer les regroupements qui sont intégrés à Configuration Manager. | Pour obtenir la liste des regroupements intégrés, consultez Présentation des regroupements dans System Center Configuration Manager. |
| **Simuler un déploiement** | Ouvre l' **Assistant Simuler un déploiement d'application** , qui vous permet de tester les résultats du déploiement d'une application sans installer ou désinstaller l'application. | Comment simuler des déploiements d'applications avec System Center Configuration Manager |

| TÂCHE DE GESTION | DÉTAILS | PLUS D'INFORMATIONS |
| --- | --- | --- |
| **Déployer** | Affiche les options suivantes :<br><br>- **Application** : ouvre l'**Assistant Déploiement logiciel**, où vous pouvez sélectionner et configurer le déploiement d'une application vers le regroupement sélectionné.<br><br>- **Programme** : ouvre l' **Assistant Déploiement logiciel** , où vous pouvez sélectionner et configurer le déploiement d'un package et d'un programme vers le regroupement sélectionné.<br><br>- **Ligne de base de configuration** : ouvre la boîte de dialogue **Déployer des lignes de base de configuration**, dans laquelle vous pouvez configurer le déploiement d'une ou de plusieurs bases de référence de configuration vers le regroupement sélectionné. | Déployer des applications avec System Center Configuration Manager<br><br>Packages et programmes dans System Center Configuration Manager<br><br>Comment déployer des bases de référence de configuration dans System Center Configuration Manager |

## Propriétés d'un regroupement

Lorsque vous ouvrez la boîte de dialogue **Propriétés** pour un regroupement, vous pouvez afficher et configurer les propriétés suivantes pour un regroupement

| NOM DE L'ONGLET | PLUS D'INFORMATIONS |
| --- | --- |
| **Général** | Permet d'afficher et de configurer des informations générales sur le regroupement sélectionné, y compris le nom du regroupement et la limitation au regroupement. |
| **Règles d'adhésion** | Permet de configurer les règles d'adhésion qui définissent l'adhésion de ce regroupement. Pour plus d'informations, consultez Guide pratique pour créer des regroupements dans System Center Configuration Manager. |
| **Gestion de l'alimentation** | Permet de configurer les modes de gestion de l'alimentation qui sont attribués aux ordinateurs du regroupement sélectionné. Pour plus d'informations, consultez Présentation de la gestion de l'alimentation. |
| **Déploiements** | Affiche tout logiciel qui a été déployé vers les membres du regroupement sélectionné. |
| **Fenêtres de maintenance** | Permet d'afficher et de configurer les fenêtres de maintenance qui sont appliquées aux membres du regroupement sélectionné. Pour plus d'informations, consultez Guide pratique pour utiliser les fenêtres de maintenance dans System Center Configuration Manager. |

| NOM DE L'ONGLET | PLUS D'INFORMATIONS |
| --- | --- |
| **Variables du regroupement** | Permet de configurer les variables qui s'appliquent à ce regroupement et peuvent être utilisées par les séquences de tâches. Pour plus d'informations, consultez Variables intégrées de séquence de tâches. |
| **Groupes de points de distribution** | Permet d'associer un ou plusieurs groupes de points de distribution aux membres du regroupement sélectionné. Pour plus d'informations, consultez Gérer le contenu et l'infrastructure de contenu pour System Center Configuration Manager. |
| **Sécurité** | Affiche les utilisateurs administratifs qui disposent d'autorisations pour le regroupement sélectionné à partir de rôles associés et d'étendues de sécurité. |
| **Analyse** | Permet de configurer le moment où des alertes sont générées pour l'état du client et Endpoint Protection. Pour plus d'informations, consultez Guide pratique pour configurer l'état du client dans System Center Configuration Manageret Guide pratique pour surveiller Endpoint Protection dans System Center Configuration Manager. |

# Comment utiliser les fenêtres de maintenance dans System Center Configuration Manager

22/06/2018 • 4 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les fenêtres de maintenance vous permettent de définir une période de temps pendant laquelle des opérations Configuration Manager peuvent être effectuées sur un regroupement d'appareils. Vous pouvez utiliser les fenêtres de maintenance afin de vous assurer que les modifications apportées à la configuration client seront effectuées pendant des périodes qui n'affectent pas la productivité.

Les opérations suivantes prennent en charge les fenêtres de maintenance :

- Déploiements de logiciels
- Déploiements de mises à jour logicielles
- Déploiement et évaluation des paramètres de compatibilité
- Déploiements de système d'exploitation
- Déploiements de séquences de tâches

  Configurez des fenêtres de maintenance avec une date de début, une heure de début et de fin, ainsi qu'une périodicité. La durée maximale d'une fenêtre doit être inférieure à 24 heures. Par défaut, les redémarrages de l'ordinateur dus à un déploiement ne sont pas autorisés à l'extérieur d'une fenêtre de maintenance, mais vous pouvez remplacer la valeur par défaut. Les fenêtres de maintenance affectent uniquement l'heure d'exécution du programme de déploiement ; les applications configurées pour un téléchargement et une exécution en local peuvent télécharger du contenu en dehors de la fenêtre.

  Quand un ordinateur client est membre d'un regroupement d'appareils avec une fenêtre de maintenance, un programme de déploiement est exécuté uniquement si la durée d'exécution maximale autorisée ne dépasse pas la durée configurée pour la fenêtre. Si le programme ne peut pas être exécuté, une alerte est générée et le déploiement est de nouveau exécuté lors de la fenêtre de maintenance planifiée suivante qui dispose de suffisamment de temps.

## Utilisation de fenêtres de maintenance multiples

Quand un ordinateur client est membre de plusieurs regroupements d'appareils avec des fenêtres de maintenance, les règles suivantes s'appliquent :

- Si les fenêtres de maintenance ne se chevauchent pas, elles sont traitées comme deux fenêtres de maintenance indépendantes.
- Si les fenêtres de maintenance se chevauchent, elles sont traitées comme une seule fenêtre de maintenance englobant la période couverte par les deux fenêtres de maintenance. Par exemple, si deux fenêtres d'une heure chacune se chevauchent de 30 minutes, la durée effective de la fenêtre de maintenance est de 90 minutes.

  Quand un utilisateur lance l'installation d'une application à partir du Centre logiciel, l'application est installée immédiatement, indépendamment de toute fenêtre de maintenance.

  Si le déploiement d'une application avec un objectif **Obligatoire** atteint son échéance d'installation pendant les heures creuses configurées par un utilisateur dans le Centre logiciel, l'application est installée.

**Comment configurer les fenêtres de maintenance**

1. Dans la console Configuration Manager, choisissez **Ressources et Conformité** > **Regroupements de périphériques**.
2. Dans la liste **Regroupements d'appareils**, sélectionnez un regroupement. Vous ne pouvez pas créer de fenêtres de maintenance pour le regroupement **Tous les systèmes** .
3. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
4. Dans l'onglet **Fenêtres de maintenance** de la boîte de dialogue **Propriétés de <nom_regroupement>**, choisissez l'icône **Nouveau**.
5. Renseignez la boîte de dialogue **<nouveau> Calendrier**.
6. Effectuez une sélection à partir de la liste déroulante **Appliquer cette planification à**.
7. Choisissez **OK**, puis fermez la boîte de dialogue **Propriétés de <nom_regroupement>**.

# Classer automatiquement des appareils dans des regroupements avec System Center Configuration Manager

22/06/2018 • 3 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez créer des catégories d'appareils pour classer automatiquement les appareils dans des regroupements d'appareils quand vous utilisez Configuration Manager avec Microsoft Intune. Les utilisateurs doivent ensuite choisir une catégorie d'appareils quand ils inscrivent un appareil dans Intune. Vous pouvez changer une catégorie d'appareils dans la console Configuration Manager.

> **IMPORTANT**
> Cette fonctionnalité est opérationnelle avec la version de Microsoft Intune de **juin 2016** et ultérieure. Vérifiez que vous avez effectué la mise à jour vers cette version avant d'essayer ces procédures.

## Créer des catégories d'appareils

1. Accédez à **Ressources et conformité** > **Vue d'ensemble** > **Regroupements d'appareils**.
2. Sous l'onglet **Accueil**, dans le groupe **Regroupements d'appareils**, choisissez **Gérer les catégories d'appareils**.
3. Créer, modifier ou supprimer des catégories.

## Associer un regroupement à une catégorie d'appareils

Quand vous associez un regroupement à une catégorie d'appareils, tous les appareils de cette catégorie sont ajoutés à ce regroupement. Vous ne pouvez pas ajouter une règle de catégorie d'appareils à un regroupement intégré comme **Tous les systèmes**.

1. Sous l'onglet **Règles d'adhésion** de la boîte de dialogue **Propriétés** pour un regroupement d'appareils, choisissez **Ajouter une règle** > **Règle de catégorie d'appareils**.
2. Dans la boîte de dialogue **Sélectionner des catégories d'appareils**, sélectionnez une ou plusieurs catégories d'appareils à appliquer à tous les appareils du regroupement.

## Changer la catégorie d'un appareil

1. Dans **Ressources et Conformité** > **Vue d'ensemble** > **Appareils**, sélectionnez un appareil dans la liste **Appareils**.
2. Sous l'onglet **Accueil**, dans le groupe **Appareil**, choisissez **Modifier la catégorie**.
3. Choisissez une catégorie, puis choisissez **OK**.

## Afficher la catégorie à laquelle appartient un appareil

Dans **Ressources et Conformité** > **Vue d'ensemble** > **Appareils**, dans la liste **Appareils**, la catégorie est affichée dans la colonne **Catégorie d'appareil**.

Si la colonne **Catégorie d'appareil** n'est pas affichée, cliquez avec le bouton droit sur l'en-tête de l'une des

colonnes dans la liste **Appareils** (comme **Nom**), puis sélectionnez **Catégorie d'appareil**.

Si vous affectez un appareil à une catégorie, puis supprimez par la suite cette catégorie, le rapport **Liste des appareils inscrits par utilisateur dans Microsoft Intune** affichera un GUID dans la colonne **Catégorie d'appareil** au lieu d'un nom de catégorie.

# Sécurité et confidentialité pour les regroupements dans System Center Configuration Manager

22/06/2018 • 3 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cette rubrique contient les bonnes pratiques en matière de sécurité et les informations de confidentialité pour les regroupements dans System Center Configuration Manager.

Il n'existe aucune information de confidentialité spécifique pour les regroupements dans Configuration Manager. Les regroupements sont des conteneurs pour les ressources, telles que les utilisateurs et les appareils. L'appartenance à un regroupement dépend souvent des informations recueillies par Configuration Manager pendant le fonctionnement standard. Par exemple, en utilisant les informations sur les ressources qui ont été collectées à partir de la découverte ou de l'inventaire, un regroupement peut être configuré pour renfermer les appareils qui répondent aux critères spécifiés. Les regroupements peuvent également reposer sur les informations d'état actuelles pour les opérations de gestion de client, telles que le déploiement de logiciels et la vérification de la compatibilité. En plus de ces regroupements basés sur des requêtes, les utilisateurs administratifs peuvent également ajouter des ressources aux regroupements.

Pour plus d'informations sur les regroupements, voir Présentation des regroupements dans System Center Configuration Manager. Pour plus d'informations sur les bonnes pratiques en matière de sécurité et les informations de confidentialité pour les opérations Configuration Manager qui peuvent être utilisées pour configurer l'appartenance à des regroupements, voir Bonnes pratiques en matière de sécurité et informations de confidentialité pour System Center Configuration Manager.

## Meilleures pratiques de sécurité pour les regroupements

Utilisez la meilleure pratique de sécurité suivante pour les regroupements.

| BONNES PRATIQUES DE SÉCURITÉ | PLUS D'INFORMATIONS |
|---|---|
| Lorsque vous exportez ou importez un regroupement à l'aide d'un fichier au format d'objet géré (MOF) qui est enregistré dans un emplacement réseau, sécurisez l'emplacement et le canal de réseau. | Veillez à restreindre l'accès au dossier réseau.<br><br>Utilisez la signature SMB ou IPsec entre l'emplacement réseau et le serveur de site pour empêcher un intrus de falsifier les données de regroupement exportées. Utilisez IPsec pour chiffrer les données sur le réseau afin d'éviter la divulgation d'informations. |

### Problèmes de sécurité pour les regroupements

Les regroupements présentent les problèmes de sécurité suivants :

- Si vous utilisez des variables de regroupement, les administrateurs locaux peuvent lire des informations potentiellement sensibles.

  Les variables de regroupement peuvent être utilisées lorsque vous déployez un système d'exploitation.

# Présentation de l'inventaire matériel dans System Center Configuration Manager

22/06/2018 • 5 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez l'inventaire matériel dans System Center Configuration Manager pour recueillir des informations sur la configuration matérielle des appareils clients de votre organisation. Pour recueillir l'inventaire matériel, le paramètre **Activer l'inventaire matériel sur les clients** doit être activé dans les paramètres client.

Une fois l'inventaire matériel activé et un cycle d'inventaire matériel exécuté par le client, ce dernier envoie les informations à un point de gestion sur le site du client. Le point de gestion transfère ensuite les informations d'inventaire au serveur de site Configuration Manager, qui les stocke dans la base de données du site. L'inventaire matériel s'exécute sur les clients en fonction de la planification que vous spécifiez dans les paramètres du client.

Vous pouvez utiliser plusieurs méthodes pour afficher les données d'inventaire matériel que Configuration Manager recueille. Ces référentiels sont notamment les suivants :

- Créer des requêtes qui retournent des appareils basés sur une configuration matérielle spécifique.
- Créer des regroupements basés sur des requêtes qui reposent sur une configuration matérielle spécifique. Les appartenances à un regroupement basé sur une requête sont mises à jour automatiquement selon un calendrier. Vous pouvez utiliser des regroupements pour plusieurs tâches, notamment le déploiement de logiciel. .
- Exécuter des rapports qui affichent des détails spécifiques sur les configurations matérielles de votre organisation.
- Utilisez l'Explorateur de ressources pour afficher des informations détaillées sur l'inventaire matériel collecté à partir d'appareils clients.

  Lorsque l'inventaire matériel s'exécute sur un appareil client, les premières données d'inventaire renvoyées par le client sont toujours un inventaire complet. Les informations d'inventaire suivantes contiennent uniquement des informations d'inventaire différentielles. Le serveur de site traite les informations d'inventaire différentielles selon l'ordre dans lequel il les reçoit. S'il manque des informations différentielles pour un client, le serveur de site rejette les informations différentielles supplémentaires et indique au client d'exécuter un cycle d'inventaire complet.

  Configuration Manager assure une prise en charge limitée des ordinateurs à double démarrage. Configuration Manager peut détecter les ordinateurs à double démarrage, mais retourne uniquement les informations d'inventaire du système d'exploitation qui était actif au moment de l'inventaire.

> **NOTE**
> Pour plus d'informations sur l'utilisation de l'inventaire matériel avec des clients qui exécutent Linux et UNIX, consultez Inventaire matériel pour Linux et UNIX dans System Center Configuration Manager.

## Extension de l'inventaire matériel Configuration Manager

En plus de l'inventaire matériel intégré dans Configuration Manager, vous pouvez également utiliser une des méthodes suivantes pour étendre l'inventaire matériel en vue de collecter des informations supplémentaires :

- Vous pouvez activer, désactiver, ajouter et supprimer des classes d'inventaire pour l'inventaire matériel à partir de la console Configuration Manager.
- Utilisez des fichiers NOIDMIF pour collecter des informations sur les appareils clients qui ne peuvent pas être inventoriés par Configuration Manager. Par exemple, vous pouvez souhaiter recueillir des informations numéros de périphérique actif qui existe uniquement en tant qu'étiquette sur le périphérique. Inventaire NOIDMIF est automatiquement associé à l'appareil client collectées à partir de.
- Utilisez des fichiers IDMIF pour collecter des informations sur les ressources qui ne sont associées à aucun client Configuration Manager ; par exemple, les projecteurs, les photocopieurs et les imprimantes réseau.

  Pour plus d'informations sur l'utilisation de ces méthodes pour étendre l'inventaire matériel de Configuration Manager, consultez Guide pratique pour configurer l'inventaire matériel dans System Center Configuration Manager.

# Comment étendre l'inventaire matériel dans System Center Configuration Manager

22/06/2018 • 20 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

L'inventaire matériel lit les informations sur les PC Windows en utilisant WMI (Windows Management Instrumentation). WMI est l'implémentation Microsoft de WBEM (Web-Based Enterprise Management), une norme sectorielle pour l'accès aux informations de gestion dans une entreprise. Dans les versions précédentes de Configuration Manager, vous étendiez l'inventaire matériel en modifiant le fichier sms_def.mof sur le serveur de site. Ce fichier contenait une liste de classes WMI qui pouvaient être lues par l'inventaire matériel. La modification de ce fichier vous permettait d'activer et de désactiver les classes existantes, et également de créer des classes à inventorier.

Le fichier Configuration.mof permet de définir les classes de données qui doivent faire l'objet d'un inventaire matériel sur le client. Il n'a pas été modifié depuis Configuration Manager 2012. Vous pouvez créer des classes de données pour inventorier les classes de données de référentiel WMI existantes ou personnalisées ou les clés de Registre présentes sur les systèmes clients.

Le fichier Configuration.mof définit également et inscrit les fournisseurs WMI d'accéder aux informations de périphérique durant l'inventaire matériel. L'enregistrement des fournisseurs définit le type de fournisseur à utiliser et les classes prises en charge par le fournisseur.

Quand les clients Configuration Manager demandent une stratégie, le fichier Configuration.mof est attaché au corps de la stratégie. Ce fichier est ensuite téléchargé et compilé par les clients. Lorsque vous ajoutez, modifiez ou supprimez des classes de données à partir du fichier Configuration.mof, les clients compilent automatiquement ces modifications sont apportées aux classes de données liées au stock. Aucune autre action n'est requise pour inventorier les classes de données nouvelles ou modifiées sur les clients Configuration Manager. Ce fichier se trouve dans **<emplacement_installation_CM>\Inboxes\clifiles.src\hinv** sur les serveurs de site principal.

Dans Configuration Manager, le fichier sms_def.mof n'a plus besoin d'être modifié comme c'était le cas dans Configuration Manager 2007. Au lieu de cela, vous pouvez activer et désactiver des classes WMI, et ajouter de nouvelles classes que l'inventaire matériel collectera, à l'aide des paramètres client. Configuration Manager permet d'étendre l'inventaire matériel à l'aide des méthodes ci-dessous.

> **NOTE**
> Si vous avez changé manuellement le fichier Configuration.mof pour ajouter des classes d'inventaire personnalisées, ces changements sont remplacés quand vous effectuez la mise à jour vers la version 1602. Pour continuer à utiliser des classes personnalisées après la mise à jour, vous devez les ajouter à la section « Added extensions » du fichier Configuration.mof après la mise à jour vers 1602.
> En revanche, vous ne devez rien modifier au-dessus de cette section, car la modification de ces sections est réservée à Configuration Manager. Une sauvegarde de votre fichier Configuration.mof personnalisé se trouve dans : **<répertoire_installation_CM>\data\hinvarchive**.

| MÉTHODE | PLUS D'INFORMATIONS |
| --- | --- |

| MÉTHODE | PLUS D'INFORMATIONS |
| --- | --- |
| Activer ou désactiver les classes d'inventaire existantes | Activez ou désactivez les classes d'inventaire par défaut ou créez des paramètres client personnalisés qui vous permettent de collecter différentes classes d'inventaire matériel depuis les regroupements de clients définis. Consultez la procédure Pour activer ou désactiver les classes existantes d'inventaire de cet article. |
| Ajouter une nouvelle classe d'inventaire | Ajoutez une nouvelle classe d'inventaire à partir de l'espace de noms WMI d'un autre appareil. Consultez la procédure Pour ajouter une nouvelle classe d'inventaire de cet article. |
| Importer et exporter des classes d'inventaire matériel | Importez et exportez des fichiers MOF (Managed Object Format) qui contiennent des classes d'inventaire à partir de la console Configuration Manager. Consultez les procédures Pour importer des classes d'inventaire matériel et Pour exporter des classes d'inventaire matériel de cet article. |
| Créer des fichiers NOIDMIF | Utilisez des fichiers NOIDMIF pour collecter des informations sur les appareils clients qui ne peuvent pas être inventoriés par Configuration Manager. Par exemple, vous pouvez souhaiter recueillir des informations numéros de périphérique actif qui existe uniquement en tant qu'étiquette sur le périphérique. Inventaire NOIDMIF est automatiquement associé à l'appareil client collectées à partir de. Consultez Pour créer des fichiers NOIDMIF dans cet article. |
| Créer les fichiers IDMIF | Utilisez des fichiers IDMIF pour collecter des informations sur les ressources de votre organisation qui ne sont associées à aucun client Configuration Manager, par exemple, les projecteurs, les photocopieurs et les imprimantes réseau. Consultez Pour créer des fichiers IDMIF dans cet article. |

# Procédures pour étendre l'inventaire matériel

Ces procédures vous aident à configurer les paramètres client par défaut pour l'inventaire matériel et elles s'appliquent à tous les clients de votre hiérarchie. Pour appliquer ces paramètres à certains clients uniquement, créez un paramètre d'appareil client personnalisé et affectez-le à un regroupement de clients spécifiques. Consultez Guide pratique pour configurer les paramètres client dans System Center Configuration Manager.

**Pour activer ou désactiver les classes existantes d'inventaire**

1. Dans la console Configuration Manager, choisissez **Administration** > **Paramètres client** > **Paramètres client par défaut**.
2. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
3. Dans la boîte de dialogue **Paramètres client par défaut**, choisissez **Inventaire matériel**.
4. Dans la liste **Paramètres du périphérique** , cliquez sur **Définir des classes**.
5. Dans la boîte de dialogue **Classes d'inventaire matériel** , sélectionnez ou désélectionnez les classes et les propriétés de classe que doit collecter l'inventaire matériel. Vous pouvez développer une classe pour sélectionner ou désélectionner des propriétés individuelles dans la classe. Utilisez le champ **Rechercher des classes d'inventaire** pour rechercher des classes individuelles.

> **IMPORTANT**
> Quand vous ajoutez de nouvelles classes à l'inventaire matériel Configuration Manager, la taille du fichier d'inventaire collecté et envoyé au serveur de site augmente. Cela peut nuire aux performances de votre réseau et du site Configuration Manager. Activez uniquement les classes d'inventaire à collecter.

**Pour ajouter une nouvelle classe d'inventaire**

Vous pouvez uniquement ajouter des classes d'inventaire à partir du serveur de niveau supérieur de la hiérarchie en modifiant les paramètres client par défaut. Cette option n'est pas disponible lorsque vous créez des paramètres de périphérique personnalisés.

1. Dans la console Configuration Manager, choisissez **Administration** > **Paramètres client** > **Paramètres client par défaut**.
2. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
3. Dans la boîte de dialogue **Paramètres client par défaut**, choisissez **Inventaire matériel**.
4. Dans la liste **Paramètres de l'appareil**, choisissez **Définir des classes**.
5. Dans la boîte de dialogue **Classes d'inventaire matériel**, choisissez **Ajouter**.
6. Dans la boîte de dialogue **Ajouter une classe d'inventaire matériel** , cliquez sur **Ajouter**.
7. Dans la boîte de dialogue **Connexion à Windows Management Instrumentation (WMI)** , définissez le nom de l'ordinateur depuis lequel vous allez extraire les classes WMI et l'espace de noms WMI à utiliser pour récupérer les classes. Si vous souhaitez récupérer toutes les classes sous l'espace de noms WMI spécifié, cliquez sur **Récursive**. Si l'ordinateur auquel vous vous connectez n'est pas l'ordinateur local, fournissez les informations d'identification d'un compte autorisé à accéder à WMI sur l'ordinateur distant.
8. Choisissez **Connexion**.
9. Dans la boîte de dialogue **Ajouter une classe d'inventaire matériel**, dans la liste des **classes d'inventaire**, sélectionnez les classes WMI à ajouter à l'inventaire matériel Configuration Manager.
10. Si vous souhaitez modifier des informations sur la classe WMI sélectionnée, choisissez **Modifier** et, dans la boîte de dialogue **Qualificatifs de classe**, fournissez les informations suivantes :

    - **Nom complet** : ce nom sera affiché dans l'Explorateur de ressources.
    - **Propriétés** : définissez l'unité dans laquelle s'affiche chaque propriété de la classe WMI.

      Vous pouvez également désigner des propriétés comme propriété de clé pour identifier de façon unique chaque instance de la classe. Si aucune clé n'est définie pour la classe et que plusieurs instances de la classe sont signalées par le client, seule la dernière instance trouvée est stockée dans la base de données.

      Une fois la configuration des propriétés terminée, cliquez sur **OK** pour fermer la boîte de dialogue **Qualificatifs de classe** et les autres boîtes de dialogue ouvertes.

**Pour importer des classes d'inventaire matériel**

Vous pouvez importer uniquement des classes d'inventaire lorsque vous modifiez les paramètres par défaut du client. Toutefois, vous pouvez utiliser des paramètres client personnalisés pour importer des informations qui n'incluent pas de changement de schéma, comme le changement de la propriété d'une classe existante en remplaçant la valeur **True** par **False**.

1. Dans la console Configuration Manager, choisissez **Administration** > **Paramètres client** > **Paramètres client par défaut**.

2. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
3. Dans la boîte de dialogue **Paramètres client par défaut**, choisissez **Inventaire matériel**.
4. Dans la liste **Paramètres de l'appareil**, choisissez **Définir des classes**.
5. Dans la boîte de dialogue **Classes d'inventaire matériel**, choisissez **Importer**.
6. Dans la boîte de dialogue **Importer**, sélectionnez le fichier MOF (Managed Object Format) à importer, puis choisissez **OK**. Passez en revue les éléments qui seront importés, puis cliquez sur **Importer**.

**Pour exporter des classes d'inventaire matériel**

1. Dans la console Configuration Manager, choisissez **Administration** > **Paramètres client** > **Paramètres client par défaut**.
2. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
3. Dans la boîte de dialogue **Paramètres client par défaut**, choisissez **Inventaire matériel**.
4. Dans la liste **Paramètres de l'appareil**, choisissez **Définir des classes**.
5. Dans la boîte de dialogue **Classes d'inventaire matériel**, choisissez **Exporter**.

   > **NOTE**
   > Lorsque vous exportez des classes, toutes les classes sélectionnées sont exportées.

6. Dans la boîte de dialogue **Exporter**, spécifiez le fichier MOF (Managed Object Format) vers lequel vous voulez exporter les classes, puis choisissez **Enregistrer**.

**Configurer l'inventaire matériel pour collecter les chaînes comportant plus de 255 caractères**

À compter de Configuration Manager 1802, vous pouvez spécifier une longueur de chaînes supérieure à 255 caractères pour les propriétés de l'inventaire matériel. Cette modification s'applique seulement aux classes nouvellement ajoutées et aux propriétés de l'inventaire matériel qui ne sont pas des clés.

1. Dans l'espace de travail **Administration**, cliquez sur **Paramètres client**, mettez en surbrillance un appareil client à modifier, cliquez avec le bouton droit, puis sélectionnez **Propriétés**.
2. Sélectionnez **Inventaire matériel**, puis **Définir des classes** et **Ajouter**.
3. Cliquez sur le bouton **Connecter**.
4. Renseignez **Nom de l'ordinateur** et **Espace de noms WMI**, et sélectionnez **Récursif** si nécessaire. Fournissez si nécessaire les informations d'identification pour la connexion. Cliquez sur **Connecter** pour afficher les classes de l'espace de noms.
5. Sélectionnez une nouvelle classe, puis cliquez sur **Modifier**.
6. Remplacez la **Longueur** de votre propriété autre que la clé et qui est une chaîne par une valeur supérieure à 255. Cliquez sur **OK**.
7. Vérifiez que la propriété modifiée est sélectionnée pour **Ajouter une classe d'inventaire matériel** et cliquez sur **OK**.

## Comment utiliser les fichiers MIF (Management Information Format) pour étendre l'inventaire matériel

Utilisez des fichiers MIF (Management Information Format) pour étendre les informations d'inventaire matériel recueillies auprès des clients par Configuration Manager. Au cours de l'inventaire matériel, les informations

stockées dans les fichiers MIF sont ajoutées au rapport d'inventaire du client et stockées dans la base de données de site. Vous pourrez utiliser les données depuis cet emplacement de la même manière que vous utilisez les données d'inventaire du client par défaut. Il existe deux types de fichiers MIF : NOIDMIF et IDMIF.

> **IMPORTANT**
> Avant d'ajouter les informations de fichiers MIF à la base de données Configuration Manager, vous devez créer ou importer des informations de classe pour eux. Pour plus d'informations, consultez les sections Pour ajouter une nouvelle classe d'inventaire et Pour importer des classes d'inventaire matériel de cet article.

**Pour créer des fichiers NOIDMIF**

Les fichiers NOIDMIF permettent d'ajouter à un inventaire matériel client des informations qui ne peuvent normalement pas être collectées par Configuration Manager et qui sont associées à un appareil client particulier. Par exemple, de nombreuses sociétés affectent à chaque ordinateur de l'organisation un numéro de ressource, puis classent ces numéros manuellement. Quand vous créez un fichier NOIDMIF, ces informations peuvent être ajoutées à la base de données Configuration Manager et être utilisées pour les requêtes et la génération de rapports. Pour plus d'informations sur la création de fichiers NOIDMIF, consultez la documentation du Kit de développement logiciel (SDK) Configuration Manager.

> **IMPORTANT**
> Quand vous créez un fichier NOIDMIF, il doit être enregistré dans un format codé ANSI. Les fichiers NOIDMIF enregistrés au format encodé UTF-8 ne peuvent pas être lus par Configuration Manager.

Après avoir créé un fichier NOIDMIF, stockez-le dans le dossier *%Windir%***\CCM\Inventory\Noidmifs** sur chaque client. Configuration Manager collecte les informations des fichiers NODMIF de ce dossier lors du prochain cycle d'inventaire matériel planifié.

**Pour créer des fichiers IDMIF**

Les fichiers IDMIF permettent d'ajouter à la base de données Configuration Manager des informations sur les ressources qui ne pourraient normalement pas être inventoriées par Configuration Manager et qui ne sont associées à aucun appareil client particulier. Par exemple, vous pouvez utiliser des fichiers IDMIF pour collecter des informations sur les projecteurs, lecteurs DVD, photocopieurs ou autres équipements qui ne disposent pas d'un client Configuration Manager. Pour plus d'informations sur la création de fichiers IDMIF, consultez la documentation du Kit de développement logiciel (SDK) Configuration Manager.

Après avoir créé un fichier IDMIF, stockez-le dans le dossier *%Windir%***\CCM\Inventory\Idmifs** sur les ordinateurs clients. Configuration Manager collecte les informations de ce fichier lors du prochain cycle d'inventaire matériel planifié. Vous devez déclarer de nouvelles classes pour les informations contenues dans le fichier en les ajoutant ou en les important.

> **NOTE**
> Les fichiers MIF peuvent contenir de grandes quantités de données et le regroupement de ces données pourrait affecter négativement les performances de votre site. Activez la collecte de fichiers MIF uniquement quand cela est nécessaire et configurez l'option **Taille maximale du fichier MIF personnalisé (Ko)** dans les paramètres d'inventaire matériel. Pour plus d'informations, consultez Présentation de l'inventaire matériel dans System Center Configuration Manager.

# Comment configurer l'inventaire matériel dans Configuration Manager

10/07/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cette procédure configure les paramètres client par défaut pour l'inventaire matériel et s'applique à tous les clients de votre hiérarchie. Si vous voulez que ces paramètres s'appliquent uniquement à certains clients, créez un paramètre client de périphérique personnalisé et affectez-le à un regroupement contenant les périphériques pour lesquels utiliser l'inventaire matériel. Consultez Guide pratique pour configurer les paramètres clients dans System Center Configuration Manager.

> **NOTE**
> Si un périphérique client reçoit des paramètres d'inventaire matériel de la part de plusieurs ensembles de paramètres client, les classes d'inventaire matériel de chaque ensemble de paramètres sont alors fusionnées lors de l'inventaire matériel.

**Pour configurer l'inventaire matériel**

1. Dans la console Configuration Manager, choisissez **Administration** > **Paramètres client** > **Paramètres client par défaut**.
2. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
3. Dans la boîte de dialogue **Paramètres par défaut**, choisissez **Inventaire matériel**.
4. Dans la liste **Paramètres de périphérique** , configurez les éléments suivants :
   - **Activer l'inventaire matériel sur les clients** : sélectionnez **Oui**.
   - **Calendrier de l'inventaire matériel** : Cliquez sur **Planifier** pour spécifier l'intervalle auquel les clients collectent l'inventaire matériel.
5. Configurez les autres paramètres clients d'inventaire matériel dont vous avez besoin.

Les périphériques client sont configurés en utilisant ces paramètres lors du prochain téléchargement de stratégie client. Pour lancer la récupération de stratégie pour un client unique, consultez Comment gérer des clients dans Configuration Manager.

# Comment utiliser l'Explorateur de ressources pour afficher l'inventaire matériel dans System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez l'Explorateur de ressources de System Center Configuration Manager pour afficher des informations sur l'inventaire matériel collecté à partir de clients de votre hiérarchie.

> **NOTE**
> L'Explorateur de ressources n'affichera pas de données d'inventaire avant qu'un cycle d'inventaire matériel ait été exécuté sur le client auquel vous êtes connecté.

L'Explorateur de ressources contient les sections suivantes relatives à l'inventaire matériel :

- **Matériel** : contient l'inventaire matériel le plus récent collecté à partir de l'appareil client indiqué. **État de la station de travail** : indique l'heure et la date du dernier inventaire matériel effectué par l'appareil.
- **Historique du matériel** : contient un historique des éléments d'inventaire qui ont été modifiés depuis le dernier inventaire matériel. Chaque élément contient un nœud **En cours** et un ou plusieurs nœuds *<date>*. Vous pouvez comparer les informations du nœud en cours à l'un des nœuds historiques pour découvrir les éléments qui ont été modifiés.

  > **NOTE**
  > Configuration Manager conserve l'historique de l'inventaire matériel pendant le nombre de jours que vous spécifiez dans la tâche de maintenance du site **Supprimer les historiques d'inventaire anciens**.

> **NOTE**
> Pour plus d'informations sur la façon d'afficher l'inventaire matériel des clients qui exécutent Linux et UNIX, consultez Guide pratique pour surveiller les clients pour des serveurs Linux et UNIX dans System Center Configuration Manager.

**Comment exécuter l'Explorateur de ressources à partir de la console Configuration Manager**

1. Dans la console Configuration Manager, choisissez **Ressources et Conformité** > **Appareils**, ou ouvrez un regroupement qui affiche des appareils.
2. Choisissez l'ordinateur contenant l'inventaire que vous souhaitez afficher puis, dans l'onglet **Accueil**, dans le groupe **Appareils**, choisissez **Démarrer** > **Explorateur de ressources**.
3. Cliquez avec le bouton droit sur un élément dans le volet droit de la fenêtre **Explorateur de ressources**, puis choisissez **Propriétés** pour ouvrir la boîte de dialogue *Propriétés de <nom_élément>* et visualiser les informations d'inventaire recueillies sous un format plus lisible.

# Inventaire matériel pour Linux et UNIX dans System Center Configuration Manager

22/06/2018 • 11 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Le client System Center Configuration Manager pour Linux et UNIX prend en charge l'inventaire matériel. Une fois l'inventaire matériel effectué, vous pouvez l'afficher dans l'Explorateur de ressources ou dans les rapports Configuration Manager, et utiliser ces informations pour créer des requêtes et des regroupements qui permettent d'effectuer les opérations suivantes :

- Déploiement logiciel
- Application de fenêtres de maintenance
- Déploiement de paramètres client personnalisés

L'inventaire matériel pour les serveurs Linux et UNIX utilise un serveur CIM (Common Information Model) basé sur des normes. Le serveur CIM s'exécute en tant que service logiciel (ou démon) et fournit une infrastructure de gestion basée sur des normes DMTF (Distributed Management Task Force). Il fournit des fonctionnalités semblables aux fonctionnalités CIM de l'infrastructure de gestion Windows (WMI, Windows Management Infrastructure) disponibles sur les ordinateurs Windows.

À partir de la mise à jour cumulative 1, le client pour Linux et UNIX utilise l' **omiserver** version 1.0.6 open source de l' **Open Group**. (Avant la mise à jour cumulative 1, le client utilisait **nanowbem** comme serveur CIM).

Le serveur CIM est installé dans le cadre de l'installation du client pour Linux et UNIX. Le client pour Linux et UNIX communique directement avec le serveur CIM. Il n'utilise pas l'interface WS-MAN du serveur CIM. Le port WS-MAN sur le serveur CIM est désactivé lors de l'installation du client. Microsoft a développé le serveur CIM désormais disponible en tant qu'open source par l'intermédiaire du projet OMI (Open Management infrastructure). Pour plus d'informations sur le projet OMI, consultez le site web The Open Group .

L'inventaire matériel sur les serveurs Linux et UNIX fonctionne en mappant les classes et les propriétés WMI Win32 existantes aux classes et propriétés équivalentes des serveurs Linux et UNIX. Ce mappage un-à-un des classes et des propriétés permet d'intégrer l'inventaire matériel Linux et UNIX à Configuration Manager. Les données d'inventaire des serveurs Linux et UNIX sont affichées avec l'inventaire des ordinateurs Windows dans la console et les rapports Configuration Manager. Vous bénéficiez ainsi d'une expérience de gestion cohérente et hétérogène.

> **TIP**
> Vous pouvez utiliser la valeur **Caption** pour la classe **Operating System** pour identifier différents systèmes d'exploitation Linux et UNIX dans les requêtes et les regroupements.

## Configuration de l'inventaire matériel pour les serveurs Linux et UNIX

Vous pouvez utiliser les paramètres client par défaut ou créer des paramètres d'appareil client personnalisés pour configurer l'inventaire matériel. Quand vous utilisez des paramètres d'appareil client personnalisés, vous pouvez configurer les classes et les propriétés que vous souhaitez collecter uniquement à partir de vos serveurs Linux et

UNIX. Vous pouvez également spécifier des planifications personnalisées pour la collecte d'inventaires delta et complets à partir de vos serveurs Linux et UNIX.

Le client pour Linux et UNIX prend en charge les classes d'inventaire matériel suivantes disponibles sur les serveurs Linux et UNIX :

- Win32_BIOS
- Win32_ComputerSystem
- Win32_DiskDrive
- Win32_DiskPartition
- Win32_NetworkAdapter
- Win32_NetworkAdapterConfiguration
- Win32_OperatingSystem
- Win32_Process
- Win32_Service
- Win32Reg_AddRemovePrograms
- SMS_LogicalDisk
- SMS_Processor

  Les propriétés de ces classes d'inventaire ne sont pas toutes activées pour les ordinateurs Linux et UNIX dans Configuration Manager.

## Opérations d'inventaire matériel

Une fois la collecte de l'inventaire matériel sur vos serveurs Linux et UNIX terminée, vous pouvez afficher et utiliser ces informations comme s'il s'agissait d'autres ordinateurs, et effectuer les opérations suivantes :

- Utiliser l'Explorateur de ressources pour afficher des informations détaillées sur l'inventaire matériel collecté à partir de serveurs Linux et UNIX
- Créer des requêtes basées sur des configurations matérielles spécifiques
- Créer des regroupements basés sur des requêtes qui reposent sur des configurations matérielles spécifiques
- Exécuter des rapports qui affichent des détails spécifiques sur les configurations matérielles

  L'inventaire matériel sur un serveur Linux ou UNIX s'exécute conformément au calendrier que vous configurez dans les paramètres client. Par défaut, l'inventaire est exécuté tous les sept jours. Le client pour Linux et UNIX prend en charge les cycles d'inventaire complet et les cycles d'inventaire delta.

  Vous pouvez également forcer le client sur un serveur Linux ou UNIX à exécuter immédiatement l'inventaire matériel. Pour exécuter l'inventaire matériel sur un client, utilisez des informations d'identification **racines** pour exécuter la commande suivante pour démarrer un cycle d'inventaire matériel : **/opt/microsoft/configmgr/bin/ccmexec -rs hinv**

  Les actions d'inventaire matériel sont entrées dans le fichier journal du client, **scxcm.log**.

## Comment utiliser l'infrastructure OMI pour créer un inventaire matériel personnalisé

Le client pour Linux et UNIX prend en charge l'inventaire matériel personnalisé que vous pouvez créer à l'aide de l'infrastructure OMI. Pour ce faire, vous devez procédez comme suit :

1. Créer un fournisseur d'inventaire personnalisé à l'aide de la source OMI
2. Configurer les ordinateurs pour qu'ils utilisent le nouveau fournisseur pour les rapports d'inventaire
3. Activer Configuration Manager pour prendre en charge le nouveau fournisseur

**Créer un fournisseur d'inventaire matériel personnalisé pour les ordinateurs Linux et UNIX :**

Pour créer un fournisseur d'inventaire matériel personnalisé pour le client Configuration Manager pour Linux et UNIX, utilisez **OMI Source - v.1.0.6** et suivez les instructions du guide de démarrage OMI. Ce processus comprend la création d'un fichier MOF (Managed Object Format) qui définit le schéma du nouveau fournisseur. Plus tard, vous importez le fichier MOF dans Configuration Manager pour activer la prise en charge de la nouvelle classe d'inventaire personnalisée.

Vous pouvez télécharger OMI Source - v.1.0.6 et le Guide de prise en main OMI à partir du site web The Open Group . Ces téléchargements se trouvent sous l'onglet **Documents** de la page web suivante sur le site web OpenGroup.org : Open Management Infrastructure (OMI).

**Configurer chaque ordinateur qui exécute Linux ou UNIX avec le fournisseur d'inventaire matériel personnalisé :**

Après avoir créé un fournisseur d'inventaire personnalisé, vous devez copier puis inscrire le fichier de bibliothèque du fournisseur sur chaque ordinateur dont vous souhaitez recueillir l'inventaire.

1. Copiez la bibliothèque du fournisseur sur chaque ordinateur Linux et UNIX dont vous souhaitez recueillir l'inventaire. Le nom de la bibliothèque du fournisseur ressemble à ceci : **XYZ_MyProvider.so**
2. Ensuite, sur chaque ordinateur Linux et UNIX, inscrivez la bibliothèque du fournisseur auprès du serveur OMI. Le serveur OMI s'installe sur l'ordinateur quand vous installez le client Configuration Manager pour Linux et UNIX, mais vous devez inscrire manuellement les fournisseurs personnalisés. Exécutez la ligne de commande suivante pour inscrire le fournisseur : **/opt/microsoft/omi/bin/omireg XYZ_MyProvider.so**
3. Une fois le nouveau fournisseur inscrit, testez-le à l'aide de l'outil **omicli** . L'outil **omicli** s'installe sur chaque ordinateur Linux et UNIX quand vous installez le client Configuration Manager pour Linux et UNIX. Par exemple, **XYZ_MyProvider** étant le nom du fournisseur que vous avez créé, exécutez la commande suivante sur l'ordinateur : **/opt/microsoft/omi/bin/omicli ei root/cimv2 XYZ_MyProvider**

   Pour plus d'informations sur **omicli** et sur la façon de tester les fournisseurs personnalisés, consultez le Guide de prise en main OMI.

> **TIP**
> Utilisez la distribution de logiciels pour déployer des fournisseurs personnalisés et pour inscrire des fournisseurs personnalisés sur chaque ordinateur client Linux et UNIX.

**Activer la nouvelle classe d'inventaire dans Configuration Manager :**

Pour que Configuration Manager puisse créer un rapport d'inventaire avec les données fournies par le nouveau fournisseur sur les ordinateurs Linux et UNIX, vous devez importer le fichier MOF qui définit le schéma de votre fournisseur personnalisé.

Pour importer un fichier MOF personnalisé dans Configuration Manager, consultez Guide pratique pour configurer l'inventaire matériel dans System Center Configuration Manager.

# Sécurité et confidentialité pour l'inventaire matériel dans System Center Configuration Manager

22/06/2018 • 6 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cette rubrique contient des informations de sécurité et de confidentialité pour l'inventaire matériel dans System Center Configuration Manager.

## Bonnes pratiques de sécurité pour l'inventaire matériel

Utilisez les meilleures pratiques de sécurité suivantes lorsque vous recueillez des données d'inventaire matériel à partir de clients :

| BONNES PRATIQUES DE SÉCURITÉ | PLUS D'INFORMATIONS |
|---|---|
| Signer et chiffrer les données d'inventaire | Lorsque les clients communiquent avec les points de gestion à l'aide du protocole HTTPS, toutes les données qu'ils envoient sont chiffrées à l'aide du protocole SSL. Toutefois, lorsque des ordinateurs clients utilisent le protocole HTTP pour communiquer avec des points de gestion sur l'intranet, les données d'inventaire client et les fichiers collectés peuvent être envoyés non signés et non chiffrés. Assurez-vous que le site est configuré pour exiger la signature et utiliser le chiffrement. En outre, si les clients peuvent prendre en charge l'algorithme SHA-256, sélectionnez l'option pour exiger SHA-256. |
| Ne pas recueillir de fichiers IDMIF et NOIDMIF dans des environnements haute sécurité | Vous pouvez utiliser le regroupement de fichiers IDMIF et NOIDMIF pour étendre l'inventaire matériel. Si nécessaire, Configuration Manager crée des tables ou modifie des tables existantes dans la base de données Configuration Manager pour prendre en compte les propriétés des fichiers IDMIF et NOIDMIF. En revanche, Configuration Manager ne valide pas les fichiers IDMIF et NOIDMIF. Ils peuvent donc être utilisés pour modifier des tables que vous ne souhaitez pas voir modifier. Les données valides peuvent être remplacées par des données non valides. En outre, de grandes quantités de données peuvent être ajoutées et le traitement de ces données peut entraîner des retards dans toutes les fonctions Configuration Manager. Pour atténuer ce risque, affectez la valeur **Aucun** au paramètre du client d'inventaire matériel **Collecter des fichiers MIF**. |

### Problèmes de sécurité pour l'inventaire matériel

La collecte d'inventaires engendre des vulnérabilités potentielles. Les intrus peuvent effectuer les opérations suivantes :

- Envoyer des données non valides qui seront acceptées par le point de gestion, même lorsque le paramètre du client d'inventaire logiciel est désactivé et le regroupement de fichiers n'est pas activé.
- Envoyer de trop grandes quantités de données dans un seul fichier et dans de nombreux fichiers, ce qui risque provoquer un déni de service.

- Accéder aux informations d'inventaire lors de leur transfert vers Configuration Manager.

  Dans la mesure où un utilisateur bénéficiant de privilèges d'administrateur local peut envoyer n'importe quelles informations comme données d'inventaire, ne considérez pas que les données d'inventaire collectées par Configuration Manager peuvent servir de référence.

  L'inventaire matériel est activé par défaut comme un paramètre client.

## Informations de confidentialité pour l'inventaire matériel

L'inventaire matériel vous permet de récupérer toutes les informations stockées dans le Registre et dans WMI sur les clients Configuration Manager. L'inventaire logiciel vous permet de découvrir tous les fichiers d'un type donné ou de collecter tous les fichiers spécifiés à partir des clients. Asset Intelligence améliore les capacités de l'inventaire en étendant l'inventaire matériel et logiciel et en ajoutant la nouvelle fonctionnalité de gestion des licences.

L'inventaire matériel est activé par défaut comme un paramètre client et les informations WMI recueillies sont déterminées par les options que vous sélectionnez. L'inventaire logiciel est activé par défaut, mais les fichiers ne sont pas recueillis par défaut. Le regroupement de données Asset Intelligence est automatiquement activé, bien que vous puissiez sélectionner les classes de rapport d'inventaire matériel à activer.

Les informations d'inventaire ne sont pas envoyées à Microsoft. Les informations d'inventaire sont stockées dans la base de données Configuration Manager. Lorsque les clients utilisent HTTPS pour se connecter à des points de gestion, les données d'inventaire qu'ils envoient au site sont chiffrées pendant le transfert. Si les clients utilisent le protocole HTTP pour se connecter à des points de gestion, vous pouvez activer le chiffrement d'inventaire. Les données d'inventaire ne sont pas stockées au format chiffré dans la base de données. Les informations sont conservées dans la base de données jusqu'à ce qu'elles soient supprimées par les tâches de maintenance du site **Supprimer les historiques d'inventaire anciens** ou **Supprimer les fichiers collectés anciens** tous les 90 jours. Vous pouvez configurer l'intervalle de suppression.

Avant de configurer l'inventaire matériel, l'inventaire logiciel, le regroupement de fichiers ou la collecte de données Asset Intelligence, tenez compte de vos exigences en matière de confidentialité.

# Présentation de l'inventaire logiciel dans System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez l'inventaire logiciel pour collecter des informations sur les fichiers présents sur les appareils clients. L'inventaire logiciel peut aussi collecter des fichiers auprès des appareils clients et les stocker sur le serveur de site. L'inventaire logiciel est collecté quand vous choisissez le paramètre **Activer l'inventaire logiciel sur les clients** dans les paramètres du client, où vous pouvez aussi planifier l'opération.

Une fois que l'inventaire logiciel est activé et que les clients exécutent un cycle d'inventaire logiciel, le client envoie les informations à un point de gestion dans le site du client. Le point de gestion transfère ensuite les informations d'inventaire au serveur de site Configuration Manager, qui les stocke dans la base de données du site.

Voici comment afficher les données de l'inventaire logiciel :

- Créez des requêtes qui retournent les appareils avec des fichiers spécifiés.
- Créez des regroupements basés sur une requête qui incluent les appareils avec des fichiers spécifiés.
- Exécutez des rapports qui fournissent des détails sur les fichiers présents sur les appareils.
- Utiliser l'Explorateur de ressources pour examiner les informations détaillées sur les fichiers qui ont été inventoriés et collectés sur les appareils clients.

  Quand un inventaire logiciel s'exécute sur un appareil client, le premier rapport d'inventaire est un inventaire complet. Les rapports d'inventaire suivants contiennent seulement des informations d'inventaire différentielles. Le serveur de site traite les informations différentielles selon l'ordre dans lequel il les reçoit. S'il manque des informations différentielles pour un client, le serveur de site rejette les informations différentielles suivantes et indique au client d'exécuter un inventaire complet.

  Configuration Manager peut détecter les ordinateurs à double démarrage, mais retourne uniquement les informations d'inventaire du système d'exploitation qui était actif au moment de l'inventaire.

**Appareils mobiles :** pour en savoir plus sur la collecte de l'inventaire des applications installées sur les appareils mobiles, voir Inventaire logiciel des appareils mobiles inscrits auprès de Microsoft Intune.

# Guide pratique pour configurer l'inventaire logiciel dans System Center Configuration Manager

22/06/2018 • 3 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cette procédure configure les paramètres par défaut du client pour l'inventaire logiciel et s'applique à tous les ordinateurs de votre hiérarchie. Si vous souhaitez appliquer ces paramètres uniquement à certains ordinateurs, créez un paramètre d'appareil client personnalisé et affectez-le à un regroupement. Pour plus d'informations sur la création de paramètres d'appareil personnalisés, consultez Guide pratique pour configurer les paramètres client dans System Center Configuration Manager.

## Pour configurer l'inventaire logiciel

1. Dans la console Configuration Manager, choisissez **Administration** > **Paramètres client Paramètres client par défaut**.
2. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
3. Dans la boîte de dialogue **Paramètres par défaut**, choisissez **Inventaire logiciel**.
4. Dans la liste **Paramètres de périphérique** , configurez les valeurs suivantes :
   - **Activer l'inventaire logiciel sur les clients** : dans la liste déroulante, sélectionnez **Vrai**.
   - **Planifier l'inventaire logiciel et le regroupement de fichiers** : définit la fréquence de collecte de l'inventaire logiciel et des fichiers par les clients.
5. Configurez les paramètres client dont vous avez besoin. La section Inventaire logiciel de l'article À propos des paramètres client dans System Center Configuration Manager contient une liste des paramètres client.

   Les ordinateurs clients sont configurés avec ces paramètres lorsqu'ils téléchargent la stratégie client. Pour lancer la récupération de stratégie pour un client unique, consultez Comment gérer les clients dans System Center Configuration Manager.

   **TIP**
   Le code d'erreur 80041006 dans inventoryprovider.log signifie que la mémoire du fournisseur WMI est insuffisante. Autrement dit, la limite de quota de mémoire pour un fournisseur a été atteinte et le fournisseur d'inventaire ne peut pas continuer. Dans ce cas, l'agent d'inventaire crée un rapport avec 0 entrée, et aucun élément d'inventaire n'est signalé.
   Une solution possible consiste à réduire l'étendue de la collecte d'inventaire logiciel. Dans les cas où l'erreur se produit après la limitation de l'étendue de l'inventaire, l'augmentation de la propriété MemoryPerHost définie dans la classe _ProviderHostQuotaConfiguration peut constituer une solution.

## Pour exclure des dossiers d'un inventaire logiciel

1. Dans Notepad.exe, créez un fichier vide intitulé **Skpswi.dat**.
2. Cliquez avec le bouton droit sur le fichier **Skpswi.dat** et cliquez sur **Propriétés**. Dans les propriétés du fichier Skpswi.dat, sélectionnez l'attribut **Masqué** .

3. Placez le fichier **Skpswi.dat** à la racine du disque dur ou de la structure de dossiers de chaque client que vous souhaitez exclure de l'inventaire logiciel.

> **NOTE**
>
> L'inventaire logiciel n'effectue pas un nouvel inventaire du lecteur de client à moins que le fichier ne soit supprimé du lecteur sur l'ordinateur client.

# Comment utiliser l'Explorateur de ressources pour afficher l'inventaire logiciel dans System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez l'Explorateur de ressources de System Center Configuration Manager pour afficher des informations sur l'inventaire logiciel collecté auprès des ordinateurs de votre hiérarchie.

> **NOTE**
> L'Explorateur de ressources n'affiche pas de données d'inventaire tant qu'un cycle d'inventaire logiciel n'a pas été exécuté sur le client.

L'Explorateur de ressources fournit les informations d'inventaire matériel et logiciel suivantes :

- **Logiciels** :
  - **Fichiers collectés** : fichiers collectés lors de l'inventaire logiciel.
  - **Détails du fichier** : fichiers qui ont été inventoriés pendant l'inventaire logiciel, et qui ne sont pas associés à un produit ou un fabricant spécifique.
  - **Dernière analyse logicielle** : date et heure de la dernière collecte d'inventaire logiciel et de fichiers pour l'ordinateur client.
  - **Détails du produit** : produits logiciels qui ont été inventoriés par l'inventaire logiciel, regroupés par fabricant.

## Pour exécuter l'Explorateur de ressources à partir de la console Configuration Manager

1. Dans la console Configuration Manager, choisissez **Ressources et Conformité**.
2. Dans l'espace de travail **Ressources et Conformité**, cliquez sur **Appareils** ou ouvrez un regroupement qui affiche des appareils.
3. Choisissez l'ordinateur contenant l'inventaire que vous voulez afficher puis, sous l'onglet **Accueil**, dans le groupe **Appareils**, choisissez **Démarrer** > **Explorateur de ressources**.
4. Vous pouvez cliquer avec le bouton droit sur un élément dans le volet droit de la fenêtre Explorateur de ressources, puis choisir **Propriétés** pour visualiser les informations d'inventaire collectées dans un format plus lisible.

# Sécurité et confidentialité pour l'inventaire logiciel dans System Center Configuration Manager

22/06/2018 • 6 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cette rubrique contient des informations de sécurité et de confidentialité pour l'inventaire logiciel dans System Center Configuration Manager.

## Meilleures pratiques de sécurité pour l'inventaire logiciel

Utilisez les meilleures pratiques de sécurité suivantes lorsque vous recueillez des données d'inventaire logiciel à partir de clients :

| BONNES PRATIQUES DE SÉCURITÉ | PLUS D'INFORMATIONS |
|---|---|
| Signer et chiffrer les données d'inventaire | Lorsque les clients communiquent avec les points de gestion à l'aide du protocole HTTPS, toutes les données qu'ils envoient sont chiffrées à l'aide du protocole SSL. Toutefois, lorsque des ordinateurs clients utilisent le protocole HTTP pour communiquer avec des points de gestion sur l'intranet, les données d'inventaire client et les fichiers collectés peuvent être envoyés non signés et non chiffrés. Assurez-vous que le site est configuré pour exiger la signature et utiliser le chiffrement. En outre, si les clients peuvent prendre en charge l'algorithme SHA-256, sélectionnez l'option pour exiger SHA-256. |
| N'utilisez pas le regroupement de fichiers pour collecter des fichiers critiques ou des informations sensibles | L'inventaire logiciel Configuration Manager utilise tous les droits du compte LocalSystem, qui permet de recueillir des copies de fichiers système critiques, tels que le Registre ou la base de données du compte de sécurité. Lorsque ces fichiers sont disponibles sur le serveur de site, un individu disposant des droits Lire la ressource ou de droits NTFS sur l'emplacement de stockage du fichier pourrait en analyser le contenu et probablement découvrir des informations essentielles sur le client, ce qui permettrait de compromettre sa sécurité. |
| Restreindre les droits d'administrateur local sur les ordinateurs client | Un utilisateur disposant des droits d'administrateur local peut envoyer des données non valides comme informations d'inventaire. |

**Problèmes de sécurité pour l'inventaire logiciel**

La collecte d'inventaires engendre des vulnérabilités potentielles. Les intrus peuvent effectuer les opérations suivantes :

- Envoyer des données non valides qui seront acceptées par le point de gestion, même lorsque le paramètre du client d'inventaire logiciel est désactivé et le regroupement de fichiers n'est pas activé.
- Envoyer de trop grandes quantités de données dans un seul fichier et dans de nombreux fichiers, ce qui risque provoquer un déni de service.
- Accéder aux informations d'inventaire lors de leur transfert vers Configuration Manager.

Si les utilisateurs savent qu'ils peuvent créer un fichier masqué appelé **Skpswi.dat** et le placer à la racine du disque dur d'un client pour l'exclure de l'inventaire logiciel, vous ne pourrez pas recueillir de données d'inventaire logiciel à partir de cet ordinateur.

Dans la mesure où un utilisateur bénéficiant de privilèges d'administrateur local peut envoyer n'importe quelles informations comme données d'inventaire, ne considérez pas que les données d'inventaire collectées par Configuration Manager peuvent servir de référence.

L'inventaire logiciel est activé par défaut comme un paramètre client.

## Informations de confidentialité pour l'inventaire logiciel

L'inventaire matériel vous permet de récupérer toutes les informations stockées dans le Registre et dans WMI sur les clients Configuration Manager. L'inventaire logiciel vous permet de découvrir tous les fichiers d'un type donné ou de collecter tous les fichiers spécifiés à partir des clients. Asset Intelligence améliore les capacités de l'inventaire en étendant l'inventaire matériel et logiciel et en ajoutant la nouvelle fonctionnalité de gestion des licences.

L'inventaire matériel est activé par défaut comme un paramètre client et les informations WMI recueillies sont déterminées par les options que vous sélectionnez. L'inventaire logiciel est activé par défaut, mais les fichiers ne sont pas recueillis par défaut. Le regroupement de données Asset Intelligence est automatiquement activé, bien que vous puissiez sélectionner les classes de rapport d'inventaire matériel à activer.

Les informations d'inventaire ne sont pas envoyées à Microsoft. Les informations d'inventaire sont stockées dans la base de données Configuration Manager. Lorsque les clients utilisent HTTPS pour se connecter à des points de gestion, les données d'inventaire qu'ils envoient au site sont chiffrées pendant le transfert. Si les clients utilisent le protocole HTTP pour se connecter à des points de gestion, vous pouvez activer le chiffrement d'inventaire. Les données d'inventaire ne sont pas stockées au format chiffré dans la base de données. Les informations sont conservées dans la base de données jusqu'à ce qu'elles soient supprimées par les tâches de maintenance du site **Supprimer les historiques d'inventaire anciens** ou **Supprimer les fichiers collectés anciens** tous les 90 jours. Vous pouvez configurer l'intervalle de suppression.

Avant de configurer l'inventaire matériel, l'inventaire logiciel, le regroupement de fichiers ou la collecte de données Asset Intelligence, tenez compte de vos exigences en matière de confidentialité.

# Présentation d'Asset Intelligence dans System Center Configuration Manager

22/06/2018 • 36 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Asset Intelligence dans System Center Configuration Manager permet d'inventorier et de gérer l'utilisation des licences logicielles dans l'entreprise en utilisant le catalogue Asset Intelligence. De nombreuses classes WMI (Windows Management Instrumentation) d'inventaire matériel améliorent l'éventail des informations collectées sur le matériel et les noms de logiciels en cours d'utilisation. Ces informations sont présentées dans plus de 60 rapports dans un format pratique. La plupart de ces rapports renvoient vers des rapports plus spécifiques qui permettent de rechercher des informations générales et d'accéder à des informations plus détaillées. Vous pouvez ajouter des informations personnalisées dans le catalogue Asset Intelligence, telles que des catégories de logiciels, des familles de logiciels, des légendes logicielles et des configurations matérielles requises personnalisées. En outre, les clients peuvent se connecter à System Center Online pour mettre à jour dynamiquement le catalogue Asset Intelligence avec les dernières informations disponibles. Les clients Microsoft peuvent également rapprocher l'utilisation des licences logicielles de l'entreprise avec les licences logicielles achetées en cours d'utilisation en important les informations de licence logicielle dans la base de données du site Configuration Manager.

## Catalogue Asset Intelligence

Le catalogue Asset Intelligence Configuration Manager est un ensemble de tables stockées dans la base de données de site qui contiennent les informations de catégorisation et d'identification de plus de 300 000 titres et versions de logiciels. Ces tables de base de données sont également utilisées pour gérer les configurations matérielles requises des titres de logiciels.

Le catalogue Asset Intelligence fournit des informations sur les licences des logiciels utilisés, Microsoft et non-Microsoft. Un ensemble prédéfini de configurations matérielles requises pour les titres de logiciels figure dans le catalogue Asset Intelligence et vous pouvez créer des informations de configuration matérielle requise définies par l'utilisateur en fonction de vos besoins. En outre, vous pouvez personnaliser les informations dans le catalogue Asset Intelligence et envoyer les informations de titres de logiciels à System Center Online pour les catégoriser.

Des mises à jour en bloc du catalogue Asset Intelligence qui contiennent les nouvelles versions des logiciels sont régulièrement téléchargeables. Ou bien, vous pouvez mettre à jour le catalogue de façon dynamique en utilisant le rôle de système de site du point de synchronisation Asset Intelligence.

### Catégories de logiciels

Les catégories de logiciels Asset Intelligence permettent de catégoriser de façon large les titres de logiciels inventoriés et comme regroupements généraux de familles de logiciels plus spécifiques. Par exemple, « Société d'énergie » peut correspondre à une catégorie de logiciels, et « Pétrole », « Gaz » ou « Hydroélectrique » peuvent correspondre à des familles de logiciels dans cette catégorie. La plupart des catégories de logiciels sont prédéfinies dans le catalogue Asset Intelligence, et vous pouvez créer des catégories définies par l'utilisateur pour spécifier plus précisément les logiciels inventoriés. L'état de validation de toutes les catégories de logiciels prédéfinies est toujours **Validé**, alors que les informations de catégories de logiciels personnalisées ajoutées au catalogue Asset Intelligence ont l'état **Défini par l'utilisateur** Pour plus d'informations sur la gestion des catégories de logiciels, consultez Configuration d'Asset Intelligence dans System Center Configuration Manager.

> **NOTE**
> Les informations de catégories de logiciels prédéfinies stockées dans le catalogue Asset Intelligence sont accessibles en lecture seule et ne peuvent pas être modifiées ni supprimées. Les utilisateurs administratifs peuvent ajouter, modifier ou supprimer des catégories de logiciels définies par l'utilisateur.

### Familles de logiciels

Les familles de logiciels Asset Intelligence permettent de définir les titres de logiciels dans les catégories de logiciels. La plupart des familles de logiciels sont prédéfinies dans le catalogue Asset Intelligence, et vous pouvez créer des catégories définies par l'utilisateur pour définir plus précisément les logiciels inventoriés. L'état de validation de toutes les familles de logiciels prédéfinies est toujours **Validé**, alors que les informations de familles de logiciels personnalisées ajoutées au catalogue Asset Intelligence ont l'état **Défini par l'utilisateur** Pour plus d'informations sur la gestion des familles de logiciels, consultez Configuration d'Asset Intelligence dans System Center Configuration Manager.

> **NOTE**
> Les informations sur les familles de logiciels prédéfinies sont accessibles en lecture seule et ne peuvent pas être modifiées. Les utilisateurs administratifs peuvent ajouter, modifier ou supprimer des familles de logiciels définies par l'utilisateur.

### Légendes logicielles

Les légendes logicielles personnalisées Asset Intelligence permettent de créer des filtres que vous pouvez utiliser pour regrouper des titres de logiciels et les afficher en utilisant des rapports Asset Intelligence. Vous pouvez utiliser des légendes logicielles pour créer des groupes de titres de logiciels ayant un attribut commun. Par exemple, vous pouvez créer la légende logicielle « Logiciel à contribution volontaire », associer la légende aux titres de logiciels à contribution volontaire et exécuter un rapport pour afficher tous les titres de logiciels avec la légende Logiciel à contribution volontaire. Les légendes logicielles ne sont pas prédéfinies. L'état de validation des légendes logicielles est toujours **Défini par l'utilisateur**. Pour plus d'informations sur la gestion des légendes logicielles, consultez Configuration d'Asset Intelligence dans System Center Configuration Manager.

### Configuration matérielle requise

Vous pouvez utiliser les informations de configuration de matériel requise pour vérifier que les ordinateurs répondent à la configuration matérielle requise pour les titres de logiciels avant d'y déployer des logiciels. Vous pouvez gérer les configurations matérielles requises pour les titres de logiciels dans l'espace de travail **Biens et conformité** dans le noeud **Configuration matérielle requise** sous le noeud **Asset Intelligence** . La plupart des configurations matérielles requises sont prédéfinies dans le catalogue Asset Intelligence et vous pouvez créer des informations de configuration matérielle définies par l'utilisateur pour répondre à des besoins spécifiques. L'état de validation de toutes les configurations matérielles requises prédéfinies est toujours **Validé**, tandis que celui des informations de configuration matérielle requise définies par l'utilisateur ajoutées au catalogue Asset Intelligence est **Défini par l'utilisateur**. Pour plus d'informations sur la gestion de la configuration matérielle requise, consultez Configuration d'Asset Intelligence dans System Center Configuration Manager.

> **NOTE**
> Les informations de configuration matérielle requise figurant dans la console Configuration Manager sont tirées du catalogue Asset Intelligence et elles ne reposent pas sur les informations de titres de logiciels inventoriés sur les clients System Center 2012 Configuration Manager. Les informations de configuration matérielle requise ne sont pas mises à jour au cours de la synchronisation avec System Center Online. Vous pouvez créer une configuration matérielle requise définie par l'utilisateur pour le logiciel inventorié n'ayant pas de configuration matérielle.

Les informations suivantes s'affichent pour chaque configuration matérielle requise répertoriée :

- **Nom du logiciel**: spécifie le titre du logiciel associé à la configuration matérielle requise.
- **Vitesse min. du processeur (MHz)**: spécifie la vitesse minimale du processeur, en mégahertz (MHz), nécessaire au logiciel.
- **Mémoire RAM minimum (Ko)**: spécifie la quantité de mémoire vive minimale en kilo-octets (Ko) nécessaire au logiciel.
- **Espace disque minimum (Ko)**: spécifie l'espace disque libre minimal en Ko nécessaire au logiciel.
- **Taille minimale du disque (Ko)**: spécifie l'espace disque libre minimal en Ko nécessaire au logiciel.
- **État de validation**: spécifie l'état de validation de la configuration matérielle requise.

  Les configurations matérielles requises prédéfinies stockées dans le catalogue Asset Intelligence sont accessibles en lecture seule et ne peuvent pas être supprimées. Les utilisateurs administratifs peuvent ajouter, modifier ou supprimer des configurations matérielles définies par l'utilisateur pour les titres de logiciels qui ne sont pas stockés dans le catalogue Asset Intelligence.

## Logiciels inventoriés

Vous pouvez afficher les informations de titres de logiciels inventoriés dans l'espace de travail **Biens et conformité** dans le noeud **Logiciels inventoriés** sous le noeud **Asset Intelligence** . L'agent du client d'inventaire matériel collecte les informations des logiciels inventoriés à partir des clients Configuration Manager en fonction des titres de logiciels stockés dans le catalogue Asset Intelligence.

> **WARNING**
> L'agent du client d'inventaire matériel collecte l'inventaire en fonction des classes de création de rapports d'inventaire matériel Asset Intelligence que vous activez. Pour plus d'informations sur l'activation des classes de création de rapports, consultez Configuration d'Asset Intelligence dans System Center Configuration Manager.

Par défaut, les informations suivantes s'affichent pour chaque titre de logiciel inventorié :

- **Nom**: spécifie le nom du logiciel inventorié.
- **Fournisseur**: spécifie le nom du fournisseur qui a développé le logiciel inventorié.
- **Version**: indique la version du produit du logiciel inventorié.
- **Catégorie**: spécifie la catégorie actuellement affectée au logiciel inventorié.
- **Famille**: spécifie la famille actuellement affectée au logiciel inventorié.
- **Légende** [**1**, **2**et **3**] : spécifie les légendes personnalisées associées au logiciel. Les titres de logiciels inventoriés peuvent avoir jusqu'à trois légendes personnalisées.
- **Nombre** : spécifie le nombre de clients Configuration Manager qui ont inventorié le logiciel.
- **État**: spécifie l'état de validation du logiciel inventorié.

> **NOTE**
> Vous pouvez modifier les informations de catégorisation (nom du produit, fournisseur, catégorie et famille) des logiciels inventoriés uniquement sur le site de niveau supérieur de votre hiérarchie. Lorsque vous modifiez les informations de catégorisation des logiciels prédéfinis, l'état de validation **Validé** des logiciels devient **Défini par l'utilisateur**.

## Point de synchronisation Asset Intelligence

Le point de synchronisation Asset Intelligence est un rôle système de site Configuration Manager utilisé pour établir une connexion à System Center Online (via le port TCP 443) pour gérer les mises à jour dynamiques des informations du catalogue Asset Intelligence. Ce rôle de site peut être installé uniquement sur le site de niveau supérieur de la hiérarchie. Vous devez configurer toutes les personnalisations de catalogue Asset Intelligence en utilisant une console Configuration Manager connectée au site de niveau supérieur. Même si toutes les mises à jour doivent être configurées sur le site de niveau supérieur, les informations de catalogue Asset Intelligence sont répliquées sur les autres sites de la hiérarchie. Le rôle de site du point de synchronisation Asset Intelligence permet de synchroniser le catalogue à la demande avec System Center Online ou de planifier la synchronisation automatique du catalogue. Outre le téléchargement des nouvelles informations du catalogue Asset Intelligence, le point de synchronisation Asset Intelligence peut envoyer les informations de titres de logiciels personnalisés à System Center Online à des fins de catégorisation. Microsoft considère tous les titres de logiciels envoyés à System Center Online pour être catégorisés comme des informations publiques. Ainsi, vous devez vérifier que vos titres de logiciels personnalisés ne contiennent pas d'informations confidentielles ou propriétaires.

> **NOTE**
> Lorsque vous envoyez un titre de logiciel non catégorisé et qu'au moins quatre clients ont demandé la catégorisation du titre, les programmes de recherche System Center Online identifient et catégorisent les informations du titre logiciel et rendent les informations de catégorisation accessibles à tous les clients qui utilisent le service en ligne. Les titres de logiciels ayant le plus grand nombre de demandes de catégorisation sont affectés de la priorité de catégorisation la plus élevée. Les logiciels personnalisés et les applications métier sont peu susceptibles de recevoir une catégorie, et nous vous conseillons de ne pas envoyer ces logiciels à Microsoft pour catégorisation.

> **NOTE**
> Le rôle de système de site du point de synchronisation Asset Intelligence est nécessaire pour se connecter System Center Online. Pour plus d'informations sur l'installation d'un point de synchronisation Asset Intelligence, consultez Configuration d'Asset Intelligence dans System Center Configuration Manager.

## Page d'accueil d'Asset Intelligence

Le nœud **Asset Intelligence** dans l'espace de travail **Biens et conformité** est la page d'accueil d'Asset Intelligence dans Configuration Manager. La page d'accueil d' **Asset Intelligence** contient une vue de tableau de bord récapitulant les informations du catalogue Asset Intelligence.

> **NOTE**
> La page d'accueil d' **Asset Intelligence** n'est pas automatiquement actualisée lorsqu'elle s'affiche.

La page d'accueil **Asset Intelligence** contient les sections suivantes :

- **Synchronisation de catalogue**: indique si Asset Intelligence est activé et l'état actuel du point de synchronisation Asset Intelligence. Cette section indique également la planification de la synchronisation, si la déclaration de licence du client est importée, la date de la dernière mise à jour de l'état et l'heure de la prochaine mise à jour planifiée, ainsi que le nombre de modifications effectuées après l'installation du système de site du point de synchronisation Asset Intelligence.

> **NOTE**
> La section de synchronisation du catalogue Asset Intelligence de la page d'accueil **Asset Intelligence** s'affiche uniquement si un rôle de système de site du point de synchronisation Asset Intelligence a été installé.

- **État des logiciels inventoriés**: indique le nombre et le pourcentage de logiciels, catégories de logiciels et familles de logiciels inventoriés qui sont identifiés par Microsoft, identifiés par un administrateur, en attente d'identification en ligne ou non identifiés et pas en attente. Les informations affichées dans un tableau indiquent le nombre pour chacun des éléments, tandis que les informations affichées dans le graphique indiquent le pourcentage de chacun des éléments.

## Rapports Asset Intelligence

Les rapports Asset Intelligence se trouvent dans la console Configuration Manager, dans l'espace de travail **Surveillance** dans le dossier Asset Intelligence sous le nœud **Rapports**. Les rapports fournissent des informations sur les matériels, la gestion des licences et les logiciels. Pour plus d'informations sur les rapports de Configuration Manager, consultez Génération de rapports dans System Center Configuration Manager.

> **NOTE**
> La précision du nombre de logiciels installés et des informations de licence affichés dans les rapports Asset Intelligence peut varier par rapport au nombre réel de logiciels installés ou de licences utilisées dans l'environnement. Cette variation est due aux dépendances et limitations complexes qu'implique l'inventaire des informations de licence des logiciels installés dans les environnements d'entreprise. N'utilisez pas les rapports Asset Intelligence comme seule source pour déterminer la conformité des licences logicielles achetées.

### Rapports matériels Asset Intelligence

Les rapports matériels Asset Intelligence fournissent des informations sur les ressources matérielles de l'organisation. En utilisant les informations d'inventaire matériel, comme la vitesse, la mémoire, les périphériques, etc., les rapports matériels Asset Intelligence peuvent contenir des informations sur les appareils USB, le matériel à mettre à niveau et même les ordinateurs qui ne sont pas prêts à recevoir une mise à niveau logicielle donnée.

> **NOTE**
> Certaines données utilisateur dans les rapports Asset Intelligence sont collectées depuis le journal des événements de la sécurité du système. Pour améliorer l'exactitude des rapports, il est recommandé de nettoyer ce journal quand vous réaffectez un ordinateur à un autre utilisateur.

### Rapports de gestion de licences Asset Intelligence

Les rapports de gestion des licences Asset Intelligence fournissent des données sur les licences en cours d'utilisation. Le rapport Grand livre des licences répertorie les applications Microsoft installées dans un format semblable à un relevé de licences Microsoft. Il fournit une méthode pratique de mise en correspondance des licences achetées et des licences utilisées. D'autres rapports de gestion des licences fournissent des informations sur les ordinateurs faisant office de serveurs exécutant le Service de gestion de clés (KMS) pour les statistiques d'activation du système d'exploitation.

> **IMPORTANT**
> Plusieurs rapports de gestion des licences Asset Intelligence présentent des informations sur la fonction du Service de gestion de clés, une méthode d'administration des licences en volume. Si aucun serveur KMS n'a été implémenté, certains rapports ne contiendront aucune donnée. Pour plus d'informations sur KMS, recherchez KMS sur Microsoft TechNet.

### Rapports logiciels Asset Intelligence

Les rapports logiciels Asset Intelligence fournissent des informations sur les familles de logiciels, les catégories et les titres de logiciels qui sont installés sur les ordinateurs de l'organisation. Ils contiennent, entre autres, des informations sur les objets Application d'assistance du navigateur et les logiciels qui démarrent automatiquement. Ces rapports peuvent permettre d'identifier les logiciels de publicité, les logiciels espions et d'autres programmes malveillants, ainsi que les redondances logicielles afin de rationaliser l'achat et le support des logiciels.

### Rapports sur les balises d'identification logicielle Asset Intelligence

Rapports de balise d'identification de logiciels Asset Intelligence fournissent des informations sur les logiciels qui contient une balise d'identification logicielle conforme à ISO/IEC 19770-2. Ces balises d'identification logicielle fournissent des informations faisant autorité servant à identifier les logiciels installés. Quand vous activez la classe de rapport d'inventaire matériel SMS_SoftwareTag, Configuration Manager collecte des informations sur les logiciels dotés de balises d'identification logicielle. Les rapports suivants fournissent des informations sur les logiciels :

- **Logiciels 14A - Recherche de logiciels dont la balise d'identification logicielle est activée** : ce rapport indique le nombre de logiciels installés qui ont une balise d'identification logicielle activée.
- **Logiciels 14B - Ordinateurs sur lesquels sont installés des logiciels ayant une balise d'identification logicielle spécifique activée** : ce rapport répertorie tous les ordinateurs qui ont installé des logiciels dotés d'une balise d'identification logicielle spécifique activée.
- **Logiciels 14C - Balise d'identification logicielle installée activée sur un ordinateur spécifique** : ce rapport répertorie tous les logiciels installés dotés d'une balise d'identification logicielle spécifique activée sur un ordinateur spécifique.

### Limites des rapports Asset Intelligence

Les rapports Asset Intelligence peuvent fournir une grande quantité d'informations sur les titres de logiciels installés et les licences logicielles achetées en cours d'utilisation. Toutefois, n'utilisez pas ces informations comme seule source pour déterminer la conformité des licence logicielles achetées.

#### Exemples de dépendances

La précision de la quantité affichée dans les rapports Asset Intelligence installé les logiciels et les informations de licence peuvent varier des quantités réelles actuellement utilisées. Cette variation est due aux dépendances complexes qu'implique l'inventaire des informations de licence des logiciels en cours d'utilisation dans les environnements d'entreprise. Les exemples suivants montrent les dépendances liées à l'inventaire des logiciels installés dans l'entreprise en utilisant Asset Intelligence, qui sont susceptibles d'affecter l'exactitude des rapports Asset Intelligence :

### Dépendances d'inventaire matériel sur les clients

Les rapports Asset Intelligence des logiciels installés sont basés sur les données collectées sur les clients Configuration Manager en étendant l'inventaire matériel afin d'activer la création de rapports Asset Intelligence. En raison de ces dépendances par rapport à la création de rapports d'inventaire matériel, les rapports Asset Intelligence contiennent uniquement les données des clients Configuration Manager qui ont terminé le processus d'inventaire matériel avec les classes de rapport Asset Intelligence WMI requises activées. En outre, puisque les clients Configuration Manager exécutent les processus d'inventaire matériel selon un calendrier défini par l'utilisateur administratif, il peut exister un décalage au niveau des rapports de données, qui affecte l'exactitude des rapports Asset Intelligence. Par exemple, un logiciel sous licence inventorié peut être désinstallé après que le client a terminé un cycle d'inventaire matériel. Toutefois, le logiciel apparaît comme étant installé dans les rapports Asset Intelligence jusqu'au prochain cycle de rapports d'inventaire matériel du client.

### Dépendances de package de logiciel

Étant donné que les rapports Asset Intelligence reposent sur les données des logiciels installés collectées en utilisant des processus standard d'inventaire matériel de client Configuration Manager, certaines données de

logiciels peuvent ne pas être collectées correctement. Par exemple, les installations logicielles non conformes aux processus d'installation standard ou modifiées avant l'installation peuvent générer des rapports Asset Intelligence inexacts.

#### Limitations légales

Les informations affichées dans les rapports Asset Intelligence sont soumises à de nombreuses limitations. Ces informations ne représentent pas un avis juridique, comptable ou professionnel. Les informations fournies par les rapports Asset Intelligence sont données à titre indicatif et ne doivent pas être utilisées dans le seul but de déterminer la conformité des licences d'utilisation de logiciels.

Les exemples de limitations suivants sont impliqués dans le processus d'inventaire des logiciels installés et des licences utilisant Asset Intelligence dans l'entreprise et susceptibles d'affecter la précision des rapports Asset Intelligence :

**Limitations quantitatives de l'utilisation des licences Microsoft**

- La quantité de licences logicielles Microsoft achetées est déterminée à partir des informations fournies par les administrateurs et elle doit être examinée en détail afin de garantir que le nombre correct de licences d'utilisation de logiciels est indiqué.
- La quantité indiquée de licences logicielles Microsoft révèle des informations qui ne concernent que les licences logicielles Microsoft achetées via les programmes de licences en volume et ne reflète pas d'informations relatives aux licences logicielles acquises auprès d'un revendeur, d'un fabricant d'ordinateurs OEM ou d'un autre point de vente de licences d'utilisation de logiciels.
- Les licences logicielles acquises au cours des 45 derniers jours peuvent ne pas figurer dans la liste des licences logicielles Microsoft fournie, selon les besoins et calendriers des rapports du revendeur de logiciels.
- Les transferts de licences logicielles résultant des fusions ou rachats d'entreprises, peuvent ne pas être inclus dans le nombre de licences logicielles Microsoft.
- Les conditions non standard d'un contrat de licences en volume Microsoft (MVLS) peuvent affecter le nombre de licences logicielles indiqué, et ainsi nécessiter une analyse supplémentaire par un représentant Microsoft.

  **Limitations quantitatives des logiciels installés**
  Les clients Configuration Manager doivent terminer correctement les cycles de diffusion d'inventaire matériel pour que les rapports Asset Intelligence reflètent précisément la quantité de logiciels installés. En outre, il peut y avoir un décalage entre l'installation ou la désinstallation d'un logiciel sous licence après un cycle de diffusion d'inventaire matériel réussi. Ce décalage ne sera pas indiqué dans les rapports Asset Intelligence avant le prochain cycle de diffusion d'inventaire matériel.

  **Limitations relatives au rapprochement des licences**
  Le rapprochement entre le nombre de logiciels installés et le nombre de licences logicielles achetées est calculé en comparant le nombre de licences spécifié par l'administrateur et le nombre de logiciels installés collectés lors des inventaires matériels du client Configuration Manager en fonction du calendrier défini par l'administrateur. Cette comparaison ne constitue pas l'avis final de Microsoft concernant les licences. L'avis concernant les licences dépend en réalité de chaque nom de licence d'utilisation de logiciel et des droits d'utilisation accordés par le contrat de licence.

## États de validation Asset Intelligence

Les états de validation Asset Intelligence représentent les états de validation actuels sources des informations du catalogue Asset Intelligence. Le tableau suivant présente les états de validation possibles d'Asset Intelligence et les actions de l'administrateur susceptibles de les déclencher.

| ÉTAT | DÉFINITION | ACTION DE L'ADMINISTRATEUR | COMMENTAIREAIRE |
|---|---|---|---|
| **Validé** | L'élément du catalogue a été défini par les fonctions de recherche de System Center Online. | aucune. | Meilleur état. |
| **Défini par l'utilisateur** | L'élément du catalogue n'a pas été défini par les fonctions de recherche de System Center Online. | Personnaliser les informations du catalogue en local. | Cet état est affiché dans les rapports Asset Intelligence. |
| **En attente** | L'élément du catalogue n'a pas été défini par les fonctions de recherche de System Center Online, mais il a été soumis à System Center Online en vue d'une catégorisation. | Demander la catégorisation depuis System Center Online. | L'élément du catalogue conserve cet état jusqu'à ce que les fonctions de recherche de System Center Online classe l'élément dans une catégorie et le catalogue Asset Intelligence est synchronisé. |
| **Peut être mis à jour** | Un élément du catalogue défini par un utilisateur a été catégorisé différemment par System Center Online lors de la synchronisation de catalogue suivante. | Personnaliser le catalogue Asset Intelligence local afin de classer un élément comme étant défini par un utilisateur. | Vous pouvez exécuter l'action Résoudre le conflit pour décider si vous allez utiliser les nouvelles informations de catégorisation ou la précédente valeur définie par l'utilisateur. Pour plus d'informations sur la résolution des conflits, consultez Opérations pour Asset Intelligence dans System Center Configuration Manager. |
| **Sans catégorie** | L'élément du catalogue n'a pas été défini par les fonctions de recherche de System Center Online, il n'a pas été soumis à System Center Online pour la catégorisation et l'administrateur n'a pas attribué une valeur de catégorisation définie par l'utilisateur. | aucune. | Nécessite une catégorisation ou la personnalisation des informations du catalogue local.<br><br>Pour plus d'informations sur la demande de catégorisation, consultez Opérations pour Asset Intelligence dans System Center Configuration Manager.<br><br>Pour plus d'informations sur la modification de la catégorie du logiciel, consultez Opérations pour Asset Intelligence dans System Center Configuration Manager. |

**NOTE**

L'état de validation des éléments de catalogue soumis à System Center Online à des fins de catégorisation est **En attente** sur un site d'administration centrale mais sur les sites principaux enfant, l'état de validation affiché pour ces éléments continue d'être **Sans catégorie** .

**NOTE**

À l'issue de la résolution d'un conflit de catégorisation, l'élément n'est plus validé comme étant un élément en conflit sauf si des mises à jour de catégorisation ultérieures apportent de nouvelles informations sur cet élément.

Pour obtenir des exemples du moment où un état de validation peut passer à un autre état, consultez Exemples de transitions d'état de validation pour Asset Intelligence dans System Center Configuration Manager.

# Conditions préalables pour Asset Intelligence dans System Center Configuration Manager

22/06/2018 • 7 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Dans System Center Configuration Manager, Asset Intelligence est soumis à des dépendances externes et à des dépendances au sein du produit.

## Dépendances externes à Configuration Manager

Le tableau suivant présente les dépendances d'Asset Intelligence qui sont externes à Configuration Manager.

| DÉPENDANCE | INFORMATIONS COMPLÉMENTAIRES |
|---|---|
| Audit des conditions requises pour les événements d'ouverture de session réussis | Quatre rapports Asset Intelligence affichent des informations extraites des journaux d'événements de sécurité Windows sur les ordinateurs client. Si les paramètres du journal des événements de sécurité ne sont pas configurés pour consigner tous les événements de connexion réussie, ces rapports ne contiennent aucune donnée, même si la classe de rapport d'inventaire matériel appropriée est activée.<br><br>Les rapports Asset Intelligence suivants dépendent des informations du journal des événements de sécurité Windows :<br><br>- Matériel 03A - Utilisateurs d'ordinateurs principaux<br>- Matériel 03B - Ordinateurs d'un utilisateur de console principal spécifique<br>- Matériel 04A - Ordinateur partagé (multi-utilisateur)<br>- Matériel 05A - Utilisateurs de console sur un ordinateur spécifique<br><br>Pour activer l'agent du client d'inventaire matériel en vue de répertorier les informations requises par ces rapports, vous devez d'abord modifier les paramètres du journal des événements de sécurité Windows sur les clients afin de consigner tous les événements de connexion réussie et activer la classe de rapport d'inventaire matériel **SMS_SystemConsoleUser** . Pour plus d'informations sur la modification des paramètres du journal des événements de sécurité afin de consigner tous les événements de connexion réussie, consultez Activer l'audit des événements de connexion réussie. |

**NOTE**

La classe de rapport d'inventaire matériel **SMS_SystemConsoleUser** conserve uniquement les données d'événement de connexion réussie enregistrées au cours des 90 derniers jours dans le journal des événements de sécurité, sans tenir compte de la longueur du journal. Si les données contenues dans le journal des événements de sécurité datent de moins de 90 jours, le journal est lu en intégralité.

## Dépendances internes à Configuration Manager

Le tableau suivant présente les dépendances d'Asset Intelligence qui sont internes à Configuration Manager.

| DÉPENDANCE | INFORMATIONS COMPLÉMENTAIRES |
|---|---|
| Conditions requises pour l'agent du client | Les rapports Asset Intelligence dépendent des informations du client obtenues par l'intermédiaire des rapports d'inventaires logiciels et matériels. Pour obtenir les informations nécessaires à tous les rapports Asset Intelligence, vous devez activer les agents clients suivants :<br><br>- Agent du client d'inventaire matériel<br>- Agent du client de contrôle des logiciels |
| Dépendances de l'agent du client d'inventaire matériel | Pour collecter les données d'inventaire requises par certains rapports Asset Intelligence, vous devez activer l'agent du client d'inventaire matériel. En outre, certaines classes de rapport d'inventaire matériel dont dépendent les rapports Asset Intelligence doivent être activées sur les ordinateurs du serveur de site principal.<br><br>Pour plus d'informations sur l'activation de l'agent du client d'inventaire matériel, consultez Comment étendre l'inventaire matériel dans System Center Configuration Manager. |
| Dépendances de l'agent du client de contrôle des logiciels | Un grand nombre de rapports Asset Intelligence sur les logiciels dépendent des données de l'agent du client de contrôle des logiciels. Pour plus d'informations sur l'activation de l'agent du client d'inventaire matériel, consultez Surveiller l'utilisation des applications avec le contrôle de logiciel dans System Center Configuration Manager.<br><br>Les rapports Asset Intelligence suivants dépendent des données de l'agent du client de contrôle des logiciels :<br><br>- Logiciel 07A - Fichiers exécutables récemment utilisés par le nombre d'ordinateurs<br>- Logiciel 07B - Ordinateurs ayant récemment utilisé un fichier exécutable spécifié<br>- Logiciel 07C - Fichiers exécutables récemment utilisés sur un ordinateur spécifique<br>- Logiciel 08A - Fichiers exécutables récemment utilisés par le nombre d'utilisateurs<br>- Logiciel 08B - Utilisateurs ayant récemment utilisé un fichier exécutable spécifié<br>- Logiciel 08C - Fichiers exécutables récemment utilisés par un utilisateur spécifié |

| DÉPENDANCE | INFORMATIONS COMPLÉMENTAIRES |
| --- | --- |
| Conditions requises pour la classe de rapports d'inventaire matériel Asset Intelligence | Dans Configuration Manager, les rapports Asset Intelligence dépendent de classes de rapports d'inventaire matériel spécifiques. Les rapports Asset Intelligence associés ne contiennent aucune donnée tant que les classes de rapport d'inventaire matériel ne sont pas activées et que les clients n'ont pas signalé d'inventaire matériel sur ces classes. Vous pouvez activer les classes de rapport d'inventaire matériel suivantes pour prendre en charge les obligations de rapport Asset Intelligence :<br><br>- SMS_SystemConsoleUsage[1]<br>- SMS_SystemConsoleUser[1]<br>- SMS_InstalledSoftware<br>- SMS_AutoStartSoftware<br>- SMS_BrowserHelperObject<br>- Win32_USBDevice<br>- SMS_InstalledExecutable<br>- SMS_SoftwareShortcut<br>- SoftwareLicensingService<br>- SoftwareLicensingProduct<br>- SMS_SoftwareTag<br><br>[1] Par défaut, les classes de rapport d'inventaire matériel Asset Intelligence **SMS_SystemConsoleUsage** et **SMS_SystemConsoleUser** sont activées.<br><br>Vous pouvez modifier les classes de rapport d'inventaire matériel Asset Intelligence dans la console Configuration Manager, dans l'espace de travail **Ressources et conformité**, quand vous cliquez sur le nœud **Asset Intelligence**. Pour plus d'informations, consultez la section Activer les classes de création de rapports d'inventaire matériel Asset Intelligence dans la rubrique Configuration d'Asset Intelligence dans Configuration Manager. |
| Point de Reporting Services | Le rôle de système de site du point de Reporting Services doit être installé avant que vous puissiez afficher les rapports des mises à jour logicielles. Pour plus d'informations sur la création d'un point de Reporting Services, consultez Configuration des rapports dans Configuration Manager. |

# Configurer Asset Intelligence dans System Center Configuration Manager

22/06/2018 • 26 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Asset Intelligence permet d'inventorier et de gérer l'utilisation des licences logicielles.

## Étapes de configuration d'Asset Intelligence

- **Étape 1** : Pour collecter les données d'inventaire pour les rapports Asset Intelligence, vous devez activer l'agent d'inventaire matériel, comme cela est expliqué dans Comment étendre l'inventaire matériel dans System Center Configuration Manager.
- **Étape 2** : Activer les classes de création de rapports d'inventaire matériel Asset Intelligence.
- **Étape 3** : Installer un point de synchronisation Asset Intelligence
- **Étape 4** : Activer l'audit des événements de connexion réussie
- **Étape 5** : Importer les informations de licence logicielle
- **Étape 6** : Configurer les tâches de maintenance Asset Intelligence

### Activer les classes de création de rapports d'inventaire matériel Asset Intelligence

Pour activer Asset Intelligence sur les sites Configuration Manager, vous devez activer au moins une des classes de création de rapports d'inventaire matériel Asset Intelligence. Vous pouvez activer les classes sur la page d'accueil **Asset Intelligence** ou, dans l'espace de travail **Administration** , dans le nœud **Paramètres client** , dans les propriétés des paramètres client. Procédez selon l'une des méthodes suivantes :

#### Pour activer les classes de création de rapports d'inventaire matériel Asset Intelligence depuis la page d'accueil Asset Intelligence

1. Dans la console Configuration Manager, choisissez **Ressources et Conformité** > **Asset Intelligence**.
2. Sous l'onglet **Accueil**, dans le groupe **Asset Intelligence**, choisissez **Modifier les classes d'inventaire**.
3. Pour activer la création de rapports Asset Intelligence, sélectionnez **Activer toutes les classes de création de rapports Asset Intelligence** ou **Activer uniquement les classes de création de rapports Asset Intelligence sélectionnées**, puis sélectionnez au moins une classe de création de rapports dans les classes affichées.

> **NOTE**
> Les rapports Asset Intelligence qui dépendent des classes d'inventaire matériel que vous activez en utilisant cette procédure n'affichent pas de données tant que les clients n'ont pas établi et retourné un inventaire matériel.

#### Pour activer les classes de création de rapports d'inventaire matériel Asset Intelligence depuis les propriétés des paramètres client

1. Dans la console Configuration Manager, choisissez **Administration** > **Paramètres client** > **Paramètres d'agent client par défaut**. Si vous avez créé des paramètres client personnalisés, vous pouvez sélectionner ces paramètres à la place.
2. Sous l'onglet **Accueil** > groupe **Propriétés**, choisissez **Propriétés**.
3. Choisissez **Inventaire matériel** > **Déf. classes**. .
4. Choisissez **Filtrer par catégorie** > **Classes de création de rapports Asset Intelligence**. La liste des

classes est actualisée avec uniquement les classes de création de rapports d'inventaire matériel Asset intelligence.

5. Sélectionnez au moins une classe de création de rapports dans la liste.

> **NOTE**
> Les rapports Asset Intelligence qui dépendent des classes d'inventaire matériel que vous activez en utilisant cette procédure n'affichent pas de données tant que les clients n'ont pas établi et retourné un inventaire matériel.

**Installer un point de synchronisation Asset Intelligence**

Le rôle de système de site du point de synchronisation Asset Intelligence permet de connecter des sites Configuration Manager à System Center Online pour synchroniser les informations du catalogue Asset Intelligence. Le point de synchronisation Asset Intelligence peut uniquement être installé sur un système de site de niveau supérieur dans la hiérarchie Configuration Manager. De plus, il a besoin d'un accès Internet pour se synchroniser avec System Center Online via le port TCP 443.

Outre le téléchargement des nouvelles informations du catalogue Asset Intelligence, le point de synchronisation Asset Intelligence peut envoyer les informations de titres de logiciels personnalisés à System Center Online à des fins de catégorisation. Microsoft considère tous les titres de logiciels téléchargés comme des informations publiques. Assurez-vous que vos titres de logiciels personnalisés ne contiennent pas d'informations confidentielles ou propriétaires. Pour plus d'informations sur la demande de catégorisation des titres de logiciels, consultez Demander une mise à jour du catalogue pour les logiciels sans catégorie.

Pour installer un rôle de système de site de point de synchronisation Asset Intelligence

1. Dans la console Configuration Manager, choisissez **Administration** > **Configuration du site** > **Serveurs et rôles de système de site**.

2. Ajoutez le rôle de système de site du point de synchronisation Asset Intelligence à un serveur de système de site nouveau ou existant :

   - Pour un **nouveau serveur de système de site** : sous l'onglet **Accueil**, dans le groupe **Créer**, choisissez **Créer un serveur de système de site** pour démarrer l'Assistant.

     > **NOTE**
     > Par défaut, quand Configuration Manager installe un rôle système de site, les fichiers d'installation sont installés sur le premier disque dur formaté NTFS disponible qui a le plus d'espace disque libre. Pour empêcher Configuration Manager d'effectuer l'installation sur des disques particuliers, créez un fichier vide « No_sms_on_drive.sms » et copiez-le dans le dossier racine du disque avant d'installer le serveur de système de site.

   - Pour un **serveur de système de site existant** : choisissez le serveur sur lequel vous souhaitez installer le rôle de système de site du point de synchronisation Asset Intelligence. Quand vous choisissez un serveur, la liste des rôles de système de site déjà installés sur le serveur s'affiche dans le volet Détails.

     Sous l'onglet **Accueil**, dans le groupe **Serveur**, choisissez **Ajouter des rôles de système de site** pour démarrer l'Assistant.

3. Renseignez la page **Général**. Lorsque vous ajoutez le point de synchronisation Asset Intelligence à un serveur de système de site existant, vérifiez les valeurs qui ont été précédemment configurées.

4. Dans la page **Sélection du rôle système**, sélectionnez **Point de synchronisation Asset Intelligence** dans la liste des rôles disponibles.

5. Dans la page des **paramètres de connexion du point de synchronisation Asset Intelligence**, choisissez **Suivant**.

   Par défaut, le paramètre **Utiliser ce point de synchronisation Asset Intelligence** est sélectionné et ne peut pas être configuré sur cette page. Comme System Center Online accepte le trafic réseau uniquement sur le port TCP 443, le paramètre de **numéro de port SSL** ne peut pas être défini dans cette page de l'Assistant.

6. Éventuellement, spécifiez le chemin du fichier de certificat d'authentification (.pfx) System Center Online. En règle générale, vous ne spécifiez pas un chemin d'accès pour le certificat, car le certificat de connexion est préparé automatiquement pendant l'installation du rôle de site.

7. Dans la page **Paramètres du serveur proxy**, indiquez si le point de synchronisation Asset Intelligence doit utiliser un serveur proxy lors de la connexion à System Center Online pour synchroniser le catalogue et si des données d'identification sont nécessaires pour se connecter au serveur proxy.

   > **WARNING**
   > Si un serveur proxy est nécessaire pour la connexion à System Center Online, le certificat de connexion peut être également supprimé si le mot de passe du compte d'utilisateur expire pour le compte défini pour l'authentification du serveur proxy.

8. Sur la page **Calendrier des synchronisations** , indiquez si vous souhaitez synchroniser le catalogue Asset Intelligence dans un calendrier. Lorsque vous activez le calendrier des synchronisations, vous pouvez définir un calendrier de synchronisation simple ou personnalisé. Pendant la synchronisation planifiée, le point de synchronisation Asset Intelligence se connecte à System Center Online pour récupérer le dernier catalogue Asset Intelligence. Vous pouvez synchroniser manuellement le catalogue Asset Intelligence depuis le nœud Asset Intelligence dans la console Configuration Manager. Pour savoir comment synchroniser manuellement le catalogue Asset Intelligence, consultez la section Pour synchroniser manuellement le catalogue Asset Intelligence dans la rubrique Opérations pour Asset Intelligence dans System Center Configuration Manager.

9. Effectuer toutes les étapes de l'Assistant

**Activer l'audit des événements de connexion réussie**

Quatre rapports Asset Intelligence affichent des informations extraites des journaux d'événements de sécurité Windows sur les ordinateurs client. Voici comment configurer les paramètres d'ouverture de session de la stratégie de sécurité des ordinateurs pour activer l'audit des événements associés aux ouvertures de session qui aboutissent.

##### Pour activer la journalisation des événements associés aux ouvertures de session qui aboutissent en utilisant une stratégie de sécurité locale

1. Sur un ordinateur client Configuration Manager, choisissez **Démarrer** > **Outils d'administration** > **Stratégie de sécurité locale**.

2. Dans la boîte de dialogue **Stratégie de sécurité locale**, sous **Paramètres de sécurité**, développez **Stratégies locales**, puis choisissez **Stratégie d'audit**.

3. Dans le volet des résultats, double-cliquez sur **Auditer les événements de connexion**, cochez la case **Succès** et choisissez **OK**.

##### Pour activer la journalisation des événements d'ouverture de session qui aboutissent en utilisant une stratégie de sécurité du domaine Active Directory

1. Sur un ordinateur contrôleur de domaine, choisissez **Démarrer**, pointez sur **Outils d'administration**, puis choisissez **Stratégie de sécurité du domaine**.

2. Dans la boîte de dialogue **Stratégie de sécurité locale**, sous **Paramètres de sécurité**, développez **Stratégies locales**, puis choisissez **Stratégie d'audit**.

3. Dans le volet des résultats, double-cliquez sur **Auditer les événements de connexion**, cochez la case **Succès** et choisissez **OK**.

### Importer les informations de licence logicielle

Les sections suivantes décrivent les procédures permettant d'importer des informations de licences logicielles Microsoft et générales dans la base de données de site Configuration Manager en utilisant l'Assistant Importer des licences logicielles. Lorsque vous importez des informations de licence de logiciel vers la base de données de site depuis des fichiers de déclaration de licence, le compte de l'ordinateur serveur de site doit disposer des autorisations **Contrôle intégral** pour le système de fichiers NTFS du partage de fichiers utilisé pour importer les informations de licence de logiciel.

> **IMPORTANT**
> Les informations de licence logicielle importées dans la base de données de site remplacent les informations existantes. Vérifiez que le fichier d'informations de licence logicielle que vous utilisez avec Assistant Importer des licences logicielles contient la liste complète des informations de licence logicielle nécessaires.

#### Pour importer des informations de licence logicielle vers le catalogue Asset Intelligence

1. Dans l'espace de travail **Ressources et Conformité**, choisissez **Asset Intelligence**.
2. Sous l'onglet **Accueil**, dans le groupe **Asset Intelligence**, choisissez **Importer des licences logicielles**.
3. Sur la page **Importer** , spécifiez si vous importez un fichier MVLS (Microsoft Volume Licensing) (.xml ou .csv) ou un fichier de déclaration de licence générale (.csv). Pour plus d'informations sur la création d'un fichier de déclaration de licence générale, voir Create a general license statement information file for import plus loin dans cette rubrique.

   > **WARNING**
   > Pour télécharger un fichier MVLS de format .csv que vous pouvez importer vers le catalogue Asset Intelligence, consultez Centre de gestion des licences en volume Microsoft. Pour accéder à ces informations, vous devez disposer d'un compte enregistré sur le site Web. Vous devez contacter votre responsable de compte Microsoft pour plus d'informations sur la façon d'obtenir votre fichier MVLS de format .xml.

4. Entrez le chemin d'accès UNC du fichier de déclaration de licence ou choisissez **Parcourir** pour sélectionner un dossier réseau partagé et un fichier.

   > **NOTE**
   > Le dossier partagé doit être correctement sécurisé pour empêcher tout accès non autorisé au fichier d'informations de licence. En outre, le compte de l'ordinateur sur lequel l'Assistant est exécuté doit avoir les autorisations de contrôle intégral sur le partage contenant le fichier d'importation de licence.

5. Effectuez toutes les étapes de l'Assistant.

### Create a general license statement information file for import

Une déclaration de licence générale peut également être importée vers le catalogue Asset Intelligence en utilisant un fichier d'importation de licence de format .csv (délimité par des virgules) créé manuellement.

> **NOTE**
>
> Seuls les champs **Nom**, **Éditeur**, **Version**et **Quantité effective** sont requis, mais ils doivent tous être entrés sur la première ligne du fichier d'importation de licence. Tous les champs de date doivent être affichés dans le format suivant : mois/jour/année, par exemple, 08/04/2008.

Asset Intelligence fait correspondre les produits que vous spécifiez dans la déclaration de licence générale en utilisant le nom du produit et la version du produit, mais pas le nom de l'éditeur. Vous devez utiliser un nom de produit dans la déclaration de licence générale qui correspond exactement au nom de produit stocké dans la base de données du site. Asset Intelligence utilise le nombre **Quantité effective** donné dans la déclaration de licence générale et le compare au nombre de produits installés trouvés dans l'inventaire Configuration Manager.

> **TIP**
>
> Pour obtenir la liste complète des noms de produits stockés dans la base de données du site Configuration Manager, exécutez la requête suivante sur la base de données du site : SELECT ProductName0 FROM v_GS_INSTALLED_SOFTWARE.

Vous pouvez spécifier les versions exactes pour un produit ou spécifier une partie de la version, comme par exemple uniquement la version principale. Les exemples suivants présentent les correspondances de version obtenues pour une entrée de version de déclaration générale de licence pour un produit spécifique.

| ENTRÉE DE DÉCLARATION DE LICENCE GÉNÉRALE | CORRESPONDANCE AVEC LES ENTRÉES DE LA BASE DE DONNÉES DE SITE |
|---|---|
| Name: "MySoftware", ProductVersion0:"2" | ProductName0: "Mysoftware", ProductVersion0: "2.01.1234"<br><br>ProductName0: "MySoftware", ProductVersion0: "2.02.5678"<br><br>ProductName0: "MySoftware", ProductVersion0: "2.05.1234"<br><br>ProductName0: "MySoftware", ProductVersion0: "2.05.5678"<br><br>ProductName0: "MySoftware", ProductVersion0: "2.05.3579.000"<br><br>ProductName0: "MySoftware", ProductVersion0: "2.10.1234" |
| Name: "MySoftware", Version "2.05" | ProductName0: "MySoftware", ProductVersion0: "2.05.1234"<br><br>ProductName0: "MySoftware", ProductVersion0: "2.05.5678"<br><br>ProductName0: "MySoftware", ProductVersion0: "2.05.3579.000" |
| Name: "Mysoftware", Version "2"<br><br>Name: "Mysoftware", Version "2.05" | Erreur lors de l'importation. L'importation échoue lorsque plusieurs entrées correspondent à la même version du produit. |

#### Pour créer un fichier d'importation de déclaration de licence générale à l'aide de Microsoft Excel

1. Ouvrez Microsoft Excel et créez une nouvelle feuille de calcul.
2. Sur la première ligne de la nouvelle feuille de calcul, saisissez tous les noms de champs de données des licences logicielles.
3. À partir de la deuxième ligne, entrez les informations de licence logicielle requises. Assurez-vous que

tous les champs de données des licences logicielles requis sont saisis sur les lignes suivantes pour chaque licence logicielle qui doit être importée. Le nom de logiciel saisi dans la feuille de calcul doit être le même que le nom de logiciel affiché dans l'Explorateur de ressources pour un ordinateur client, après avoir exécuté l'inventaire matériel.

4. Enregistrez le fichier au format .csv.
5. Copiez le fichier .csv dans le partage de fichiers utilisé pour l'importation des informations de licence logicielle dans le catalogue Asset Intelligence.
6. Dans la console Configuration Manager, utilisez l'Assistant Importer des licences logicielles pour importer le nouveau fichier .csv.
7. Générez le **rapport de rapprochement des licences logicielles tierces (licence 15A)** d'Asset Intelligence pour vérifier que les informations de licence ont bien été importées dans le catalogue Asset Intelligence.

> **NOTE**
> Pour obtenir un exemple de fichier de licence logicielle générale que vous pouvez utiliser à des fins de test, consultez Exemple de fichier d'importation de licence générale Asset Intelligence dans System Center Configuration Manager.

**Exemple de tableau utilisé pour décrire des licences logicielles**

Lors de la création d'un fichier d'importation de déclaration de licence générale, les informations figurant dans le tableau suivant peuvent être utilisées pour décrire les licences logicielles à importer dans le catalogue Asset Intelligence.

| NOM DE LA COLONNE | TYPE DE DONNÉES | OBLIGATOIRE | EXEMPLE |
|---|---|---|---|
| Nom | Jusqu'à 255 caractères | Oui | Nom du logiciel |
| Éditeur | Jusqu'à 255 caractères | Oui | Éditeur du logiciel |
| Version | Jusqu'à 255 caractères | Oui | Version du logiciel |
| Langage | Jusqu'à 255 caractères | Oui | Langue du logiciel |
| Quantité effective | Valeur entière | Oui | Nombre de licences achetées |
| Numéro BC | Jusqu'à 255 caractères | Non | Informations sur les BC |
| Nom du revendeur | Jusqu'à 255 caractères | Non | Informations sur le revendeur |
| Date d'achat | Date au format suivant : MM/JJ/AAAA | Non | Date d'achat de la licence |
| Achat de la prise en charge | Valeur en bits | Non | 0 ou 1 (0 pour Oui, 1 pour Non) |
| Date d'expiration de la prise en charge | Date au format suivant : MM/JJ/AAAA | Non | Date de fin de la prise en charge achetée |
| Commentaires | Jusqu'à 255 caractères | Non | Commentaires facultatifs |

### Configurer les tâches de maintenance Asset Intelligence

Les tâches de maintenance suivantes sont disponibles pour Asset Intelligence :

- **Vérifier le titre de l'application à l'aide des informations d'inventaire** : vérifie si le nom du logiciel indiqué dans l'inventaire logiciel correspond au nom du logiciel figurant dans le catalogue Asset Intelligence. Par défaut, cette tâche est activée et planifiée pour être exécutée le samedi entre 00 h 00 et 5 h 00. Cette tâche de maintenance est uniquement disponible sur le site de niveau supérieur de la hiérarchie Configuration Manager.
- **Résumer les données du logiciel installé** : fournit les informations affichées dans l'espace de travail **Ressources et Conformité**, dans le nœud **Logiciels inventoriés**, sous le nœud **Asset Intelligence**. Quand la tâche s'exécute, Configuration Manager compte les titres de logiciels inventoriés sur le site principal. Par défaut, cette tâche est activée et planifiée pour être exécutée tous les jours entre 00 h 00 et 5 h 00. Cette tâche de maintenance est disponible uniquement sur les sites principaux.

#### Pour configurer les tâches de maintenance Asset Intelligence

1. Dans la console Configuration Manager, choisissez **Administration** > **Configuration du site** > **Sites**.
2. Sélectionnez le site sur lequel vous allez configurer la tâche de maintenance Asset Intelligence.
3. Sous l'onglet **Accueil**, dans le groupe **Paramètres**, choisissez **Maintenance de site**. Sélectionnez une tâche, puis choisissez **Modifier** pour modifier les paramètres.

   Nous vous recommandons de définir la période aux heures creuses d'utilisation du site. La période représente l'intervalle de temps au cours duquel la tâche peut être exécutée. Elle est définie par les paramètres **Démarrer après** et **Heure de début au plus tard** spécifiés dans la boîte de dialogue **Propriétés de la tâche** .

   Vous pouvez lancer immédiatement la tâche en sélectionnant le jour actuel et en réglant la valeur **Démarrer après** quelques minutes après le moment présent.
4. Choisissez **OK** pour enregistrer vos paramètres. La tâche est désormais exécutée conformément à sa planification.

> **NOTE**
> Si l'exécution d'une tâche échoue à la première tentative, Configuration Manager retente de l'exécuter jusqu'à la réussite de l'opération ou l'expiration de la période d'exécution planifiée.

# Guide pratique pour utiliser Asset Intelligence dans System Center Configuration Manager

22/06/2018 • 34 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cette rubrique contient des informations destinées à vous aider à gérer les tâches courantes Asset Intelligence dans votre hiérarchie System Center Configuration Manager :

## Afficher les informations Asset Intelligence

Vous pouvez afficher les informations Asset Intelligence sur la page d'accueil **Asset Intelligence** et dans les rapports Asset Intelligence.

### Page d'accueil d'Asset Intelligence

La page d'accueil d' **Asset Intelligence** contient un tableau de bord récapitulant les informations du catalogue Asset Intelligence. Sur la page d'accueil, vous pouvez visualiser des informations sur la synchronisation du catalogue et l'état des logiciels inventoriés. La page d'accueil d' **Asset Intelligence** comporte les sections suivantes :

- **Synchronisation de catalogue**: indique si Asset Intelligence est activé, l'état du point de synchronisation Asset Intelligence, la planification de la synchronisation, si la déclaration de licence du client est importée, la date/heure de la dernière mise à jour de l'état et de la prochaine mise à jour planifiée et le nombre de modifications effectuées après l'installation du système de site du point de synchronisation Asset Intelligence.

  > **NOTE**
  > La section de synchronisation du catalogue Asset Intelligence de la page d'accueil **Asset Intelligence** s'affiche uniquement si un rôle de système de site du point de synchronisation Asset Intelligence a été installé.

- **État des logiciels inventoriés**: indique le nombre et le pourcentage de logiciels, catégories de logiciels et familles de logiciels inventoriés qui sont identifiés par Microsoft, identifiés par un utilisateur administratif, en attente d'identification en ligne ou non identifiés et pas en attente. Les informations affichées dans un tableau indiquent le nombre pour chacun des éléments, tandis que les informations affichées dans le graphique indiquent le pourcentage de chacun des éléments.

  Utilisez la procédure suivante pour afficher les informations Asset Intelligence sur la page d'accueil **Asset Intelligence** .

#### Pour afficher les informations Asset Intelligence sur la page d'accueil Asset Intelligence

1. Dans la console Configuration Manager, cliquez sur **Ressources et Conformité**.
2. Dans l'espace de travail **Biens et conformité** , cliquez sur **Asset Intelligence**. Les rapports Asset Intelligence s'affichent.

### Rapports Asset Intelligence

Il existe plus de 60 rapports Asset Intelligence qui affichent les informations collectées par Asset Intelligence. La plupart de ces rapports renvoient vers des rapports plus spécifiques qui permettent de rechercher des informations générales et d'accéder à des informations plus détaillées. Les rapports Asset Intelligence se trouvent dans la console Configuration Manager, dans l'espace de travail **Surveillance**, sous le nœud **Rapports**.

Les rapports fournissent des informations sur les matériels, la gestion des licences et les logiciels. Pour plus d'informations sur les rapports Configuration Manager, consultez Génération de rapports dans System Center Configuration Manager.

> **NOTE**
> L'exactitude des nombres de titres de logiciels et des informations de licence affichés dans les rapports Asset Intelligence peut varier par rapport au nombre réel de titres de logiciels installés ou de licences utilisées dans l'environnement. Ceci est dû aux dépendances complexes et aux limitations propres à l'inventaire des informations de licences logicielles pour les titres de logiciels installés dans les environnements d'entreprise. N'utilisez pas uniquement Asset Intelligence pour déterminer la conformité des licences logicielles achetées.

Utilisez la procédure suivante pour afficher les informations Asset Intelligence en utilisant les rapports Asset Intelligence.

#### Pour afficher les informations Asset Intelligence collectées en utilisant les rapports Asset Intelligence

1. Dans la console Configuration Manager, cliquez sur **Surveillance**.
2. Dans l'espace de travail **Surveillance** , développez **Rapports**et **Rapports**, puis cliquez sur **Asset Intelligence**. Les rapports Asset Intelligence s'affichent.

   > **WARNING**
   > Si aucun dossier de rapport n'existe sous le noeud **Rapports** , vérifiez que vous avez configuré la création de rapports. Pour plus d'informations, consultez Configuration de la génération de rapports dans System Center Configuration Manager.

3. Sélectionnez le rapport Asset Intelligence à exécuter, puis dans l'onglet **Accueil** , dans le groupe **Groupe de rapports** , cliquez sur **Exécuter**.

## Synchroniser le catalogue Asset Intelligence

Vous pouvez synchroniser le catalogue local Asset Intelligence avec System Center Online pour récupérer la dernière catégorisation de titres de logiciels. Quand vous demandez manuellement la synchronisation du catalogue avec System Center Online, l'achèvement du processus de synchronisation avec System Center Online peut prendre 15 minutes ou plus. Configuration Manager met à jour le paramètre **Dernière mise à jour réussie** dans la page d'accueil d'**Asset Intelligence** avec l'heure à laquelle la synchronisation se termine.

> **NOTE**
> Pour pouvoir utiliser les procédures, vous devez installer préalablement un rôle de système de site de point de synchronisation Asset Intelligence. Pour plus d'informations sur l'installation d'un point de synchronisation Asset Intelligence, consultez Configuration d'Asset Intelligence dans System Center Configuration Manager.

Utilisez la procédure suivante pour créer une planification de synchronisation pour le catalogue Asset Intelligence.

#### Pour créer une planification de synchronisation pour le catalogue Asset Intelligence

1. Dans la console Configuration Manager, cliquez sur **Ressources et Conformité**.
2. Dans l'espace de travail **Biens et conformité** , cliquez sur **Asset Intelligence**.
3. Sur l'onglet **Accueil** , dans le groupe **Créer** , cliquez sur **Synchroniser**, puis sur **Planifier la synchronisation**.

4. Dans la boîte de dialogue **Planification de point de synchronisation Asset Intelligence** , sélectionnez **Activer la synchronisation dans un calendrier**, puis définissez une planification simple ou personnalisée.

5. Cliquez sur **OK** pour enregistrer les modifications.

> **NOTE**
> Pour plus d'informations sur la planification de la synchronisation, y compris la prochaine synchronisation planifiée, consultez le nœud **Asset Intelligence** dans l'espace de travail **Ressources et Conformité** sur le site de niveau supérieur de la hiérarchie.

Utilisez la procédure suivante pour synchroniser manuellement le catalogue Asset Intelligence.

> **WARNING**
> System Center Online n'accepte qu'une seule demande de synchronisation manuelle sur une période de 12 heures.

**Pour synchroniser manuellement le catalogue Asset Intelligence**

1. Dans la console Configuration Manager, cliquez sur **Ressources et Conformité**.

2. Dans l'espace de travail **Biens et conformité** , cliquez sur **Asset Intelligence**.

3. Sur l'onglet **Accueil** , dans le groupe **Créer** , cliquez successivement sur **Synchroniser**, **Synchroniser le catalogue Asset Intelligence**et **OK**.

# Personnaliser le catalogue Asset Intelligence

Les informations de catégorisation du catalogue Asset Intelligence envoyées par System Center Online sont stockées en lecture seule dans la base de données de site et elles ne peuvent donc pas être modifiées, ni supprimées. Toutefois, vous pouvez créer, modifier et supprimer des catégories de logiciels, des familles de logiciels, des légendes logicielles et des informations de configuration matérielle personnalisées dans le catalogue. Ensuite, vous pouvez utiliser les informations de catégorisation personnalisées à la place des informations fournies par System Center Online pour les informations de titres de logiciels définies par l'utilisateur ou existantes. Lorsque vous modifiez ou ajoutez des informations de catégorisation, les informations du catalogue sont considérées avoir été définies par l'utilisateur. Les informations de catégorisation définies par l'utilisateur ne sont pas stockées dans les mêmes tables de base de données que les informations validées du catalogue.

### Catégories de logiciels

Les catégories de logiciels Asset Intelligence sont utilisées pour catégoriser de façon large les titres de logiciels inventoriés et pour les regroupements généraux de familles de logiciels plus spécifiques. Par exemple, « Société d'énergie » peut correspondre à une catégorie de logiciels, et « Pétrole », « Gaz » ou « Hydroélectrique » peuvent correspondre à des familles de logiciels dans cette catégorie. La plupart des catégories de logiciels sont prédéfinies dans le catalogue Asset Intelligence et des catégories définies par l'utilisateur peuvent être créées pour définir plus précisément les logiciels inventoriés. L'état de validation de toutes les catégories de logiciels prédéfinies est toujours **Validé**, alors que les informations de catégories de logiciels personnalisées ajoutées au catalogue Asset Intelligence ont l'état **Défini par l'utilisateur**

Utilisez la procédure suivante pour créer une catégorie de logiciels définie par l'utilisateur.

**Pour créer une catégorie de logiciels définie par l'utilisateur**

1. Dans la console Configuration Manager, cliquez sur **Ressources et Conformité**.

2. Dans l'espace de travail **Biens et conformité** , cliquez sur **Asset Intelligence**, puis sur **Catalogue**.

3. Dans l'onglet **Accueil** , dans le groupe **Créer** , cliquez sur **Créer une catégorie logicielle**.
4. Sur la page **Général** , entrez le nom de la nouvelle catégorie de logiciels et, éventuellement, une description.

   > **NOTE**
   > L'état de validation de toutes les nouvelles catégories personnalisées de logiciels est toujours **Défini par l'utilisateur**.

   Cliquez sur **Suivant**.
5. Sur la page **Résumé** , vérifiez les paramètres, puis cliquez sur **Suivant**.
6. Sur la page **Dernière étape** , cliquez sur **Fermer** pour quitter l'Assistant.

### Familles de logiciels

Les familles de logiciels Asset Intelligence permettent de définir plus précisément les titres de logiciels dans les catégories de logiciels. Par exemple, « Société d'énergie » peut correspondre à une catégorie de logiciels, et « Pétrole », « Gaz » ou « Hydroélectrique » peuvent correspondre à des familles de logiciels dans cette catégorie. La plupart des familles de logiciels sont prédéfinies dans le catalogue Asset Intelligence et des familles additionnelles définies par l'utilisateur peuvent être créées pour définir les logiciels inventoriés. L'état de validation de toutes les familles de logiciels prédéfinies est toujours **Validé**, alors que les informations de familles de logiciels personnalisées ajoutées au catalogue Asset Intelligence ont l'état **Défini par l'utilisateur**

Utilisez la procédure suivante pour créer une famille de logiciels définie par l'utilisateur.

#### Pour créer une famille de logiciels définie par l'utilisateur

1. Dans la console Configuration Manager, cliquez sur **Ressources et Conformité**.
2. Dans l'espace de travail **Biens et conformité** , cliquez sur **Asset Intelligence**, puis sur **Catalogue**.
3. Dans l'onglet **Accueil** , dans le groupe **Créer** , cliquez sur **Créer une famille logicielle**.
4. Sur la page **Général** , entrez le nom de la nouvelle famille de logiciels et, éventuellement, une description.

   > **NOTE**
   > L'état de validation de toutes les nouvelles familles personnalisées de logiciels est toujours **Défini par l'utilisateur**.
5. Sur la page **Résumé** , vérifiez les paramètres, puis cliquez sur **Suivant**.
6. Sur la page **Dernière étape** , cliquez sur **Fermer** pour quitter l'Assistant.

### Légendes logicielles

Les légendes logicielles personnalisées Asset Intelligence permettent de créer des filtres que vous pouvez utiliser pour regrouper les titres de logiciels et les afficher en utilisant des rapports Asset Intelligence. Par exemple, vous pouvez créer une légende logicielle appelée « logiciel à contribution volontaire », l'associer à un certain nombre d'applications, puis exécuter un rapport pour afficher tous les titres ayant la légende logicelle « logiciel à contribution volontaire ». L'état de validation est **Défini par l'utilisateur** pour toutes les légendes logicielles personnalisées que vous ajoutez au catalogue Asset Intelligence.

Utilisez la procédure suivante pour créer une légende personnalisée définie par l'utilisateur.

#### Pour créer une légende logicielle définie par l'utilisateur

1. Dans la console Configuration Manager, cliquez sur **Ressources et Conformité**.
2. Dans l'espace de travail **Biens et conformité** , cliquez sur **Asset Intelligence**, puis sur **Catalogue**.

3. Dans l'onglet **Accueil** , dans le groupe **Créer** , cliquez sur **Créer une légende logicielle**.
4. Sur la page **Général** , entrez le nom de la nouvelle famille de logiciels et, éventuellement, une description.

> **NOTE**
> L'état de validation de toutes les nouvelles légendes logicielles personnalisées est toujours **Défini par l'utilisateur**.

5. Sur la page **Résumé** , vérifiez les paramètres, puis cliquez sur **Suivant**.
6. Sur la page **Dernière étape** , cliquez sur **Fermer** pour quitter l'Assistant.

**Configuration matérielle requise**

Les informations de configuration matérielle requise permettent de vérifier que les ordinateurs répondent à la configuration matérielle requise pour les titres de logiciels avant d'y déployer les logiciels. La plupart des configurations matérielles requises sont prédéfinies dans le catalogue Asset Intelligence et vous pouvez créer des informations de configuration matérielle définies par l'utilisateur pour répondre à des besoins spécifiques. L'état de validation de toutes les configurations matérielles requises prédéfinies est toujours **Validé**, tandis que celui des informations de configuration matérielle requise définies par l'utilisateur ajoutées au catalogue Asset Intelligence est **Défini par l'utilisateur**.

> **IMPORTANT**
> Les informations de configuration matérielle requise figurant dans la console Configuration Manager sont tirées du catalogue Asset Intelligence sur l'ordinateur local et ne reposent pas sur les informations de titres de logiciels inventoriés sur les clients System Center 2012 Configuration Manager. Les informations de configuration matérielle requise ne sont pas mises à jour au cours de la synchronisation avec System Center Online. Vous pouvez créer une configuration matérielle requise définie par l'utilisateur pour le logiciel inventorié n'ayant pas de configuration matérielle.

Utilisez la procédure suivante pour créer une configuration matérielle requise définie par l'utilisateur.

Pour créer une configuration matérielle requise définie par l'utilisateur

1. Dans la console Configuration Manager, cliquez sur **Ressources et Conformité**.
2. Dans l'espace de travail **Biens et conformité** , cliquez sur **Asset Intelligence**, puis sur **Configuration matérielle requise**.
3. Dans l'onglet **Accueil** , dans le groupe **Créer** , cliquez sur **Créer la configuration matérielle requise**.
4. Sur la page **Général** , spécifiez les informations suivantes :
   a. **Nom du logiciel**: spécifie le nom du logiciel auquel la configuration matérielle requise est associée. Le titre du logiciel ne peut pas exister déjà dans le catalogue Asset Intelligence.
   b. **État de validation**: indique l'état de validation, tel que **Défini par l'utilisateur** , de la configuration matérielle requise. Vous ne pouvez pas modifier ce paramètre.
   c. **Vitesse min. du processeur (MHz)**: spécifie la vitesse minimale du processeur, en mégahertz (MHz), nécessaire au logiciel.
   d. **Mémoire RAM minimum (Ko)**: spécifie la quantité de mémoire vive minimale en kilo-octets (Ko) nécessaire au logiciel.
   e. **Espace disque minimum (Ko)**: spécifie l'espace disque libre minimal en Ko nécessaire au logiciel.
   f. **Taille minimale du disque (Ko)**: spécifie l'espace disque libre minimal en Ko nécessaire au logiciel.

Cliquez sur **Suivant**.

5. Sur la page **Résumé** , vérifiez les paramètres, puis cliquez sur **Suivant**.
6. Sur la page **Dernière étape** , cliquez sur **Fermer** pour quitter l'Assistant.

### Modifier les informations de catégorisation des logiciels inventoriés

Le logiciel prédéfini dans le catalogue Asset Intelligence est configuré avec des informations de catégorisation spécifiques, telles que le nom du produit, le fournisseur, la catégorie du logiciel et la famille du logiciel. Lorsque les informations de catégorisation prédéfinies ne répondent pas à vos besoins, vous pouvez modifier les informations dans les propriétés du titre du logiciel. Lorsque vous modifiez les informations de catégorisation des logiciels prédéfinis, l'état de validation **Validé** des modifications de logiciels devient **Défini par l'utilisateur**.

> **IMPORTANT**
> Les informations de catégorisation peuvent être uniquement modifiées sur le site de niveau supérieur.

Utilisez la procédure suivante pour modifier les informations de catégorisation des logiciels inventoriés.

#### Pour modifier les catégorisations des titres de logiciels

1. Dans la console Configuration Manager, cliquez sur **Ressources et Conformité**.
2. Dans l'espace de travail **Biens et conformité** , cliquez sur **Asset Intelligence**, puis sur **Logiciels inventoriés**.
3. Sélectionnez le ou les titres de logiciels dont vous voulez modifier les catégorisations.
4. Dans l'onglet **Accueil** , dans le groupe **Propriétés** , cliquez sur **Propriétés**.
5. Sur l'onglet **Général** , vous pouvez modifier les informations de catégorisation suivantes :
   - **Nom du produit**: spécifie le nom du logiciel inventorié.
   - **Fournisseur**: spécifie le nom du fournisseur qui a développé le logiciel inventorié.
   - **Catégorie**: spécifie la catégorie de logiciels actuellement affectée au logiciel inventorié.
   - **Famille**: spécifie la famille de logiciels actuellement affectée au logiciel inventorié.
6. Cliquez sur **OK** pour enregistrer les modifications.

Utilisez la procédure suivante pour restaurer les informations de catégorisation d'origine d'un logiciel.

### Restaurer les paramètres d'origine des informations de catégorisation des logiciels

Configuration Manager stocke les informations de catégorisation obtenues de System Center Online dans la base de données. Les informations ne peuvent pas être supprimées. Une fois les informations modifiées, vous pouvez restaurer les informations de catégorisation System Center Online. Vous pouvez également restaurer les paramètres d'origine des logiciels inventoriés qui ne figurent pas dans le catalogue Asset Intelligence.

Utilisez la procédure suivante pour restaurer les paramètres d'origine des informations de catégorisation.

#### Pour restaurer les paramètres d'origine des informations de catégorisation

1. Dans la console Configuration Manager, cliquez sur **Ressources et Conformité**.
2. Dans l'espace de travail **Biens et conformité** , cliquez sur **Asset Intelligence**, puis sur **Logiciels inventoriés**.
3. Sélectionnez le ou les titres de logiciels dont vous voulez restaurer les paramètres d'origine. Seuls les logiciels ayant l'état **Défini par l'utilisateur** peuvent faire l'objet d'une restauration.

> **TIP**
> Cliquez sur la colonne **État** pour trier selon l'état de validation. Le tri vous permet de voir tous les logiciels en fonction de leur état de validation et de sélectionner rapidement plusieurs éléments pour rétablir les paramètres d'origine.

4. Dans l'onglet **Accueil** , dans le groupe **Produit** , cliquez sur **Restaurer**.
5. Cliquez sur **Oui** pour restaurer les informations de catégorisation d'origine du logiciel.
6. Lorsque vous restaurez les informations de catégorisation d'un logiciel qui se trouve dans le catalogue Asset Intelligence, l'état de validation passe de **Défini par l'utilisateur** à **Validé**. Lorsque vous restaurez un logiciel qui n'est pas dans le catalogue, l'état de validation passe de **Défini par l'utilisateur** à **Sans catégorie**.

## Demander une mise à jour du catalogue pour les logiciels sans catégorie

Les informations sur les noms de logiciels sans catégorie peuvent être soumises à System Center Online afin d'être examinées et catégorisées. Une fois qu'un logiciel sans catégorie est soumis et s'il existe au moins 4 demandes de catégorisation de la part de clients pour le même logiciel, les fonctions de recherche identifient, classent, puis mettent les informations de catégorisation des logiciels à la disposition de tous les clients qui utilisent le service System Center Online. Microsoft donne la priorité la plus élevée aux logiciels qui possèdent le plus de requêtes de catégorisation. Les logiciels personnalisés et les applications métier sont peu susceptibles de recevoir une catégorie, et nous vous conseillons de ne pas envoyer ces logiciels à Microsoft pour catégorisation.

Lorsque des informations sur les noms de logiciels sont soumises à System Center Online pour catégorisation, les conditions suivantes s'appliquent :

- Seules les informations de base sur les noms de logiciels sont transmises à System Center Online, et elles peuvent être vérifiées avant leur soumission.
- Aucune information de licence de logiciel n'est transmise.
- Les noms de logiciels téléchargés sont ouvertement publiés dans le catalogue de System Center Online et peuvent être téléchargés par d'autres clients.
- La source du nom du logiciel n'est pas stockée dans le catalogue de System Center Online. Toutefois, il est recommandé de ne pas soumettre à System Center Online des noms d'applications contenant des informations propriétaires ou confidentielles.

> **NOTE**
> Pour en savoir plus sur les informations de confidentialité Asset Intelligence, consultez Sécurité et confidentialité pour Asset Intelligence dans System Center Configuration Manager.

Procédez comme suit pour demander à System Center Online la catégorisation d'un nom de logiciel du catalogue Asset Intelligence.

**Pour demander une mise à jour du catalogue pour les logiciels sans catégorie**

1. Dans la console Configuration Manager, cliquez sur **Ressources et Conformité**.
2. Dans l'espace de travail **Biens et conformité** , cliquez sur **Asset Intelligence**, puis sur **Logiciels inventoriés**.
3. Sélectionnez un ou plusieurs noms de produits à soumettre à System Center Online pour catégorisation.

Seuls les noms de logiciels inventoriés sans catégorie peuvent être soumis. Si un logiciel inventorié a été catégorisé par un administrateur, entraînant un état défini par l'utilisateur, vous devez cliquer dessus avec le bouton droit, puis cliquer sur **Restaurer** pour rétablir le logiciel dans l'état **Sans catégorie** avant qu'il puisse être soumis à System Center Online pour catégorisation.

> **NOTE**
> Configuration Manager peut traiter jusqu'à 100 titres de logiciels à la fois pour catégorisation. Si vous sélectionnez plus de 100 logiciels, seuls les 100 premiers logiciels seront traités. Vous devez sélectionner les logiciels restants pour catégorisation par lots de moins de 100.

> **TIP**
> Cliquez sur la colonne **État** pour trier selon l'état de validation. Cela vous permet de voir tous les noms de produit sans catégorie et de sélectionner rapidement plusieurs éléments à soumettre pour catégorisation.

4. Dans l'onglet **Accueil** , dans le groupe **Produit** , cliquez sur **Demander une mise à jour du catalogue**.
5. Consultez le message de confidentialité de soumission de catégorisation de System Center Online. Cliquez sur **Détails** pour afficher les informations qui seront envoyées à System Center Online.
6. Sélectionnez **J'ai bien lu et compris ce message**, puis cliquez sur **OK** pour autoriser les logiciels sélectionnés à être soumis à la catégorisation.
7. Vérifiez que l'état des noms de produits logiciels inventoriés soumis à System Center Online pour catégorisation est passé de **Sans catégorie** à **En attente**.

> **NOTE**
> L'état de validation du logiciel soumis à System Center Online pour catégorisation est **En attente** sur un site d'administration centrale mais sur les sites principaux enfant, l'état de validation affiché pour ces éléments continue d'être **Sans catégorie** .

## Résoudre les conflits de détails de logiciel

Suite à la réception par System Center Online de détails de catégorisation de logiciels nouvellement mis à jour et qui entrent en conflit avec des informations détaillées de logiciels existants, vous pouvez choisir la manière dont le conflit sera résolu. L'état de validation d'un logiciel en conflit est **Peut être mis à jour**. Après la résolution d'un conflit de détails de logiciel, les informations de catégorisation de logiciels sont conservées dans le catalogue Asset Intelligence en fonction des paramètres que vous avez définis. Un conflit de détails de logiciel ne peut pas se produire plusieurs fois pour la même valeur de catégorisation de logiciels à moins que la valeur System Center Online soit modifiée après la résolution du conflit.

Procédez comme suit pour résoudre un conflit de détails de logiciel.

#### Pour résoudre un conflit de détails de logiciel

1. Dans la console Configuration Manager, cliquez sur **Ressources et Conformité**.
2. Dans l'espace de travail **Biens et conformité** , cliquez sur **Asset Intelligence**, puis sur **Logiciels inventoriés**.
3. Passez en revue la colonne **État** pour les logiciels dont l'état est **Peut être mis à jour** .
4. Sélectionnez le logiciel pour lequel vous devez résoudre un conflit, puis sur l'onglet **Accueil** , dans le groupe **Produit** , puis cliquez sur **Résoudre le conflit**.

5. Passez en revue les informations suivantes :

   - **Valeur locale**: spécifie les informations existantes de catégorisation de logiciels dans le catalogue Asset Intelligence qui entrent en conflit avec les détails de catégorisation de logiciels System Center Online plus récents.
   - **Valeur téléchargée**: spécifie les nouvelles informations de catégorisation de logiciels System Center Online pour les informations de catégorisation de logiciels en conflit dans le catalogue Asset Intelligence.

6. Sélectionnez l'un des paramètres suivants pour résoudre le conflit de détails du logiciel :

   - **Ne changez pas la valeur des informations de catalogue modifiées localement**: résout le conflit de détails de logiciel en conservant les informations existantes de catégorisation de logiciels du catalogue Asset Intelligence. Lorsque vous sélectionnez ce paramètre, l'état du logiciel passe de **Peut être mis à jour** à **Défini par l'utilisateur**.
   - **Remplacez la valeur des informations de catalogue modifiées localement par la valeur System Center Online téléchargée**: résout le conflit de détails de logiciel en remplaçant les informations existantes de catégorisation de logiciels du catalogue Asset Intelligence par les nouvelles informations obtenues depuis System Center Online. Lorsque vous sélectionnez ce paramètre, l'état du logiciel passe de **Peut être mis à jour** à **Validé**.

     Cliquez sur **OK** pour enregistrer la résolution du conflit.

# Sécurité et confidentialité pour Asset Intelligence dans System Center Configuration Manager

22/06/2018 • 6 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cette rubrique contient des informations sur la sécurité et la confidentialité pour Asset Intelligence dans System Center Configuration Manager.

## Meilleures pratiques de sécurité pour Asset Intelligence

Utilisez les meilleures pratiques de sécurité suivantes dans l'optique d'utiliser Asset Intelligence.

| BONNES PRATIQUES DE SÉCURITÉ | PLUS D'INFORMATIONS |
|---|---|
| Lorsque vous importez un fichier de licence (fichier de licence en volume Microsoft ou fichier de déclaration générale de licence), sécurisez le fichier et le canal de communication. | Utilisez les autorisations du système de fichier pour vous assurer que seuls les utilisateurs autorisés peuvent accéder aux fichiers de licence et utilisez la signature SMB pour garantir l'intégrité des données lors de leur transfert au serveur de site pendant le processus d'importation. |
| Utilisez le principe des autorisations minimales pour importer les fichiers de licence. | Utilisez l'administration basée sur les rôles pour accorder l'autorisation Gérer Asset Intelligence à l'utilisateur administratif qui importe des fichiers de licence. Le rôle intégré d'Asset Manager inclut cette autorisation. |

## Informations confidentielles pour Asset Intelligence

Asset Intelligence étend les fonctions d'inventaire de Configuration Manager afin de permettre une meilleure visibilité des ressources au sein de l'entreprise. La collecte d'informations Asset Intelligence n'est pas activée automatiquement. Vous pouvez modifier le type d'informations collectées en activant les classes de rapport d'inventaire matériel. Pour plus d'informations, consultez Configuration d'Asset Intelligence dans System Center Configuration Manager.

Comme les informations d'inventaire, les informations Asset Intelligence sont stockées dans la base de données Configuration Manager. Lorsque les clients se connectent aux points de gestion à l'aide de HTTPS, les données sont toujours chiffrées lors du transfert vers le point de gestion. Lorsque les clients se connectent à l'aide de HTTP, vous pouvez configurer le transfert de données d'inventaire pour qu'il soit signé et chiffré. Les données d'inventaire ne sont pas stockées au format chiffré dans la base de données. Les informations sont conservées dans la base de données jusqu'à ce que la tâche de maintenance de site **Supprimer les historiques d'inventaire anciens** les supprime par intervalle de 90 jours. Vous pouvez configurer l'intervalle de suppression.

Asset Intelligence n'envoie pas d'informations sur les utilisateurs, les ordinateurs ou l'utilisation des licences à Microsoft. Vous pouvez choisir d'envoyer des requêtes System Center Online en vue d'une catégorisation. Ainsi, vous pouvez inventorier un ou plusieurs noms de logiciel sans catégorie et les envoyer dans System Center Online afin de les rechercher, puis de les classer. Une fois un nom de logiciel téléchargé, les fonctions de recherche de Microsoft l'identifient, le classent, puis le mettent à la disposition de tous les clients qui utilisent le service en ligne. Vous devez être conscient des conséquences de la soumission d'informations via System Center Online en termes de confidentialité :

- Le téléchargement s'applique uniquement aux informations génériques relatives au nom du logiciel (nom,

éditeur, etc.) que vous choisissez d'envoyer au System Center Online. Les informations d'inventaire ne peuvent faire l'objet d'un téléchargement.

- Le téléchargement ne se produit jamais automatiquement et le système n'est pas conçu pour que cette tâche soit automatisée. Vous devez sélectionner et approuver manuellement le téléchargement de chaque nom de logiciel.
- Une boîte de dialogue vous indique exactement quelles données seront téléchargées, avant le démarrage du processus de téléchargement.
- Les informations de licence ne sont pas envoyées à Microsoft. Les informations de licence sont stockées dans une zone séparée de la base de données Configuration Manager et elles ne peuvent pas être envoyées à Microsoft.
- Tous les noms de logiciel téléchargés deviennent dès lors publiques, car l'application correspondante ainsi que sa classification sont intégrées au catalogue System Center Online Asset Intelligence, puis seront téléchargées par d'autres utilisateurs du catalogue.
- La source du nom du logiciel n'est pas enregistrée dans le catalogue Asset Intelligence. Elle n'est donc pas disponible pour les autres utilisateurs. Vous devez toutefois toujours veiller à ne pas charger de noms d'application contenant des informations confidentielles.
- Les données téléchargées ne peuvent pas être rappelées.

  Avant de configurer le regroupement de données Asset Intelligence et de décider de soumettre des informations à System Center Online, pensez aux besoins de votre organisation en matière de confidentialité.

# Exemples de transitions d'état de validation pour Asset Intelligence dans System Center Configuration Manager

22/06/2018 • 7 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les états de validation Asset Intelligence dans System Center Configuration Manager ne sont pas statiques et peuvent se distinguer des actions administratives que vous exécutez pour affecter les données stockées dans le catalogue Asset Intelligence. Cette rubrique propose des exemples possibles de transition d'état de validation.

## Un élément de catalogue sans catégorie est catégorisé par l'utilisateur administratif

| TRANSITION D'ÉTAT | DESCRIPTION DE LA TRANSITION D'ÉTAT |
|---|---|
| **Sans catégorie** | Titre de logiciel inventorié qui n'a pas été catégorisé précédemment par System Center Online ou saisi par l'utilisateur administratif dans le catalogue Asset Intelligence. |
| **Sans catégorie** à **Définipar l'utilisateur** | L'élément sans catégorie est catégorisé par l'utilisateur administratif. |

## Un élément de catalogue catégorisé est de nouveau catégorisé par l'utilisateur administratif

| TRANSITION D'ÉTAT | DESCRIPTION DE LA TRANSITION D'ÉTAT |
|---|---|
| **Validé** | L'élément du catalogue a été défini par les chercheurs de System Center Online et figure dans le catalogue Asset Intelligence. |
| **Validé** à **Défini par l'utilisateur** | Un élément de catalogue validé est de nouveau catégorisé par l'utilisateur administratif. |

**NOTE**

Étant donné que les informations de catégorisation obtenues à partir de System Center Online sont stockées dans la base de données et ne peuvent pas être supprimées, l'utilisateur administratif peut restaurer la catégorisation de System Center Online ultérieurement.

## Un élément du catalogue défini par l'utilisateur est de nouveau catégorisé par System Center Online

| TRANSITION D'ÉTAT | DESCRIPTION DE LA TRANSITION D'ÉTAT |
|---|---|
| **Sans catégorie** | Un titre logiciel inventorié sans catégorie par System Center Online ou par l'utilisateur administratif est ajouté au catalogue Asset Intelligence. |
| **Défini par l'utilisateur** | L'élément sans catégorie est catégorisé par l'utilisateur administratif. |
| **Défini par l'utilisateur** à **Peut être mis à jour** | Un élément de catalogue défini par l'utilisateur a été catégorisé différemment par System Center Online au cours de mises à jour manuelles en bloc ultérieures du catalogue Asset Intelligence.<br><br>L'utilisateur administratif peut utiliser la boîte de dialogue **Résolution de conflit de détails de logiciel** pour décider s'il souhaite utiliser les nouvelles informations de catégorisation ou la valeur précédente définie par l'utilisateur. |
| **Peut être mis à jour** à **Validé** | L'utilisateur administratif utilise la boîte de dialogue **Résolution de conflit de détails de logiciel** pour utiliser les nouvelles informations de catégorisation reçues depuis System Center Online au cours de la mise à jour précédente du catalogue. |
| ou | |
| **Peut être mis à jour** à **Défini par l'utilisateur** | L'utilisateur administratif utilise la boîte de dialogue **Résolution de conflit de détails de logiciel** pour utiliser la valeur précédente définie par l'utilisateur. |

**NOTE**

Étant donné que les informations de catégorisation obtenues à partir de System Center Online sont stockées dans la base de données et ne peuvent pas être supprimées, l'utilisateur administratif peut restaurer la catégorisation de System Center Online ultérieurement.

## Un élément de catalogue sans catégorie est soumis à System Center Online à des fins de catégorisation

| TRANSITION D'ÉTAT | DESCRIPTION DE LA TRANSITION D'ÉTAT |
|---|---|
| **Sans catégorie** | Un titre logiciel inventorié sans catégorie par System Center Online ou par l'utilisateur administratif est ajouté à la base de données Asset Intelligence. |
| **Sans catégorie** à **En attente** | L'élément sans catégorie est soumis à System Center Online afin que l'utilisateur administratif puisse le classer. |
| **En attente** à **Validé** | L'élément est catégorisé par System Center Online. L'utilisateur administratif importe l'élément dans le catalogue Asset Intelligence à l'aide d'une mise à jour en bloc du catalogue ou de la synchronisation du catalogue Asset Intelligence. Les deux sont disponibles en utilisant le rôle de système de site du point de synchronisation Asset Intelligence. |

| TRANSITION D'ÉTAT | DESCRIPTION DE LA TRANSITION D'ÉTAT |
| --- | --- |

## Un élément de catalogue défini par l'utilisateur est soumis à System Center Online à des fins de catégorisation

| TRANSITION D'ÉTAT | DESCRIPTION DE LA TRANSITION D'ÉTAT |
| --- | --- |
| **Sans catégorie** | Un titre logiciel inventorié sans catégorie précédemment par un utilisateur administratif ou par System Center Online est ajouté à la base de données Asset Intelligence. |
| **Défini par l'utilisateur** | Vous avez catégorisé l'élément sans catégorie. |
| **Défini par l'utilisateur** à **En attente** | Vous soumettez l'élément défini par l'utilisateur à System Center Online à des fins de catégorisation. |
| **En attente** à **Peut être mis à jour** | Un élément du catalogue défini par un utilisateur a été catégorisé différemment par System Center Online lors de la synchronisation de catalogue suivante. Vous pouvez exécuter l'action **Résoudre le conflit** pour décider si vous allez utiliser les nouvelles informations de catégorisation ou la précédente valeur définie par l'utilisateur. Pour plus d'informations sur la résolution des conflits, consultez Résoudre les conflits de détails de logiciel. |
| **Peut être mis à jour** à **Validé** | Vous exécutez l'action **Résoudre le conflit** et sélectionnez les nouvelles informations de catégorisation reçues depuis System Center Online lors de la précédente mise à jour de catalogue. Pour plus d'informations sur la résolution des conflits, consultez Résoudre les conflits de détails de logiciel. |
| ou | |
| **Peut être mis à jour** à **Défini par l'utilisateur** | Vous exécutez l'action **Résoudre le conflit** et choisissez d'utiliser la précédente valeur définie par l'utilisateur. Pour plus d'informations sur la résolution des conflits, consultez Résoudre les conflits de détails de logiciel. |

**NOTE**

Étant donné que les informations de catégorisation obtenues à partir de System Center Online sont stockées dans la base de données et ne peuvent pas être supprimées, vous pouvez restaurer la catégorisation de System Center Online ultérieurement.

# Exemple de fichier d'importation de licence générale Asset Intelligence dans System Center Configuration Manager

22/06/2018 • 3 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Les informations données à titre d'exemple dans cette rubrique peuvent être utilisées pour créer un exemple de fichier de licence logicielle générale afin d'importer des licences logicielles dans le catalogue Asset Intelligence à l'aide de l'Assistant Importer des licences logicielles. Vous pouvez copier et coller le tableau suivant dans une nouvelle feuille de calcul Microsoft Excel et l'enregistrer avec l'extension .csv afin de pouvoir l'utiliser en tant qu'exemple de fichier d'importation de licence générale à des fins de test. Lors de la création d'un fichier d'importation de licence, tous les champs d'en-tête sont requis alors que seules les valeurs de données Nom, Éditeur, Version et Quantité effective sont requises dans la feuille de calcul. Pour plus d'informations sur l'importation de licences logicielles dans le catalogue Asset Intelligence, consultez Configuration d'Asset Intelligence dans System Center Configuration Manager.

| NOM | ÉDITEUR | VERSION | LANGAGE | QUANTITÉ EFFECTIVE | NUMÉRO BC | NOM DU REVENDEUR | DATE D'ACHAT | ACHAT DE LA PRISE EN CHARGE | DATE D'EXPIRATION DE LA PRISE EN CHARGE | COMMENTAIRES |
|---|---|---|---|---|---|---|---|---|---|---|
| Nom du logiciel 1 | Éditeur du logiciel | 1.01 | Anglais | 1 | Numéro d'achat | Nom du revendeur | 10/10/2010 | 0 | 10/10/2012 | Commentaire |
| Nom du logiciel 2 | Éditeur du logiciel | 1.02 | Anglais | 1 | Numéro d'achat | Nom du revendeur | 10/10/2010 | 0 | 10/10/2012 | Commentaire |
| Nom du logiciel 3 | Éditeur du logiciel | 1.03 | Anglais | 1 | Numéro d'achat | Nom du revendeur | 10/10/2010 | 0 | 10/10/2012 | Commentaire |
| Nom du logiciel 4 | Éditeur du logiciel | 1.04 | Anglais | 1 | Numéro d'achat | Nom du revendeur | 10/10/2010 | 0 | 10/10/2012 | Commentaire |
| Nom du logiciel 5 | Éditeur du logiciel | 1.05 | Anglais | 1 | Numéro d'achat | Nom du revendeur | 10/10/2010 | 0 | 10/10/2012 | Commentaire |

| NOM | ÉDITEUR | VERSION | LANGAGE | QUANTITÉ EFFECTIVE | NUMÉRO BC | NOM DU REVENDEUR | DATE D'ACHAT | ACHAT DE LA PRISE EN CHARGE | DATE D'EXPIRATION DE LA PRISE EN CHARGE | COMMENTAIRES |
|---|---|---|---|---|---|---|---|---|---|---|
| Nom du logiciel 6 | Éditeur du logiciel | 1.06 | Anglais | 1 | Numéro d'achat | Nom du revendeur | 10/10/2010 | 0 | 10/10/2012 | Commentaire |
| Nom du logiciel 7 | Éditeur du logiciel | 1.07 | Anglais | 1 | Numéro d'achat | Nom du revendeur | 10/10/2010 | 0 | 10/10/2012 | Commentaire |
| Nom du logiciel 8 | Éditeur du logiciel | 1.08 | Anglais | 1 | Numéro d'achat | Nom du revendeur | 10/10/2010 | 0 | 10/10/2012 | Commentaire |
| Nom du logiciel 9 | Éditeur du logiciel | 1.09 | Anglais | 1 | Numéro d'achat | Nom du revendeur | 10/10/2010 | 0 | 10/10/2012 | Commentaire |
| Nom du logiciel 10 | Éditeur du logiciel | 1.10 | Anglais | 1 | Numéro d'achat | Nom du revendeur | 10/10/2010 | 0 | 10/10/2012 | Commentaire |

# Utilisez le tableau de bord Cycle de vie du produit pour gérer la stratégie de cycle de vie Microsoft dans System Center Configuration Manager

22/06/2018 • 8 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Technical Preview)*

À partir de la Technical Preview version 1802, vous pouvez utiliser le tableau de bord Cycle de vie du produit de Configuration Manager. Le tableau de bord affiche l'état de la stratégie de cycle de vie des produits Microsoft installés sur des appareils gérés avec Configuration Manager. Le tableau de bord fournit des informations sur les produits Microsoft dans votre environnement, l'état de prise en charge et les dates de fin de prise en charge. Vous pouvez utiliser le tableau de bord pour comprendre la disponibilité de la prise en charge pour chaque produit. Ce qui vous aide à planifier quand mettre à jour les produits Microsoft que vous utilisez avant la fin de leur prise en charge.

Pour plus d'informations sur la stratégie de cycle de vie du produit Microsoft, consultez la page Stratégie de cycle de vie Microsoft.

## Prérequis

Pour afficher les données dans le Tableau de bord Cycle de vie du produit, les conditions suivantes sont requises :

- Internet Explorer 9 ou version ultérieure doit être installé sur l'ordinateur qui exécute la console Configuration Manager.
- Un point de Reporting Services est requis pour la fonctionnalité de lien hypertexte dans le tableau de bord dans la mesure où les liens hypertexte mènent à un rapport SQL Server Reporting Services (SSRS). Pour plus d'informations, consultez Génération de rapports dans System Center Configuration Manager.
- Le point de synchronisation Asset Intelligence doit être configuré et synchronisé. Pour plus d'informations, consultez Configurer Asset Intelligence dans System Center Configuration Manager.

Les données dans le tableau de bord dépendent du point de synchronisation Asset Intelligence installé. Le tableau de bord utilise le catalogue Asset Intelligence sous forme de métadonnées pour les noms des produits. Les métadonnées sont comparées aux données d'inventaire dans votre hiérarchie.

> **NOTE**
>
> Si vous configurez le point de service Asset Intelligence pour la première fois, veillez à activer les classes d'inventaire matériel Asset Intelligence. Le tableau de bord Cycle de vie dépend des classes d'inventaire matériel Asset Intelligence et n'affiche pas de données tant que les clients n'ont pas établi et retourné un inventaire matériel.

## Utilisez le tableau de bord Cycle de vie du produit Microsoft

Selon les données d'inventaire que vous collectez à partir des appareils gérés, le tableau de bord affiche des informations sur tous les produits actuels. Toutefois, les informations affichées pour les systèmes d'exploitation et SQL Server sont limitées aux versions suivantes :

- Windows Server 2008 et versions ultérieures
- Windows XP et versions ultérieures
- SQL Server 2008 et versions ultérieures

Pour accéder au tableau de bord Cycle de vie dans la console Configuration Manager, accédez à **Biens et conformité** > **Asset Intelligence** > **Cycle de vie du produit** .

> **NOTE**
> Les données dans le tableau de bord sont basées sur le site auquel la console Configuration Manager se connecte. Si la console se connecte à votre site de niveau supérieur, les données pour l'ensemble de la hiérarchie s'affichent. Lorsqu'elle est connectée à un site principal enfant, seules les données de ce site s'affichent.

**Tableau de bord Cycle de vie du produit**

Le tableau de bord comporte les vignettes suivantes :

- **Cinq produits principaux dont la fin de vie est écoulée :** cette vignette est une vue consolidée des produits dans votre environnement dont la fin de vie est écoulée. Le graphe affiche les logiciels installés qui ont expiré lors de la comparaison avec le cycle de vie du produit pour les systèmes d'exploitation et les produits SQL Server.
- **Cinq produits principaux dont la fin de vie est proche :** cette vignette est une vue consolidée des produits dans votre environnement dont la fin de vie est prévue dans les six prochains mois. Le graphe affiche les logiciels installés dont la fin de vie est prévue dans les six prochains mois lors de la comparaison avec le cycle de vie du produit pour les systèmes d'exploitation et les produits SQL Server.
- **Données du cycle de vie des produits installés :** cette vignette vous donne une idée générale du moment de la transition d'un produit de l'état pris en charge à l'état expiré. Le graphe fournit une répartition du nombre de clients où le produit est installé, l'état de disponibilité de prise en charge, avec un lien pour en savoir plus sur les étapes à suivre. Les informations suivantes sont incluses dans le graphe :
  - Temps de prise en charge restant
  - Nombre dans l'environnement
  - Date de fin de la prise en charge grand public
  - Date de fin de la prise en chargé étendue
  - Étapes suivantes

> **IMPORTANT**
> Les informations affichées dans ce tableau de bord sont fournies pour des raisons pratiques et uniquement destinées à une utilisation en interne dans votre entreprise. Vous ne devez pas vous fier uniquement à ces informations pour confirmer la conformité. Veillez à vérifier l'exactitude des informations fournies, ainsi que la disponibilité des informations de prise en charge en consultant le site https://support.microsoft.com/en-us/lifecycle.

## Rapports

Les nouveaux rapports ci-dessous sont ajoutés sous la catégorie **Cycle de vie du produit** :

- **Vue d'ensemble du cycle de vie du produit général :** affichez la liste des cycles de vie des produits. La liste peut être filtrée par nom de produit et de jours restants avant l'expiration définissables par l'utilisateur.
- **Ordinateurs équipés d'un logiciel spécifique :** affichez la liste des ordinateurs sur lesquels un produit spécifique est détecté.
- **Liste des produits expirés trouvés dans l'organisation :** affichez les détails sur les produits dans votre environnement dont les dates du cycle de vie ont expiré.
- **Liste des ordinateurs avec des produits expirés dans l'organisation :** affichez les ordinateurs sur lesquels des produits ont expiré. Vous pouvez filtrer ce rapport par nom de produit.

# Étapes suivantes

Pour obtenir des informations complémentaires sur l'installation ou la mise à jour de l'édition Technical Preview, consultez Technical Preview pour System Center Configuration Manager.

# Présentation du contrôle à distance dans System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez le contrôle à distance pour administrer, fournir une assistance ou afficher à distance n'importe quel ordinateur client de la hiérarchie. Vous pouvez l'utiliser également pour résoudre les problèmes de configuration matérielle et logicielle sur les ordinateurs clients et pour fournir une assistance. Le Gestionnaire de configuration prend en charge le contrôle à distance de tous les ordinateurs du groupe de travail et de tous les ordinateurs joints à un domaine qui fonctionnent sous des systèmes d'exploitation pris en charge pour le client Gestionnaire de configuration. Pour plus d'informations, consultez l'article Systèmes d'exploitation pris en charge pour les clients et les appareils pour System Center Configuration Manager.

Configuration Manager vous permet aussi de configurer les paramètres clients pour exécuter les services Windows Bureau à distance et Assistance à distance à partir de la console Configuration Manager.

> **NOTE**
> Il n'est pas possible d'établir une session Assistance à distance de la console Configuration Manager vers un ordinateur client qui se trouve dans un groupe de travail.

Vous pouvez démarrer une session de contrôle à distance dans la console Configuration Manager à partir de **Ressources et conformité** > **Appareils**, d'un regroupement d'appareils, de la fenêtre d'invite de commandes Windows ou du menu **Démarrer** de Windows.

# Configuration requise pour le contrôle à distance dans System Center Configuration Manager

22/06/2018 • 3 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Le contrôle à distance dans System Center Configuration Manager comporte des dépendances externes et des dépendances au sein du produit.

## Dépendances externes à Configuration Manager

| DÉPENDANCE | PLUS D'INFORMATIONS |
|---|---|
| Pilote de carte vidéo d'ordinateur | Assurez-vous que la toute dernière version du pilote vidéo est installée sur les ordinateurs clients pour garantir des performances optimales du contrôle à distance. |

Les appareils exécutant Windows Embedded, Windows Embedded for Point of Service (POS) et Windows Fundamentals for Legacy PCs ne prennent pas en charge l'observateur de contrôle à distance, mais ils prennent en charge le client du contrôle à distance.

Le contrôle à distance de Configuration Manager ne permet pas d'administrer à distance les ordinateurs clients qui exécutent Systems Management Server 2003 ou Configuration Manager 2007.

> **NOTE**
> Aucun service Windows n'est nécessaires en tant que dépendance externe pour le contrôle à distance.

**Systèmes d'exploitation pris en charge pour l'observateur de contrôle à distance**

La visionneuse de contrôle à distance est gérée sur tous les systèmes d'exploitation pris en charge pour la console Configuration Manager. Pour plus d'informations, consultez l'article Configurations prises en charge pour les consoles System Center Configuration Manager.

## Dépendances de Configuration Manager

| DÉPENDANCE | PLUS D'INFORMATIONS |
|---|---|
| Le contrôle à distance doit être activé pour les clients | Par défaut, le contrôle à distance n'est pas activé quand vous installez Configuration Manager. Pour plus d'informations sur l'activation et la configuration du contrôle à distance, consultez Configuration du contrôle à distance dans System Center Configuration Manager. |
| Point de Reporting Services | Le rôle de système de site du point de Reporting Services doit être installé avant que vous puissiez exécuter des rapports pour le contrôle à distance. Pour plus d'informations, consultez Génération de rapports dans System Center Configuration Manager. |

| DÉPENDANCE | PLUS D'INFORMATIONS |
| --- | --- |
| Autorisations de sécurité pour gérer le contrôle à distance | Pour accéder aux ressources du regroupement et lancer une session de contrôle à distance à partir de la console Configuration Manager : autorisations **Lecture**, **Lire la ressource** et **Contrôle à distance** pour l'objet **Regroupement**.<br><br>Le rôle de sécurité **Opérateur d'outils à distance** inclut ces autorisations qui sont nécessaires pour gérer le contrôle à distance dans Configuration Manager.<br><br>Pour plus d'informations, consultez Configurer l'administration basée sur des rôles pour System Center Configuration Manager.<br><br>Par ailleurs, il faut donner aux utilisateurs concernés l'autorisation d'utiliser le contrôle à distance en les ajoutant à la liste **Observateurs autorisés du contrôle à distance et de l'assistance à distance** dans les paramètres client **Outils de contrôle à distance**. |

# Configuration du contrôle à distance dans System Center Configuration Manager

22/06/2018 • 5 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cette procédure décrit la configuration des paramètres client par défaut pour le contrôle à distance. Ces paramètres s'appliquent à tous les ordinateurs de votre hiérarchie. Si vous voulez que ces paramètres s'appliquent seulement à certains ordinateurs, affectez un paramètre client personnalisé à un regroupement contenant ces ordinateurs. Pour plus d'informations, consultez Guide pratique pour configurer les paramètres client dans System Center Configuration Manager.

Pour utiliser l'Assistance à distance ou le Bureau à distance, vous devez les installer et les configurer sur l'ordinateur qui exécute la console Configuration Manager. Pour plus d'informations sur la procédure d'installation et de configuration de l'Assistance à distance ou du Bureau à distance, consultez votre documentation Windows.

#### Pour activer le contrôle à distance et configurer les paramètres client

1. Dans la console Configuration Manager, choisissez **Administration** > **Paramètres client** > **Paramètres client par défaut**.
2. Sous l'onglet **Accueil**, dans le groupe **Propriétés**, choisissez **Propriétés**.
3. Dans la boîte de dialogue **Par défaut**, choisissez **Outils de contrôle à distance**.
4. Configurez les paramètres client du contrôle à distance, de l'Assistance à distance et du Bureau à distance. Pour obtenir la liste des paramètres client des outils de contrôle à distance que vous pouvez configurer, consultez Outils de contrôle à distance.

   Vous pouvez modifier le nom de l'entreprise qui apparaît dans la boîte de dialogue **Contrôle à distance ConfigMgr** en configurant une valeur pour **Nom d'organisation affiché dans le Centre logiciel** dans les paramètres client **Agent ordinateur** .

   Les ordinateurs clients sont configurés avec ces paramètres la prochaine fois qu'ils téléchargent la stratégie du client. Pour lancer la récupération de stratégie pour un client unique, consultez Comment gérer les clients dans System Center Configuration Manager.

#### Activer la traduction du clavier

Par défaut, Configuration Manager transmet la position des touches à partir de l'emplacement de la personne qui visualise vers l'emplacement de la personne effectuant le partage. Ceci peut poser un problème pour les configurations de clavier qui diffèrent entre la personne qui visualise et la personne effectuant le partage. Par exemple, un afficheur avec un clavier anglais tapait un « A », mais le clavier français de la personne effectuant le partage fournissait un « Q ». Nous pouvons maintenant configurer le contrôle à distance afin que le caractère lui-même soit transmis du clavier de la personne qui visualise vers la personne effectuant le partage, et que ce que la personne qui visualise veut taper parvienne à la personne effectuant le partage.

Pour activer la traduction du clavier, dans **Contrôle à distance de Configuration Manager**, choisissez **Action** et choisissez **Activer la traduction du clavier** pour transmettre la position des touches.

> **NOTE**
>
> Les touches spéciales, notamment ~!#@$%, ne seront pas traduites correctement.

# Raccourcis clavier relatifs à l'observateur de contrôle à distance

| RACCOURCI CLAVIER | DESCRIPTION |
|---|---|
| Alt+Pg préc | Bascule entre les programmes en cours d'exécution de gauche à droite. |
| Alt+Pg suiv | Bascule entre les programmes en cours d'exécution de droite à gauche. |
| Alt+Inser | Parcourt les programmes en cours d'exécution dans l'ordre dans lequel ils ont été ouverts. |
| Alt+Origine | Affiche le menu **Démarrer** . |
| Ctrl+Alt+Fin | Affiche la boîte de dialogue Sécurité de Windows (Ctrl+Alt+Suppr). |
| Alt+Suppr | Affiche le menu Windows. |
| Ctrl+Alt+Signe moins (sur le pavé numérique) | Copie la fenêtre active de l'ordinateur local vers le Presse-papiers de l'ordinateur distant. |
| Ctrl+Alt+Signe plus (sur le pavé numérique) | Copie la zone entière de la fenêtre de l'ordinateur local dans le Presse-papiers de l'ordinateur distant. |

# Comment administrer à distance un ordinateur client Windows à l'aide de System Center Configuration Manager

22/06/2018 • 6 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Avant de commencer à utiliser le contrôle à distance, veillez à consulter les informations des rubriques suivantes :

- Prérequis pour le contrôle à distance dans System Center Configuration Manager
- Configuration du contrôle à distance dans System Center Configuration Manager

Vous pouvez démarrer l'observateur de contrôle à distance de trois manières :

- Dans la console Configuration Manager.
- À une invite de commandes Windows.
- Dans le menu **Démarrer** de Windows sur un ordinateur qui exécute la console Configuration Manager à partir du groupe de programmes **Microsoft System Center**.

**Pour administrer à distance un ordinateur client à partir de la console Configuration Manager**

1. Dans la console Configuration Manager, choisissez **Actifs et Conformité** > **Appareils** ou **Regroupements d'appareils**.
2. Sélectionnez l'ordinateur à administrer à distance puis, sous l'onglet **Accueil**, dans le groupe **Appareil**, choisissez **Démarrer** > **Contrôle à distance**.

   > **IMPORTANT**
   > Si le paramètre client **Inviter l'utilisateur à autoriser le contrôle à distance** a la valeur **True**, la connexion ne démarre pas tant que l'utilisateur de l'ordinateur distant n'accepte pas l'invite de contrôle à distance. Pour plus d'informations, consultez Configuration du contrôle à distance dans System Center Configuration Manager.

3. Lorsque la fenêtre **Contrôle à distance de Configuration Manager** s'ouvre, vous pouvez administrer à distance l'ordinateur client. Utilisez les options suivantes pour configurer la connexion.

   > **NOTE**
   > Si l'ordinateur auquel vous vous connectez dispose de plusieurs moniteurs, l'affichage de tous les moniteurs apparaît dans la fenêtre de contrôle à distance.

   - **Fichier - Connecter** : se connecte à un autre ordinateur. Cette option n'est pas disponible lorsqu'une session de contrôle à distance est active.
   - **Fichier - Déconnecter** : déconnecte la session active de contrôle à distance, mais ne ferme pas la fenêtre **Contrôle à distance de Configuration Manager**.
   - **Fichier - Quitter** : déconnecte la session de contrôle à distance active et ferme la fenêtre **Contrôle à distance de Configuration Manager**.

> **NOTE**
> Quand vous vous déconnectez d'une session de contrôle à distance, le contenu du Presse-papiers de Windows sur l'ordinateur que vous visualisez est supprimé.

- **Affichage - Plein écran** : optimise la fenêtre **Contrôle à distance de Configuration Manager**.

  > **NOTE**
  > Pour quitter le mode plein écran, appuyez sur Ctrl+Alt+Pause.

- **Afficher - Ajuster à la page** : redimensionne l'affichage de l'ordinateur distant pour l'adapter à la taille de la fenêtre **Contrôle à distance de Configuration Manager**.
- **Afficher - Barre d'état** : active ou désactive l'affichage de la barre d'état de la fenêtre **Contrôle à distance de Configuration Manager**.
- **Action - Envoyer Ctrl+Alt+Suppr** : envoie la séquence de touches Ctrl+Alt+Suppr à l'ordinateur distant.
- **Action - Activer le partage du Presse-papiers** : permet de copier et coller des éléments vers et depuis l'ordinateur distant. Si vous modifiez cette valeur, vous devez redémarrer la session de contrôle à distance pour appliquer la modification.

  > **NOTE**
  > Si vous ne voulez pas que le partage du Presse-papiers soit activé dans la console Configuration Manager, sur l'ordinateur exécutant la console, définissez la valeur de la clé de Registre **HKEY_CURRENT_USER\Software\Microsoft\ConfigMgr10\Remote Control\Clipboard Sharing** sur **0**.

- **Action - Verrouiller le clavier distant et la souris** : verrouille le clavier et la souris distants pour empêcher l'utilisateur d'utiliser l'ordinateur distant.
- **Aide - À propos du contrôle à distance** : affiche la version actuelle de l'observateur.

4. Les utilisateurs de l'ordinateur distant peuvent afficher plus d'informations sur la session de contrôle à distance lorsqu'ils cliquent sur l'icône **Contrôle à distance** de Configuration Manager dans la zone de notification de Windows ou sur l'icône dans la barre de la session de contrôle à distance.

**Pour démarrer l'observateur de contrôle à distance à partir de la ligne de commande Windows**

- À l'invite de commandes Windows, tapez <*Dossier d'installation Configuration Manager*>**\AdminConsole\Bin\x64\CmRcViewer.exe**

CmRcViewer.exe prend en charge les options de ligne de commande suivantes :

- *Adresse* : spécifie le nom NetBIOS, le nom de domaine complet (FQDN) ou l'adresse IP de l'ordinateur client auquel vous voulez vous connecter.
- *Nom du serveur de site* : indique le nom du serveur de site System Center Configuration Manager auquel vous voulez envoyer des messages d'état associés à la session de contrôle à distance.
- **/?** : affiche les options de ligne de commande de l'observateur de contrôle à distance.

**Example:CmRcViewer.exe** <*Adresse*> <*Nom du serveur de site*>

# Comment auditer l'utilisation du contrôle à distance dans System Center Configuration Manager

22/06/2018 • 3 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez utiliser les rapports System Center Configuration Manager pour afficher les informations d'audit du contrôle à distance.

Pour plus d'informations sur la configuration des rapports dans Configuration Manager, consultez Rapports dans System Center Configuration Manager.

Les deux rapports suivants sont disponibles avec la catégorie **Messages d'état - Audit**:

- **Contrôle à distance - Tous les ordinateurs contrôlés à distance par un utilisateur spécifique** : affiche un résumé de l'activité de contrôle à distance initiée par un utilisateur spécifique.
- **Contrôle à distance - Toutes les informations de contrôle à distance** : affiche un résumé des messages d'état concernant le contrôle à distance des ordinateurs clients.

**Pour exécuter le rapport Contrôle à distance - Tous les ordinateurs contrôlés à distance par un utilisateur spécifique**

1. Dans la console Configuration Manager, cliquez sur **Surveillance**.
2. Dans l'espace de travail **Surveillance** , développez **Rapports**, puis cliquez sur **Rapports**.
3. Dans le nœud **Rapports** , cliquez sur la colonne **Catégorie** pour trier les rapports, ce qui vous permettra de trouver plus rapidement les rapports dans la catégorie **Messages d'état - Audit**.
4. Sélectionnez le rapport **Contrôle à distance - Tous les ordinateurs contrôlés à distance par un utilisateur spécifique**, puis, sous l'onglet **Accueil** , dans **Groupe de rapports**, cliquez sur **Exécuter**.
5. Dans la liste **Nom d'utilisateur** de **Contrôle à distance - Tous les ordinateurs contrôlés à distance par un utilisateur spécifique**, indiquez l'utilisateur pour lequel vous voulez afficher des informations d'audit, puis cliquez sur **Afficher le rapport**.
6. Une fois que vous avez terminé de consulter les données du rapport, fermez la fenêtre du rapport.

**Pour exécuter le rapport Contrôle à distance - Toutes les informations de contrôle à distance**

1. Dans la console Configuration Manager, cliquez sur **Surveillance**.
2. Dans l'espace de travail **Surveillance** , développez **Rapports**, puis cliquez sur **Rapports**.
3. Dans le nœud **Rapports** , cliquez sur la colonne **Catégorie** pour trier les rapports, ce qui vous permettra de trouver plus rapidement les rapports dans la catégorie **Messages d'état - Audit**.
4. Sélectionnez le rapport **Contrôle à distance - Toutes les informations de contrôle à distance**, puis, sous l'onglet **Accueil** , dans **Groupe de rapports**, cliquez sur **Exécuter** pour ouvrir la fenêtre **Contrôle à distance - Toutes les informations de contrôle à distance** .
5. Une fois que vous avez terminé de consulter les données du rapport, fermez la fenêtre du rapport.

# Sécurité et confidentialité pour le contrôle à distance dans System Center Configuration Manager

22/06/2018 • 9 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cette rubrique contient des informations de sécurité et de confidentialité pour le contrôle à distance dans System Center 2012 Configuration Manager.

## Meilleures pratiques de sécurité pour le contrôle à distance

Utilisez les meilleures pratiques de sécurité suivantes lorsque vous gérez des ordinateurs client à l'aide du contrôle à distance.

| BONNES PRATIQUES DE SÉCURITÉ | PLUS D'INFORMATIONS |
|---|---|
| Quand vous vous connectez à un ordinateur distant, ne continuez pas si l'authentification NTLM est utilisée au lieu de l'authentification Kerberos. | Quand Configuration Manager détecte que la session de contrôle à distance est authentifiée à l'aide de NTLM plutôt que Kerberos, une invite apparaît pour vous avertir que l'identité de l'ordinateur distant ne peut pas être vérifiée. Ne poursuivez pas la session de contrôle à distance. L'authentification NTLM est un protocole d'authentification plus faible que Kerberos et elle est vulnérable à la relecture et à l'emprunt d'identité. |
| N'activez pas le partage du Presse-papiers dans l'observateur de contrôle à distance. | Le Presse-papiers prend en charge des objets tels que des fichiers exécutables ou du texte et il peut être utilisé par l'utilisateur sur l'ordinateur hôte pendant la session de contrôle à distance pour exécuter un programme sur l'ordinateur d'origine. |
| N'entrez pas de mots de passe pour les comptes privilégiés en cas d'administration à distance d'un ordinateur. | Des logiciels qui observent les saisies clavier peuvent intercepter le mot de passe. Ou bien, si le programme en cours d'exécution sur l'ordinateur client n'est pas celui auquel l'utilisateur du contrôle à distance pense, ce programme peut être en train de capturer le mot de passe. Lorsque des comptes et des mots de passe sont demandés, ils doivent être saisis par l'utilisateur final. |
| Verrouillez le clavier et la souris pendant une session de contrôle à distance. | Si Configuration Manager détecte que la connexion de contrôle à distance est terminée, Configuration Manager verrouille automatiquement le clavier et la souris afin qu'aucun utilisateur ne puisse prendre le contrôle de la session de contrôle à distance ouverte. Toutefois, cette détection peut ne pas se produire immédiatement et ne se produit pas si le service de contrôle à distance est terminé.<br><br>Sélectionnez l'action **Verrouiller le clavier distant et la souris** dans la fenêtre **Contrôle à distance ConfigMgr** . |

| BONNES PRATIQUES DE SÉCURITÉ | PLUS D'INFORMATIONS |
| --- | --- |
| N’autorisez pas les utilisateurs à configurer les paramètres de contrôle à distance dans le Centre logiciel. | N'activez pas le paramètre client **Les utilisateurs peuvent modifier les paramètres de stratégie ou de notification dans le Centre logiciel** pour empêcher l'espionnage des utilisateurs.<br><br>Ce paramètre est destiné à l’ordinateur et non à l’utilisateur connecté. |
| Activez le profil de pare-feu Windows **Domaine** . | Activez le paramètre client **Activer le contrôle à distance sur les profils d'exception de pare-feu clients** , puis sélectionnez le pare-feu Windows **Domaine** pour les ordinateurs de l'intranet. |
| Si vous fermez une session pendant un contrôle à distance et vous connectez en tant qu’utilisateur différent, assurez-vous de fermer la session avant de déconnecter la session de contrôle à distance. | Si vous ne fermez pas la session selon ce scénario, la session reste ouverte. |
| N’accordez pas aux utilisateurs des droits d’administrateur local. | Lorsque vous accordez aux utilisateurs des droits d'administrateur local, ils peuvent reprendre votre session de contrôle à distance ou compromettre vos informations d'identification. |
| Utilisez une stratégie de groupe ou Configuration Manager pour configurer les paramètres d’assistance à distance, mais pas les deux. | Vous pouvez utiliser Configuration Manager et une stratégie de groupe pour modifier la configuration des paramètres d’assistance à distance. Quand la stratégie de groupe est actualisée sur le client, par défaut, le processus est optimisé en modifiant uniquement les stratégies qui ont été modifiées sur le serveur. Configuration Manager modifie les paramètres de la stratégie de sécurité locale, qui ne peuvent pas être remplacés, sauf si la mise à jour de la stratégie de groupe est imposée.<br><br>Définir la stratégie aux deux emplacements peut provoquer des incohérences. Choisissez l'une des méthodes ci-dessous pour configurer vos paramètres d'assistance à distance. |
| Activez le paramètre client **Inviter l’utilisateur à autoriser le contrôle à distance**. | Bien qu'il soit possible de contourner ce paramètre client qui invite un utilisateur à confirmer une session de contrôle à distance, activez ce paramètre afin de réduire le risque d'espionnage des utilisateurs lorsqu'ils travaillent sur des tâches confidentielles.<br><br>En outre, apprenez aux utilisateurs à vérifier le nom du compte qui est affiché pendant la session de contrôle à distance et à fermer la session s'ils pensent que le compte n'est pas autorisé. |
| Limitez la liste des observateurs autorisés. | Des droits d'administrateur local ne sont pas nécessaires à l'utilisation du contrôle à distance par un utilisateur. |

### Problèmes de sécurité pour le contrôle à distance

La gestion d'ordinateurs client à l'aide du contrôle à distance présente les problèmes de sécurité suivants :

- Ne considérez pas les messages d’audit de contrôle à distance comme fiables.

  Si vous démarrez une session de contrôle à distance et vous vous connectez ensuite à l’aide d’autres informations d’identification, c’est le compte d’origine qui envoie les messages d’audit et non le compte qui

a utilisé les autres informations d'identification.

Les messages d'audit ne sont pas envoyés si vous copiez les fichiers binaires pour le contrôle à distance au lieu d'installer la console Configuration Manager, puis exécutez le contrôle à distance à partir de l'invite de commandes.

## Informations de confidentialité pour le contrôle à distance

Le contrôle à distance vous permet d'afficher les sessions actives sur les ordinateurs clients Configuration Manager et de consulter éventuellement des informations stockées sur ces ordinateurs. Par défaut, le contrôle à distance n'est pas activé.

Bien que vous puissiez le configurer pour envoyer des avis importants et obtenir le consentement d'un utilisateur avant le début d'une session de contrôle à distance, il peut également surveiller les utilisateurs sans qu'ils le veuillent ou le sachent. Vous pouvez configurer le niveau d'accès Afficher uniquement, de sorte que rien ne puisse être modifié sur le contrôle à distance ou le contrôle intégral. Le compte de l'administrateur de connexion s'affiche dans la session de contrôle à distance pour aider les utilisateurs à savoir qui se connecte à leur ordinateur.

Par défaut, Configuration Manager accorde au groupe Administrateurs local des autorisations de contrôle à distance.

Avant de configurer le contrôle à distance, analysez vos besoins en matière de confidentialité.

# Présentation de la gestion de l'alimentation dans System Center Configuration Manager

22/06/2018 • 5 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

La gestion de l'alimentation dans System Center Configuration Manager répond au besoin de nombreuses organisations de contrôler et réduire la consommation d'énergie de leurs ordinateurs. Cette fonctionnalité tire parti des fonctionnalités de la gestion de l'alimentation intégrée à Windows pour appliquer les paramètres pertinents et cohérents aux ordinateurs de l'organisation. Vous pouvez appliquer différents paramètres d'alimentation aux ordinateurs pendant les heures de bureau et les heures creuses. Par exemple, vous pouvez souhaiter appliquer un mode d'alimentation plus restrictif aux ordinateurs pendant les heures creuses. Dans les cas où les ordinateurs doivent toujours rester allumés, vous pouvez empêcher l'application des paramètres de gestion de l'alimentation.

La gestion de l'alimentation dans Configuration Manager comprend plusieurs rapports permettant d'analyser la consommation énergétique et les paramètres d'alimentation des ordinateurs de votre organisation. Vous pouvez également utiliser les rapports pour vous aider à résoudre les problèmes de gestion de l'alimentation.

Pour obtenir un flux de travail détaillé sur la configuration et l'utilisation de la gestion de l'alimentation, consultez Liste de contrôle de l'administrateur pour la gestion de l'alimentation dans System Center Configuration Manager.

> **IMPORTANT**
> La gestion de l'alimentation dans Configuration Manager n'est pas prise en charge sur les ordinateurs virtuels. Vous ne pouvez pas appliquer les modes d'alimentation aux ordinateurs virtuels, ni signaler de données d'alimentation à partir de ces ordinateurs.

## Flux de travail de la gestion de l'alimentation

Appliquez les trois étapes suivantes pour planifier et mettre en œuvre la gestion de l'alimentation dans Configuration Manager.

**Phase de surveillance et de planification**

La gestion de l'alimentation utilise l'inventaire matériel de Configuration Manager pour recueillir des données sur les paramètres d'alimentation et d'utilisation des ordinateurs du site. Il existe un certain nombre de rapports que vous pouvez utiliser pour analyser ces données et déterminer les paramètres optimaux de gestion de l'alimentation pour les ordinateurs. Par exemple, pendant la phase de surveillance et de planification du flux de travail de la gestion de l'alimentation, vous pouvez créer des regroupements à partir des données incluses dans le rapport **Fonctions de gestion de l'alimentation** et utiliser ces données pour identifier les ordinateurs qui ne sont pas capables d'effectuer la gestion de l'alimentation. Ensuite, vous pouvez exclure ces ordinateurs de la gestion de l'alimentation.

**IMPORTANT**

N'appliquez pas de modes d'alimentation aux ordinateurs de votre site avant de recueillir et d'analyser les données d'alimentation d'ordinateurs client. Si vous appliquez de nouveaux paramètres de gestion de l'alimentation aux ordinateurs sans examiner préalablement les paramètres existants, vous risquez d'observer une augmentation de la consommation d'énergie.

### Phase de mise en œuvre

La gestion de l'alimentation vous permet de créer des modes d'alimentation que vous pouvez appliquer aux regroupements d'ordinateurs de votre site. Ces modes d'alimentation configurent les paramètres de gestion de l'alimentation Windows sur les ordinateurs. Vous pouvez utiliser les modes de gestion de l'alimentation inclus dans Configuration Manager ou configurer vos propres modes personnalisés. Vous pouvez utiliser les données d'alimentation recueillies pendant la phase de surveillance et de planification comme ligne de base pour vous aider à évaluer les économie d'énergie après avoir appliqué un mode d'alimentation aux ordinateurs. Pour plus d'informations, consultez Liste de contrôle de l'administrateur pour la gestion de l'alimentation dans System Center Configuration Manager.

### Phase de compatibilité

Dans la phase de compatibilité, vous pouvez exécuter des rapports qui vous aident à évaluer les économies à réaliser en matière de consommation énergétique et de coût de l'alimentation dans votre organisation. Vous pouvez également exécuter des rapports décrivant les améliorations relatives à la quantité de CO2 générée par les ordinateurs. Il existe également des rapports qui vous aident à vérifier que les paramètres d'alimentation ont été correctement appliqués aux ordinateurs, ce qui vous aide à résoudre les problèmes liés à la fonction de gestion de l'alimentation.

# Configuration requise pour la gestion de l'alimentation dans System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

La gestion de l'alimentation dans System Center Configuration Manager comporte des dépendances externes et des dépendances au sein du produit.

## Dépendances externes à Configuration Manager

Le tableau suivant répertorie les dépendances externes à Configuration Manager pour l'utilisation de la gestion de l'alimentation.

| DÉPENDANCE | PLUS D'INFORMATIONS |
|---|---|
| Les ordinateurs client doivent être en mesure de prendre en charge les états requis de l'alimentation | Pour utiliser toutes les fonctionnalités de la gestion de l'alimentation, les ordinateurs client doivent être en mesure de prendre en charge la mise en veille, la mise en veille prolongée, la sortie du mode veille et la sortie du mode veille prolongée. Vous pouvez utiliser le rapport **Fonctions de gestion de l'alimentation** afin de déterminer si les ordinateurs peuvent prendre en charge ces actions. Pour plus d'informations, consultez le rapport Fonctions de gestion de l'alimentation dans la rubrique Guide pratique pour surveiller et planifier la gestion de l'alimentation dans System Center Configuration Manager. |

## Dépendances de Configuration Manager

Le tableau suivant répertorie les dépendances au sein de Configuration Manager pour l'utilisation de la gestion de l'alimentation.

| DÉPENDANCE | INFORMATIONS COMPLÉMENTAIRES |
|---|---|
| Vous devez activer la gestion de l'alimentation avant de pouvoir créer et surveiller des modes d'alimentation. | Pour plus d'informations sur la façon d'activer et de configurer la gestion de l'alimentation, consultez Configuration de la gestion de l'alimentation dans System Center Configuration Manager. |
| Point de Reporting Services | Vous devez configurer un point de Reporting Services avant de pouvoir afficher des rapports de gestion de l'alimentation. Pour plus d'informations, consultez Génération de rapports dans System Center Configuration Manager. |

# Meilleures pratiques de gestion de l'alimentation dans System Center Configuration Manager

22/06/2018 • 8 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez les bonnes pratiques de gestion de l'alimentation suivantes dans System Center Configuration Manager.

## Effectuer la phase de surveillance à un moment représentatif

La phase de surveillance de la gestion de l'alimentation fournit des informations sur la consommation d'énergie, l'activité, les fonctionnalités de gestion de l'alimentation et l'impact sur l'environnement des ordinateurs de votre organisation. Veillez à choisir une période représentative pour effectuer la phase de surveillance. Par exemple, l'exécution de la phase de surveillance un jour férié ne fournit pas un rapport réaliste sur l'utilisation énergétique des ordinateurs.

## Créer un regroupement de contrôle d'ordinateurs sans appliquer de modes de gestion de l'alimentation.

Créez deux regroupements d'ordinateurs pour vous aider à surveiller les effets de l'application de modes de gestion de l'alimentation aux ordinateurs. Le premier regroupement doit contenir la majorité des ordinateurs auxquels vous souhaitez appliquer les paramètres d'alimentation et l'autre regroupement (le regroupement de contrôle) doit contenir les autres ordinateurs. Appliquez le mode de gestion de l'alimentation requis au regroupement contenant la majorité des ordinateurs. Vous pouvez ensuite exécuter des rapports pour comparer le coût de l'alimentation, la gestion de l'alimentation et l'impact sur l'environnement des ordinateurs auxquels vous avez appliqué des paramètres d'alimentation et le regroupement de contrôle auquel vous n'avez pas appliqué de paramètres d'alimentation.

## Exécuter le rapport des paramètres d'alimentation avant d'appliquer un mode de gestion de l'alimentation

Avant d'appliquer un mode de gestion de l'alimentation à un regroupement d'ordinateurs, exécutez le rapport **Paramètres d'alimentation** pour mieux comprendre les paramètres de gestion de l'alimentation qui sont déjà configurés sur les ordinateurs du regroupement. Si vous appliquez les nouveaux paramètres de gestion de l'alimentation aux ordinateurs sans examiner préalablement les paramètres existants, cela peut entraîner une augmentation de la consommation d'énergie.

## Exclure les serveurs de la gestion de l'alimentation

La gestion de l'alimentation n'est pas prise en charge pour les ordinateurs qui exécutent Windows Server (bien que les données de gestion de l'alimentation soient collectées). Veillez à ajouter les serveurs à un regroupement et à exclure ce dernier de la gestion de l'alimentation.

## Exclure les ordinateurs que vous ne souhaitez pas gérer

Si vous disposez d'ordinateurs que vous ne souhaitez pas gérer avec la gestion de l'alimentation, ajoutez-les à un regroupement et assurez-vous que le regroupement est exclu de la gestion de l'alimentation.

Voici quelques exemples d'ordinateurs à exclure de la gestion de l'alimentation :

- Les ordinateurs qui doivent rester allumés.
- Les ordinateurs auxquels des utilisateurs ont besoin de se connecter à l'aide de la connexion Bureau à distance.
- Les ordinateurs qui ne peuvent pas utiliser la gestion de l'alimentation.
- Ordinateurs dotés du rôle de système de site de point de distribution.
- Ordinateurs publics tels que les bornes d'informations, les écrans d'affichage ou les consoles de surveillance pour lesquels l'ordinateur et le moniteur doivent toujours être allumés.

  Pour plus d'informations, consultez Configuration de la gestion de l'alimentation dans System Center Configuration Manager.

## Appliquer d'abord les modes de gestion de l'alimentation à un regroupement test d'ordinateurs

Testez toujours les conséquences liées à l'application d'un mode de gestion de l'alimentation à un regroupement test d'ordinateurs avant d'appliquer le mode d'alimentation à un plus grand regroupement d'ordinateurs.

Les paramètres d'alimentation appliqués aux ordinateurs exécutant Windows XP ou Windows Server 2003 ne sont pas rétablis selon leurs valeurs d'origine, même si vous excluez l'ordinateur de la gestion de l'alimentation. Sur les versions ultérieures de Windows, l'exclusion d'un ordinateur de la gestion de l'alimentation entraîne le rétablissement des valeurs d'origine de tous les paramètres d'alimentation. Il est impossible de rétablir les valeurs d'origine de chaque paramètre d'alimentation.

## Appliquer individuellement les paramètres de mode de gestion de l'alimentation

Surveiller les conséquences liées à l'application de chaque paramètre d'alimentation avant d'appliquer le paramètre suivant pour s'assurer que chaque paramètre a l'effet requis. Pour plus d'informations sur les paramètres du mode de gestion de l'alimentation, consultez Paramètres de mode de gestion de l'alimentation disponibles dans la rubrique Guide pratique pour créer et appliquer des modes de gestion de l'alimentation dans System Center Configuration Manager.

## Surveiller régulièrement les ordinateurs pour voir si plusieurs modes de gestion de l'alimentation leur sont appliqués

La gestion de l'alimentation inclut un rapport qui affiche les ordinateurs auxquels plusieurs modes d'alimentation sont appliqués.

Si un ordinateur est membre de plusieurs regroupements, chacun appliquant des modes de gestion de l'alimentation différents, les actions suivantes sont effectuées :

- Mode de gestion de l'alimentation : si plusieurs valeurs sont appliquées à un ordinateur comme paramètres d'alimentation, la valeur la moins restrictive est utilisée.
- Heure d'éveil : si plusieurs heures d'éveil sont appliquées à un ordinateur de bureau, l'heure la plus proche de minuit est utilisée.

  Pour plus d'informations, consultez Ordinateurs avec plusieurs modes de gestion de l'alimentation dans la rubrique Guide pratique pour surveiller et planifier la gestion de l'alimentation dans System Center Configuration Manager. Pour plus d'informations sur la manière dont la gestion de l'alimentation résout les conflits, consultez Guide pratique pour créer et appliquer des modes de gestion de l'alimentation dans System Center Configuration Manager.

# Enregistrer ou exporter les informations de gestion de l'alimentation pendant la phase de surveillance et de planification de la gestion de l'alimentation

Les informations de gestion de l'alimentation utilisées par les rapports quotidiens sont conservées dans la base de données du site Configuration Manager pendant 31 jours.

Les informations de gestion de l'alimentation utilisées par les rapports mensuels sont conservées dans la base de données du site Configuration Manager pendant 13 mois.

Quand vous exécutez des rapports pendant les phases de surveillance, de planification et de conformité de la gestion de l'alimentation, enregistrez ou exportez les résultats de tous les rapports pour lesquels vous souhaitez conserver les données afin de les comparer ultérieurement au cas où ils seraient ensuite supprimés par Configuration Manager.

# Liste de contrôle de l'administrateur de gestion de l'alimentation dans System Center Configuration Manager

22/06/2018 • 11 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cette liste de vérification de l'administrateur fournit les étapes recommandées pour l'utilisation de la gestion de l'alimentation System Center Configuration Manager au sein de votre organisation.

## Configuration de la gestion de l'alimentation

Suivez ces étapes pour vous aider à configurer votre hiérarchie afin de recueillir des informations sur la gestion de l'alimentation à partir d'ordinateurs client.

> **IMPORTANT**
> N'appliquez pas de modes d'alimentation pour les ordinateurs de votre hiérarchie avant d'avoir recueilli et analysé les données d'alimentation à partir d'ordinateurs client. Si vous appliquez les nouveaux paramètres de gestion de l'alimentation aux ordinateurs sans examiner préalablement les paramètres existants, cela peut entraîner une augmentation de la consommation d'énergie.

| TÂCHE | DÉTAILS |
|---|---|
| Passez en revue les concepts de gestion de l'alimentation dans la bibliothèque de documentation Configuration Manager. | Voir Présentation de la gestion de l'alimentation. |
| Passez en revue les prérequis de la gestion de l'alimentation dans la bibliothèque de documentation Configuration Manager. | Voir Configuration requise pour la gestion de l'alimentation. |
| Passez en revue les meilleures pratiques pour la gestion de l'alimentation. | Voir Bonnes pratiques de gestion de l'alimentation. |
| Configurez vos regroupements pour gérer la consommation électrique des ordinateurs au sein de votre environnement. | Utilisez **Regroupement pour les rapports sur les données de base**, **Regroupement d'ordinateurs ne prenant pas en charge la gestion l'alimentation**, **Regroupements d'ordinateurs auxquels seront appliqués des modes de gestion de l'alimentation** et **Regroupements d'ordinateurs qui exécutent Windows Server** pour gérer les paramètres d'alimentation des ordinateurs dans votre hiérarchie. Vous pouvez créer plusieurs regroupements et appliquer différents modes d'alimentation à chaque regroupement. |
| Activez la gestion de l'alimentation. | Avant de pouvoir commencer à utiliser la gestion de l'alimentation, vous devez l'activer et configurer les paramètres client requis. Pour plus d'informations, voir Configuration de la gestion de l'alimentation. |

| TÂCHE | DÉTAILS |
| --- | --- |
| Recueillez des informations de gestion de l'alimentation à partir d'ordinateurs client. | Les données de gestion de l'alimentation sont communiquées par les clients via l'inventaire matériel Configuration Manager. Selon le calendrier d'inventaire matériel que vous avez configuré, la récupération de l'inventaire depuis tous les ordinateurs client peut prendre un certain temps. |

## Phase de surveillance et de planification

| TÂCHE | DÉTAILS |
| --- | --- |
| Exécutez le rapport **Activité de l'ordinateur**. | Le rapport **Activité de l'ordinateur** affiche un graphique illustrant l'activité du moniteur, de l'ordinateur et de l'utilisateur pour un regroupement spécifique au cours d'une période donnée. Ce rapport est lié au rapport **Détails de l'activité de l'ordinateur** qui affiche les capacités de mise en veille et de mise en éveil des ordinateurs dans le regroupement spécifique. Pour plus d'informations, voir Guide pratique pour surveiller et planifier la gestion de l'alimentation. |
| Exécutez le rapport **Consommation énergétique** ou **Consommation énergétique journalière**. | Les rapports **Consommation énergétique** et **Consommation énergétique journalière** affichent la consommation énergétique mensuelle totale en kilowatts par heure (kWh) pour un regroupement spécifique au cours d'une période donnée. Pour plus d'informations, voir Guide pratique pour surveiller et planifier la gestion de l'alimentation. |
| Exécutez le rapport **Incidence sur l'environnement** ou **Incidence journalière sur l'environnement**. | Les rapports **Incidence sur l'environnement** et **Incidence journalière sur l'environnement** affichent un graphique présentant les émissions de dioxyde de carbone (CO2) enregistrées par un regroupement spécifique d'ordinateurs au cours d'une période donnée. Pour plus d'informations, voir Guide pratique pour surveiller et planifier la gestion de l'alimentation. |
| Exécutez le rapport **Coût énergétique** ou **Coût énergétique journalier**. | Les rapports **Coût énergétique** et **Coût énergétique journalier** affichent le coût de la consommation énergétique totale au cours d'une période donnée. Pour plus d'informations, voir Guide pratique pour surveiller et planifier la gestion de l'alimentation. |
| Exécutez le rapport **Fonctions de gestion de l'alimentation**. | Le rapport **Fonctions de gestion de l'alimentation** affiche les fonctions de gestion de l'alimentation des ordinateurs dans le regroupement spécifique. Pour plus d'informations, voir Guide pratique pour surveiller et planifier la gestion de l'alimentation. |
| Exécutez le rapport **Paramètres d'alimentation**. | Le rapport **Paramètres d'alimentation** affiche une liste agrégée des paramètres d'alimentation actuels utilisés par les ordinateurs d'un regroupement spécifique. Pour plus d'informations, voir Guide pratique pour surveiller et planifier la gestion de l'alimentation. |
| Excluez tous les regroupements d'ordinateurs requis de la gestion de l'alimentation. | Voir Configuration de la gestion de l'alimentation. |

**IMPORTANT**

Veillez à enregistrer les informations provenant des rapports de gestion de l'alimentation générés pendant la phase de planification et de surveillance. Vous pouvez comparer ces données aux informations de gestion de l'alimentation générées pendant les phases de mise en œuvre et de conformité pour vous aider à évaluer les économies à réaliser en matière de consommation énergétique, de coût de l'alimentation et d'incidence sur l'environnement lors de l'application d'un mode d'alimentation aux ordinateurs de votre hiérarchie.

## Phase de mise en œuvre

| TÂCHE | DÉTAILS |
|---|---|
| Sélectionnez les modes d'alimentation existants ou créez de nouveaux modes d'alimentation pour les regroupements d'ordinateurs de votre organisation. | Voir Guide pratique pour créer et appliquer des modes de gestion de l'alimentation. |
| Appliquez ces modes d'alimentation aux ordinateurs. | Voir Guide pratique pour créer et appliquer des modes de gestion de l'alimentation. |

## Phase de compatibilité

| TÂCHE | DÉTAILS |
|---|---|
| Exécutez le rapport **Activité de l'ordinateur**. | Le rapport **Activité de l'ordinateur** affiche un graphique illustrant l'activité du moniteur, de l'ordinateur et de l'utilisateur pour un regroupement spécifique au cours d'une période donnée. Ce rapport est lié au rapport **Détails de l'activité par l'ordinateur** qui affiche les capacités de mise en veille et de mise en éveil des ordinateurs dans le regroupement spécifique. Pour plus d'informations, voir Guide pratique pour surveiller et planifier la gestion de l'alimentation. |
| Exécutez le rapport **Consommation énergétique** ou **Consommation énergétique journalière**. | Les rapports **Consommation énergétique** et **Consommation énergétique journalière** affichent la consommation énergétique mensuelle totale en kilowatts par heure (kWh) pour un regroupement spécifique au cours d'une période donnée. Pour plus d'informations, voir Guide pratique pour surveiller et planifier la gestion de l'alimentation. |
| Exécutez le rapport **Incidence sur l'environnement** ou **Incidence journalière sur l'environnement**. | Les rapports **Incidence sur l'environnement** et **Incidence journalière sur l'environnement** affichent un graphique présentant les émissions de dioxyde de carbone (CO2) enregistrées par un regroupement spécifique d'ordinateurs au cours d'une période donnée. Pour plus d'informations, voir Guide pratique pour surveiller et planifier la gestion de l'alimentation. |
| Exécutez le rapport **Coût énergétique** ou **Coût énergétique journalier**. | Les rapports **Coût énergétique** et **Coût énergétique journalier** affichent le coût de la consommation énergétique totale au cours d'une période donnée. Pour plus d'informations, voir Guide pratique pour surveiller et planifier la gestion de l'alimentation. |

## Résolution des problèmes

| TÂCHE | DÉTAILS |
| --- | --- |
| Si les ordinateurs de votre hiérarchie ne sont pas entrés en veille ou en veille prolongée, exécutez le rapport **Rapport sur la non mise en veille** pour afficher les causes possibles. | Le **Rapport sur la non mise en veille** affiche une liste des causes courantes qui ont empêché les ordinateurs d'entrer en veille ou en veille prolongée et le nombre d'ordinateurs affectés par chaque cause pendant une période spécifique. Pour plus d'informations, voir Guide pratique pour surveiller et planifier la gestion de l'alimentation. |
| Si plusieurs modes d'alimentation sont appliqués à un seul ordinateur, le mode d'alimentation le moins restrictif est appliqué. Exécutez le rapport **Ordinateurs avec plusieurs modes de gestion de l'alimentation** pour afficher les ordinateurs auxquels sont appliqués plusieurs modes d'alimentation. | Voir **Ordinateurs avec plusieurs modes de gestion de l'alimentation** dans Guide pratique pour surveiller et planifier la gestion de l'alimentation. |

# Configuration de la gestion de l'alimentation dans System Center Configuration Manager

22/06/2018 • 6 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Avant de pouvoir utiliser la gestion de l'alimentation dans System Center Configuration Manager, vous devez effectuer les étapes de configuration suivantes.

## Activer et configurer les paramètres client de gestion de l'alimentation

Cette procédure configure les paramètres client par défaut pour la gestion de l'alimentation et s'appliquera à tous les ordinateurs de votre hiérarchie. Si vous souhaitez que ces paramètres s'appliquent uniquement à certains ordinateurs, créez un paramètre client de périphérique personnalisé et affectez-le à un regroupement contenant les ordinateurs pour lesquels vous souhaitez utiliser la gestion de l'alimentation. Pour plus d'informations sur la création de paramètres d'appareil personnalisés, consultez Guide pratique pour configurer les paramètres client dans System Center Configuration Manager.

**Pour activer la gestion de l'alimentation et configurer les paramètres client**

1. Dans la console Configuration Manager, cliquez sur **Administration**.
2. Dans l'espace de travail **Administration** , cliquez sur **Paramètres client**.
3. Cliquez sur **Paramètres client par défaut**.
4. Dans l'onglet **Accueil** , dans le groupe **Propriétés** , cliquez sur **Propriétés**.
5. Dans la boîte de dialogue **Paramètres client par défaut** , cliquez sur **Gestion de l'alimentation**.
6. Configurez la valeur suivante pour les paramètres client de gestion de l'alimentation :
   - **Autoriser la gestion de l'alimentation des périphériques** – Dans la liste déroulante, sélectionnez **Vrai** pour activer la gestion de l'alimentation.
7. Configurez les paramètres client dont vous avez besoin. Pour obtenir la liste des paramètres client de gestion de l'alimentation que vous pouvez configurer, consultez la section Gestion de l'alimentation dans la rubrique À propos des paramètres client dans System Center Configuration Manager.
8. Cliquez sur **OK** pour fermer la boîte de dialogue **Paramètres client par défaut** .

   Les ordinateurs clients sont configurés avec ces paramètres lorsqu'ils téléchargent la stratégie client. Pour lancer la récupération de stratégie pour un client unique, consultez Comment gérer les clients dans System Center Configuration Manager.

## Exclure des ordinateurs de la gestion de l'alimentation

Vous pouvez empêcher les regroupements d'ordinateurs de recevoir les paramètres de gestion de l'alimentation. Si un ordinateur est membre d'un regroupement qui est exclu des paramètres de gestion de l'alimentation, cet ordinateur n'applique pas les paramètres de gestion de l'alimentation, même s'il est membre d'un autre regroupement qui applique les paramètres de gestion de l'alimentation.

Vous pouvez exclure des ordinateurs de la gestion de l'alimentation pour l'une des raisons suivantes :

- Une exigence métier requiert que les ordinateurs soient constamment allumés.

- Vous avez créé un regroupement de contrôle d'ordinateurs sur lesquels vous ne souhaitez pas appliquer les paramètres de gestion de l'alimentation.
- Certains de vos ordinateurs sont incapables d'appliquer des paramètres de gestion de l'alimentation.
- Vous voulez exclure des ordinateurs qui exécutent Windows Server à partir de la gestion de l'alimentation.

> **NOTE**
> Si l'option **Autoriser les utilisateurs à exclure leur périphérique de la gestion de l'alimentation** est configurée dans les paramètres client, les utilisateurs peuvent exclure leurs propres ordinateurs de la gestion de l'alimentation à l'aide du Centre logiciel.

Pour savoir quels ordinateurs ont été exclus de la gestion de l'alimentation, exécutez le rapport **Ordinateurs exclus**. Pour plus d'informations sur ce rapport, consultez Ordinateurs exclus dans Guide pratique pour surveiller et planifier la gestion de l'alimentation dans System Center Configuration Manager.

> **IMPORTANT**
> Les paramètres d'alimentation appliqués aux ordinateurs qui exécutent Windows XP ou Windows Server 2003 ne sont pas rétablis selon leurs valeurs d'origine, même si vous excluez l'ordinateur de la gestion de l'alimentation. Sur les versions ultérieures de Windows, l'exclusion d'un ordinateur de la gestion de l'alimentation entraîne le rétablissement des valeurs d'origine de tous les paramètres d'alimentation. Il est impossible de rétablir les valeurs d'origine de chaque paramètre d'alimentation.

#### Pour exclure un regroupement d'ordinateurs de la gestion de l'alimentation

1. Dans la console Configuration Manager, cliquez sur **Ressources et Conformité**.
2. Dans l'espace de travail **Ressources et Conformité** , cliquez sur **Regroupements de périphériques**.
3. Dans la liste **Regroupements de périphériques** , sélectionnez le regroupement que vous souhaitez exclure de la gestion de l'alimentation, puis, dans l'onglet **Accueil** , dans le groupe **Propriétés** , cliquez sur **Propriétés**.
4. Sous l'onglet **Gestion de l'alimentation** de la boîte de dialogue *Propriétés de <nom_regroupement>*, sélectionnez **Ne jamais appliquer les paramètres de gestion de l'alimentation aux ordinateurs de ce regroupement**.
5. Cliquez sur **OK** pour fermer la boîte de dialogue *Propriétés de <nom_regroupement>* et pour enregistrer vos paramètres.

# Comment créer et appliquer des modes de gestion de l'alimentation dans System Center Configuration Manager

22/06/2018 • 15 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

La gestion de l'alimentation dans System Center Configuration Manager vous permet d'appliquer les modes de gestion de l'alimentation fournis avec Configuration Manager à des regroupements d'ordinateurs de votre hiérarchie, ou de créer vos propres modes de gestion de l'alimentation personnalisés. Procédez comme indiqué dans cette rubrique pour appliquer un mode d'alimentation intégré ou personnalisé aux ordinateurs.

> **IMPORTANT**
> Vous pouvez uniquement appliquer les modes de gestion de l'alimentation Configuration Manager à des regroupements d'appareils.

Si un ordinateur est membre de plusieurs regroupements, chacun appliquant des modes de gestion de l'alimentation différents, les actions suivantes sont effectuées :

- Mode de gestion de l'alimentation : si plusieurs valeurs sont appliquées à un ordinateur en tant que paramètres d'alimentation, la valeur la moins restrictive est utilisée.
- Heure de sortie de veille : si plusieurs heures d'éveil sont appliquées à un ordinateur de bureau, l'heure la plus proche de minuit est utilisée.

  Utilisez le rapport **Ordinateurs avec plusieurs modes de gestion de l'alimentation** pour afficher tous les ordinateurs auxquels sont appliqués plusieurs modes d'alimentation. Cela peut vous aider à détecter les ordinateurs qui présentent des conflits de l'alimentation. Pour plus d'informations sur les rapports de gestion de l'alimentation, consultez Comment surveiller et planifier la gestion de l'alimentation dans System Center Configuration Manager.

> **IMPORTANT**
> Les paramètres d'alimentation configurés à l'aide de la stratégie de groupe Windows remplacent les paramètres configurés par la gestion de l'alimentation Configuration Manager.

Procédez comme suit pour créer et appliquer un mode de gestion de l'alimentation Configuration Manager.

**Pour créer et appliquer un mode d'alimentation**

1. Dans la console Configuration Manager, cliquez sur **Ressources et Conformité**.
2. Dans l'espace de travail **Ressources et Conformité** , cliquez sur **Regroupements de périphériques**.
3. Dans la liste **Regroupements de périphériques** , cliquez sur le regroupement auquel vous souhaitez appliquer les paramètres de gestion de l'alimentation, puis, dans l'onglet **Accueil** , dans le groupe **Propriétés** , cliquez sur **Propriétés**.
4. Sous l'onglet **Gestion de l'alimentation** de la boîte de dialogue *Propriétés de <nom_regroupement>*, sélectionnez **Spécifier les paramètres de gestion de l'alimentation de ce regroupement**.

> **NOTE**
> Vous pouvez également cliquer sur **Parcourir** , puis copier les paramètres de gestion de l'alimentation à partir d'un regroupement sélectionné vers le regroupement sélectionné.

5. Dans les champs **Début** et **Fin** , spécifiez l'heure de début et l'heure de fin des heures de pointe (ou de bureau).

6. Activez **Heure de reprise (ordinateurs de bureau)** pour indiquer une heure de sortie du mode veille ou du mode veille prolongée d'un ordinateur de bureau afin d'installer des mises à jour planifiées ou des logiciels.

   > **IMPORTANT**
   > La gestion de l'alimentation utilise la fonction d'heure de reprise Windows interne pour sortir les ordinateurs du mode veille ou du mode veille prolongée. Les paramètres de l'heure de sortie de veille ne sont pas appliqués aux ordinateurs portables afin d'éviter qu'ils ne sortent de veille alors qu'ils ne sont pas branchés. L'heure de sortie de veille est aléatoire et les ordinateurs peuvent sortir de veille pendant une heure à partir de l'heure de sortie de veille spécifiée.

7. Si vous souhaitez configurer un mode d'alimentation personnalisé pour les heures de pointe (ou de bureau), sélectionnez **Pic personnalisé (ConfigMgr)** dans la liste déroulante **Mode forte alimentation** , puis cliquez sur **Modifier**. Si vous souhaitez configurer un mode d'alimentation pour les heures creuses, sélectionnez **Non-pic personnalisé (ConfigMgr)** dans la liste déroulante **Faible alimentation** , puis cliquez sur **Modifier**.

   > **NOTE**
   > Vous pouvez utiliser le rapport **Activité de l'ordinateur** pour vous aider à déterminer les planifications à utiliser pour les heures de pointe et les heures creuses lorsque vous appliquez des modes d'alimentation à des regroupements d'ordinateurs. Pour plus d'informations, consultez Guide pratique pour surveiller et planifier la gestion de l'alimentation dans System Center Configuration Manager.

   Vous pouvez également sélectionner dans les modes d'alimentation intégrés, **Équilibré (ConfigMgr)**, **Hautes performances (ConfigMgr)** ou **Économiseur d'énergie (ConfigMgr)**, puis cliquer sur **Afficher** pour afficher les propriétés de chaque mode d'alimentation.

   > **NOTE**
   > Vous ne pouvez pas modifier les modes d'alimentation intégrés.

8. Dans la boîte de dialogue *Propriétés de <nom_mode_gestion_alimentation>*, configurez les paramètres suivants :

   - **Nom** : spécifiez un nom pour ce mode de gestion de l'alimentation ou utilisez la valeur par défaut fournie.
   - **Description** : spécifiez une description pour ce mode de gestion de l'alimentation ou utilisez la valeur par défaut fournie.
   - **Spécifier les propriétés pour ce mode d'alimentation** : configurez les propriétés du mode de gestion de l'alimentation. Pour désactiver une propriété, désactivez sa case. Pour plus d'informations sur les paramètres disponibles, consultez Paramètres du mode de gestion de

l'alimentation disponibles dans cette rubrique.

> **IMPORTANT**
> Les paramètres activés sont appliqués aux ordinateurs lorsque le mode d'alimentation est appliqué. Si vous désactivez une case à cocher du paramètre d'alimentation, la valeur sur l'ordinateur client n'est pas modifiée lorsque le mode d'alimentation est appliqué. Le fait de désactiver une case ne permet pas de restaurer la valeur du paramètre d'alimentation sélectionnée avant l'application d'un mode d'alimentation.

9. Cliquez sur **OK** pour fermer la boîte de dialogue *Propriétés de <nom_mode_gestion_alimentation>*.
10. Cliquez sur **OK** pour fermer la boîte de dialogue *Paramètres de <nom_regroupement>* et pour appliquer le mode de gestion de l'alimentation.

## Available power management plan settings

Le tableau suivant répertorie les paramètres de gestion de l'alimentation disponibles dans Configuration Manager. Vous pouvez configurer d'autres paramètres pour les périodes où l'ordinateur est branché ou sur batterie. Selon la version de Windows que vous utilisez, il est possible que certains paramètres ne soient pas configurables.

> **NOTE**
> Les paramètres d'alimentation que vous ne configurez pas conservent leur valeur actuelle sur les ordinateurs clients.

| NOM | DESCRIPTION |
|---|---|
| **Désactiver l'affichage après (minutes)** | Spécifie la durée en minutes, pendant laquelle l'ordinateur doit être inactif avant que l'affichage ne soit désactivé. Spécifiez une valeur **0** si vous ne voulez pas que la gestion de l'alimentation désactive l'affichage. |
| **Mise en veille après (minutes)** | Spécifie la durée en minutes, pendant laquelle l'ordinateur doit être inactif avant d'entrer en mode veille. Spécifiez une valeur **0** si vous ne voulez pas que la gestion de l'alimentation passe l'ordinateur en mode veille. |
| **Demander un mot de passe à la reprise** | Une valeur **Oui** ou **Non** spécifie si un mot de passe est nécessaire pour déverrouiller l'ordinateur lorsqu'il sort du mode veille. |
| **Action du bouton d'alimentation** | Spécifie l'action qui est effectuée lorsque l'utilisateur appuie sur le bouton d'alimentation. Spécifie l'action qui se produit lorsque l'utilisateur ferme le capot d'un ordinateur portable. Valeurs possibles **Ne rien faire**, **Mettre en veille**, **Mettre en veille prolongée** et **Arrêter**. |
| **Bouton de mise sous tension du menu Démarrer** | Spécifie l'action qui se produit quand vous appuyez sur le bouton d'alimentation du menu **Démarrer** de l'ordinateur. Spécifie l'action qui se produit lorsque l'utilisateur ferme le capot d'un ordinateur portable. Valeurs possibles **Mettre en veille**, **Mettre en veille prolongée** et **Arrêter**. |

| NOM | DESCRIPTION |
| --- | --- |
| **Action du bouton de mise en veille** | Spécifie l'action qui se produit quand vous appuyez sur le bouton de **mise en veille** de l'ordinateur. Spécifie l'action qui se produit lorsque l'utilisateur ferme le capot d'un ordinateur portable. Valeurs possibles **Ne rien faire**, **Mettre en veille**, **Mettre en veille prolongée** et **Arrêter**. |
| **Action à la fermeture du capot** | Spécifie l'action qui se produit lorsque l'utilisateur ferme le capot d'un ordinateur portable. Valeurs possibles **Ne rien faire**, **Mettre en veille**, **Mettre en veille prolongée** et **Arrêter**. |
| **Désactiver le disque dur après (minutes)** | Spécifie la durée en minutes, pendant laquelle le disque dur doit être inactif avant d'être désactivé. Spécifiez une valeur **0** si vous ne voulez pas que la gestion de l'alimentation mette hors tension le disque dur de l'ordinateur. |
| **Mise en veille prolongée après (minutes)** | Spécifie la durée en minutes, pendant laquelle l'ordinateur doit être inactif avant d'entrer en veille prolongée. Spécifiez une valeur **0** si vous ne voulez pas que la gestion de l'alimentation mette l'ordinateur en veille prolongée. |
| **Action sur batterie faible** | Spécifie l'action qui se produit lorsque la batterie de l'ordinateur atteint le niveau de notification de batterie faible spécifié. Spécifie l'action qui se produit lorsque l'utilisateur ferme le capot d'un ordinateur portable. Valeurs possibles **Ne rien faire**, **Mettre en veille**, **Mettre en veille prolongée** et **Arrêter**. |
| **Action sur batterie critique** | Spécifie l'action qui est effectuée lorsque la batterie de l'ordinateur atteint le niveau de notification de batterie critique spécifié. Spécifie l'action qui se produit lorsque l'utilisateur ferme le capot d'un ordinateur portable. Les valeurs possibles incluent **Mettre en veille**, **Mettre en veille prolongée** et **Arrêter**. |
| **Autoriser la veille hybride** | La sélection de la valeur **Activé** ou **Désactivé** spécifie si Windows doit enregistrer un fichier de mise en veille prolongée lors de l'entrée en mode veille, qui peut être utilisé pour restaurer l'état de l'ordinateur en cas de perte d'alimentation alors qu'il est en veille.<br><br>La mise en veille hybride est conçue pour les ordinateurs de bureau et, par défaut, n'est pas activée sur les ordinateurs portables. Sur les ordinateurs qui exécutent Windows 7, la mise en veille hybride désactive la fonctionnalité de mise en veille prolongée. |
| **Autoriser l'état d'attente lors de l'action de mise en veille** | La sélection de la valeur **Activé** ou **Désactivé** permet à l'ordinateur de se mettre en attente, ce qui consomme toujours du courant, mais permet à l'ordinateur de sortir plus rapidement du mode veille. Si ce paramètre a la valeur **Désactivé**, l'ordinateur peut uniquement être mis en veille prolongée ou mis hors tension. |
| **Inactivité requise avant la mise en veille (%)** | Spécifie le pourcentage de temps d'inactivité du temps processeur nécessaire à l'ordinateur pour entrer en mode veille. Sur les ordinateurs qui exécutent Windows 7, cette valeur est toujours définie sur **0**. |

| NOM | DESCRIPTION |
| --- | --- |
| **Activer le minuteur de réveil Windows pour les ordinateurs de bureau** | La sélection de la valeur **Activer** ou **Désactiver** peut permettre à la gestion de l'alimentation d'utiliser l'horloge Windows intégrée pour sortir un ordinateur de bureau du mode veille. Lorsqu'un ordinateur de bureau quitte le mode veille grâce au minuteur de réveil Windows, il reste actif pendant 10 minutes par défaut afin de laisser le temps à l'ordinateur d'installer toutes les mises à jour ou de recevoir la stratégie.<br><br>Les minuteurs de réveil ne sont pas pris en charge sur les ordinateurs portables afin d'éviter les scénarios dans lesquels ils pourraient se mettre en éveil lorsqu'ils ne sont pas branchés. |

# Comment surveiller et planifier la gestion de l'alimentation dans System Center Configuration Manager

22/06/2018 • 68 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Utilisez les informations suivantes pour mieux surveiller et planifier la gestion de l'alimentation dans System Center Configuration Manager.

## Comment utiliser les rapports de gestion de l'alimentation

La gestion de l'alimentation dans Configuration Manager comprend plusieurs rapports permettant d'analyser la consommation énergétique et les paramètres d'alimentation des ordinateurs de votre organisation. Les rapports peuvent également servir à résoudre des problèmes.

Pour pouvoir utiliser les rapports de gestion de l'alimentation, vous devez configurer des rapports pour votre hiérarchie. Pour plus d'informations sur la création de rapports dans Configuration Manager, consultez Génération de rapports dans System Center Configuration Manager.

> **NOTE**
> Les informations de gestion de l'alimentation utilisées par les rapports quotidiens sont conservées dans la base de données du site Configuration Manager pendant 31 jours.
> Les informations de gestion de l'alimentation utilisées par les rapports mensuels sont conservées dans la base de données du site Configuration Manager pendant 13 mois.
>
> Quand vous exécutez des rapports pendant les phases de surveillance, de planification et de conformité de la gestion de l'alimentation, enregistrez ou exportez les résultats de tous les rapports pour lesquels vous souhaitez conserver les données afin de les comparer ultérieurement au cas où ils seraient ensuite supprimés par Configuration Manager.

## Liste des rapports de gestion de l'alimentation

La liste ci-dessous répertorie les rapports de gestion de l'alimentation disponibles dans Configuration Manager.

> **NOTE**
> Les rapports de gestion de l'alimentation indiquent le nombre d'ordinateurs physiques et le nombre d'ordinateurs virtuels dans un regroupement sélectionné. Toutefois, seules les informations de gestion de l'alimentation des ordinateurs physiques sont affichées dans les rapports de gestion de l'alimentation.

**Rapport Activité de l'ordinateur**

Le rapport **Activité de l'ordinateur** affiche un graphique indiquant l'activité suivante pour un regroupement spécifié sur une période donnée :

- **Ordinateur allumé** : l'ordinateur a été mis sous tension.

- **Moniteur allumé** : l'écran a été mis sous tension.
- **Utilisateur actif** : une activité a été détectée au niveau de la souris ou du clavier de l'ordinateur ou d'une connexion Bureau à distance à l'ordinateur.

  Ce rapport est utilisé pendant les phases de surveillance, de planification et d'application pour comprendre le parallèle entre l'activité de l'ordinateur, l'activité de l'écran et l'activité de l'utilisateur pendant une période de 24 heures. Si vous exécutez le rapport sur un nombre de jours, les données sont agrégées pour cette période. Ce rapport peut vous aider à déterminer les heures d'activité (de pointe) et les heures d'inactivité (heures creuses) types pour le regroupement sélectionné pour déterminer quand il est nécessaire d'appliquer les modes de gestion d'alimentation configurés.

  Le graphique indique les périodes au cours desquelles un ordinateur peut être allumé sans aucune activité de l'utilisateur. Pensez à appliquer des paramètres d'alimentation plus restrictifs durant ces périodes pour réduire les coûts d'électricité des ordinateurs qui sont sous tension, mais pas utilisés. Un ordinateur est considéré actif s'il existe une activité d'ordinateur, d'utilisateur ou de surveillance pendant au moins une minute pour une heure donnée sur le graphique. Si un ordinateur ne signale pas de données de gestion de l'alimentation, il ne figure pas dans le rapport **Activité de l'ordinateur** .

  Utilisez les paramètres suivants pour configurer ce rapport.

#### Paramètres de rapport obligatoires

Les paramètres suivants doivent être spécifiés pour exécuter ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Date de début** | Dans la liste déroulante, sélectionnez la date de début du rapport. |
| **Date de fin (facultative)** | Dans la liste déroulante, sélectionnez la date de fin facultative du rapport. |
| **Nom du regroupement** | Dans la liste déroulante, sélectionnez le regroupement à utiliser pour ce rapport. |
| **Type d'appareil** | Dans la liste déroulante, sélectionnez le type d'ordinateur pour lequel vous souhaitez obtenir un rapport. Les valeurs valides sont **Tout** (ordinateurs portables et postes de travail), **Bureau** (postes de travail uniquement) et **Ordinateur portable** (ordinateurs portables uniquement). |

#### Paramètres de rapport masqués

Ce rapport n'a aucun paramètre masqué que vous pouvez définir.

#### Liens de rapports

Si vous ne définissez aucune **date de fin (facultative)** , le rapport contient un lien vers le rapport suivant qui fournit des informations complémentaires.

| NOM DU RAPPORT | DÉTAILS |
|---|---|

| NOM DU RAPPORT | DÉTAILS |
| --- | --- |
| **Détails de l'activité de l'ordinateur** | Cliquez sur le lien **Cliquez pour obtenir des informations détaillées** pour afficher la liste des ordinateurs actifs, inactifs et qui n'envoient aucune donnée pour la date spécifiée.<br><br>Pour plus d'informations, consultez Computer Activity Details Report dans cette rubrique. |

### Rapport Activité par ordinateur

Le rapport **Activité par ordinateur** contient un graphique qui indique l'activité suivante pour un ordinateur spécifié à une date donnée :

- **Ordinateur allumé** : l'ordinateur a été mis sous tension.
- **Moniteur allumé** : l'écran a été mis sous tension.
- **Utilisateur actif** : une activité a été détectée au niveau de la souris ou du clavier de l'ordinateur ou d'une connexion Bureau à distance à l'ordinateur.

  Ce rapport peut être exécuté indépendamment ou appelé par le rapport **Détails de l'activité de l'ordinateur** .

> **NOTE**
> Les informations sur l'activité des ordinateurs sont collectées depuis les ordinateurs clients durant l'inventaire matériel. L'activité pendant un mode de faible ou de forte alimentation appliqué peut être collectée, selon le moment où l'inventaire matériel est exécuté.

Utilisez les paramètres suivants pour configurer ce rapport.

#### Paramètres de rapport obligatoires

Les paramètres suivants doivent être spécifiés pour exécuter ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
| --- | --- |
| **Date du rapport** | Dans la liste déroulante, sélectionnez une date pour ce rapport. |
| **Nom de l'ordinateur** | Entrez le nom de l'ordinateur pour lequel vous souhaitez obtenir un rapport. |

#### Paramètres de rapport masqués

Ce rapport n'a aucun paramètre masqué que vous pouvez définir.

#### Liens de rapports

Ce rapport contient des liens vers le rapport suivant qui fournit des informations supplémentaires sur l'élément sélectionné.

| NOM DU RAPPORT | DÉTAILS |
| --- | --- |
| **Détails de l'ordinateur** | Cliquez sur le lien **Cliquez pour obtenir des informations détaillées** pour afficher les fonctions de gestion de l'alimentation, les paramètres d'alimentation et les modes d'alimentation appliqués de l'ordinateur sélectionné. |

### Computer Activity Details report

Le rapport **Détails de l'activité de l'ordinateur** contient la liste des ordinateurs actifs ou inactifs avec leurs fonctions de veille et de sortie de veille. Ce rapport est appelé par le Computer Activity Report et il n'est pas destiné à être exécuté directement par l'administrateur du site.

Utilisez les paramètres suivants pour configurer ce rapport.

#### Paramètres de rapport obligatoires

Les paramètres suivants doivent être spécifiés pour exécuter ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Nom du regroupement** | Dans la liste déroulante, sélectionnez le regroupement à utiliser pour ce rapport. |
| **Date du rapport** | Dans la liste déroulante, sélectionnez une date à utiliser pour ce rapport. |
| **Heure du rapport** | Dans la liste déroulante, sélectionnez une heure pour la date définie pour laquelle vous souhaitez exécuter ce rapport . Les valeurs valides sont comprises entre **0 h 00** et **23 h 00**. |
| **État de l'ordinateur** | Dans la liste déroulante, sélectionnez l'état de l'ordinateur pour lequel vous souhaitez exécuter ce rapport. Les valeurs valides sont **Tout** (ordinateurs mis sous tension ou hors tension), **Activé** (ordinateurs mis sous tension) et **Désactivé** (ordinateurs mis hors tension, en veille ou en veille prolongée). Ces valeurs sont retournées uniquement pour la période de création de rapports sélectionnée. |
| **Type d'appareil** | Dans la liste déroulante, sélectionnez le type d'ordinateur pour lequel vous souhaitez obtenir un rapport. Les valeurs valides sont **Tout** (ordinateurs portables et postes de travail), **Bureau** (postes de travail uniquement) et **Ordinateur portable** (ordinateurs portables uniquement). Ces valeurs sont retournées uniquement pour la période de création de rapports sélectionnée. |
| **Compatible avec le mode veille** | Dans la liste déroulante, indiquez si vous souhaitez afficher les ordinateurs compatibles avec le mode veille dans le rapport. Les valeurs valides sont **Tout** (ordinateurs aptes et inaptes à être mis en veille), **Non** (ordinateurs inaptes à être mis en veille) et **Oui** (ordinateurs aptes à être mis en veille). |
| **Compatible avec la sortie de veille** | Dans la liste déroulante, indiquez si vous souhaitez afficher les ordinateurs compatibles avec le mode de sortie de veille dans le rapport. Les valeurs valides sont **Tout** (ordinateurs aptes et inaptes à sortir de veille), **Non** (ordinateurs inaptes à sortir de veille) et **Oui** (ordinateurs aptes à sortir de veille). |

| NOM DU PARAMÈTRE | DESCRIPTION |
| --- | --- |
| **Gestion de l'alimentation** | Dans la liste déroulante, sélectionnez les types de modes d'alimentation à afficher dans le rapport. Les valeurs valides sont **Tout** (ordinateurs auxquels aucun mode de gestion de l'alimentation ne s'applique ; ordinateurs auxquels un mode de gestion de l'alimentation s'applique ; ordinateurs exclus de la gestion de l'alimentation), **Non spécifié** (ordinateurs auxquels aucun mode de gestion de l'alimentation ne s'applique), **Défini** (ordinateurs auxquels un mode de gestion de l'alimentation s'applique) et **Exclu** (ordinateurs exclus de la gestion de l'alimentation). |
| **Système d'exploitation** | Dans la liste déroulante, sélectionnez les systèmes d'exploitation à afficher dans le rapport ou sélectionnez **Tout** pour afficher tous les systèmes d'exploitation. |

#### Paramètres de rapport masqués

Ce rapport n'a aucun paramètre masqué que vous pouvez définir.

#### Liens de rapports

Ce rapport contient des liens vers le rapport suivant qui fournit des informations supplémentaires sur l'élément sélectionné.

| NOM DU RAPPORT | DÉTAILS |
| --- | --- |
| **Activité par ordinateur** | Cliquez sur un nom d'ordinateur pour voir l'activité spécifique pour cet ordinateur sur une période de création de rapports choisie. Ces activités incluent **Ordinateur allumé** (l'ordinateur a-t-il été allumé ?), **Moniteur allumé** (le moniteur a-t-il été allumé ?) et **Utilisateur actif** (une activité a été détectée à partir de la souris, du clavier ou d'une connexion Bureau à distance de l'ordinateur).<br><br>Pour plus d'informations, consultez Computer Activity by Computer Report dans cette rubrique. |

### Rapport Détails de l'ordinateur

Le rapport **Détails de l'ordinateur** affiche des informations détaillées sur les fonctions de gestion de l'alimentation, les paramètres d'alimentation et les modes d'alimentation appliqués à un ordinateur spécifié. Ce rapport est appelé par le rapport **Activité par ordinateur** , le rapport **Ordinateurs avec plusieurs modes de gestion de l'alimentation** , le rapport **Fonctions de gestion de l'alimentation** et le rapport **Détails des paramètres du mode de gestion de l'alimentation** . Il n'est pas destiné à être exécuté directement par l'administrateur du site.

#### Paramètres de rapport obligatoires

Les paramètres suivants doivent être spécifiés pour exécuter ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
| --- | --- |
| **Nom de l'ordinateur** | Entrez le nom de l'ordinateur pour lequel vous souhaitez obtenir un rapport. |

| NOM DU PARAMÈTRE | DESCRIPTION |
| --- | --- |
| **Mode d'alimentation** | Dans la liste déroulante, sélectionnez le type de paramètres d'alimentation à afficher dans les résultats du rapport. Sélectionnez **Sur secteur** pour afficher les paramètres d'alimentation configurés quand l'ordinateur est branché sur secteur et **Sur batterie** pour afficher les paramètres d'alimentation configurés quand l'ordinateur fonctionne sur batterie. |

**Paramètres de rapport masqués**

Ce rapport ne dispose pas de paramètres masqués que vous pouvez définir.

**Liens de rapports**

Ce rapport n'établit pas de liaison à d'autres rapports de gestion de l'alimentation.

### Rapport Pas de rapport détaillé pour l'ordinateur

Le rapport **Pas de rapport détaillé pour l'ordinateur** affiche la liste des ordinateurs dans un regroupement spécifique qui n'ont pas signalé d'activité d'alimentation à une date et une heure données. Ce rapport est appelé par le **Computer Activity Report** et il n'est pas destiné à être exécuté directement par l'administrateur du site.

> **NOTE**
> Les ordinateurs envoient les informations de gestion de l'alimentation dans le cadre de leur calendrier d'inventaire matériel. Avant de conclure qu'un ordinateur n'envoie pas d'informations, vérifiez qu'il a signalé un inventaire matériel.

Utilisez les paramètres suivants pour configurer ce rapport.

**Paramètres de rapport obligatoires**

Les paramètres suivants doivent être spécifiés pour exécuter ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
| --- | --- |
| **Nom du regroupement** | Dans la liste déroulante, sélectionnez le regroupement à utiliser pour ce rapport. |
| **Date du rapport** | Dans la liste déroulante, sélectionnez une date pour ce rapport. |
| **Heure du rapport** | Dans la liste déroulante, sélectionnez une heure pour la date définie pour laquelle vous souhaitez exécuter ce rapport . Les valeurs valides sont comprises entre **0 h 00** et **23 h 00**. |
| **Type d'appareil** | Dans la liste déroulante, sélectionnez le type d'ordinateur pour lequel vous souhaitez obtenir un rapport. Les valeurs valides sont **Tout** (ordinateurs portables et postes de travail), **Bureau** (postes de travail uniquement) et **Ordinateur portable** (ordinateurs portables uniquement). Ces valeurs sont retournées uniquement pour la période de création de rapports sélectionnée. |

**Paramètres de rapport masqués**

Ce rapport n'a aucun paramètre masqué que vous pouvez définir.

**Liens de rapports**

Ce rapport n'établit pas de liaison à d'autres rapports de gestion de l'alimentation.

### Ordinateurs exclus

Le rapport **Ordinateurs exclus** affiche la liste des ordinateurs d'un regroupement qui ont été exclus de la gestion d'alimentation Configuration Manager.

Utilisez les paramètres suivants pour configurer ce rapport.

#### Paramètres de rapport obligatoires

Les paramètres suivants doivent être spécifiés pour exécuter ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Regroupement** | Dans la liste déroulante, sélectionnez un regroupement pour ce rapport. |
| **Raison** | Dans la liste déroulante, sélectionnez la raison pour laquelle les ordinateurs ont été exclus de la gestion de l'alimentation. Vous pouvez afficher **Tout** (tous les ordinateurs exclus), **Exclusion par l'administrateur** (seuls les ordinateurs qui ont été exclus par un utilisateur administratif) et **Exclusion par l'utilisateur** (seuls les ordinateurs qui ont été exclus par un utilisateur du Centre logiciel). |

#### Paramètres de rapport masqués

Ce rapport n'a aucun paramètre masqué que vous pouvez définir.

#### Liens de rapports

Ce rapport contient des liens vers le rapport suivant qui fournit des informations supplémentaires sur l'élément sélectionné.

| NOM DU RAPPORT | DÉTAILS |
|---|---|
| **Détails de l'ordinateur** | Cliquez sur un nom d'ordinateur pour afficher les fonctions de gestion de l'alimentation, les paramètres d'alimentation et les modes de gestion de l'alimentation appliqués à l'ordinateur sélectionné.<br><br>Pour plus d'informations, consultez Computer Details Report dans cette rubrique. |

### Ordinateurs avec plusieurs modes de gestion de l'alimentation

Le rapport **Ordinateurs avec plusieurs modes de gestion de l'alimentation** affiche la liste des ordinateurs qui sont membres de plusieurs regroupements, chacun appliquant des modes différents de gestion de l'alimentation. Pour chaque ordinateur ayant potentiellement des paramètres d'alimentation conflictuels, le rapport indique le nom de l'ordinateur et les modes de gestion de l'alimentation appliqués pour chaque regroupement dont l'ordinateur est membre.

> **IMPORTANT**
>
> Si un ordinateur est membre de plusieurs regroupements et que chaque regroupement a un mode de gestion de l'alimentation différent, le mode de gestion de l'alimentation le moins restrictif s'applique.
>
> Si un ordinateur est membre de plusieurs regroupements et que chaque regroupement a une heure de mise en éveil différente, l'heure la plus proche de minuit est utilisée.

Utilisez les paramètres suivants pour configurer ce rapport.

#### Paramètres de rapport obligatoires

Les paramètres suivants doivent être spécifiés pour exécuter ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Nom du regroupement** | Dans la liste déroulante, sélectionnez un regroupement pour ce rapport. |

#### Paramètres de rapport masqués

Ce rapport n'a aucun paramètre masqué que vous pouvez définir.

#### Liens de rapports

Ce rapport contient des liens vers le rapport suivant qui fournit des informations supplémentaires sur l'élément sélectionné.

| NOM DU RAPPORT | DÉTAILS |
|---|---|
| **Détails de l'ordinateur** | Cliquez sur un nom d'ordinateur pour afficher les fonctions de gestion de l'alimentation, les paramètres d'alimentation et les modes de gestion de l'alimentation appliqués à l'ordinateur sélectionné.<br><br>Pour plus d'informations, consultez Computer Details Report dans cette rubrique. |

### Rapport Consommation énergétique

Le rapport **Consommation énergétique** affiche les informations suivantes :

- Un graphique indiquant la consommation électrique mensuelle totale des ordinateurs, exprimée en kilowatts/heure (kWh) dans le regroupement spécifié pour la période indiquée.
- Un graphique indiquant la consommation électrique moyenne, exprimée en kilowatts/heure (kWh) de chaque ordinateur dans le regroupement spécifié pour la période indiquée.
- Un tableau montrant la consommation électrique mensuelle totale, exprimée en kilowatts/heure (kWh) et la consommation électrique moyenne des ordinateurs du regroupement spécifié pour la période indiquée.

  Ces informations peuvent être utilisées pour comprendre les tendances de consommation électrique dans votre environnement. Après avoir appliqué un mode d'alimentation aux ordinateurs du regroupement sélectionné, la consommation électrique des ordinateurs doit diminuer.

> **NOTE**
> Si vous ajoutez ou supprimez des membres dans le regroupement après avoir appliqué un mode d'alimentation, les résultats du rapport **Consommation énergétique** changent et peuvent compliquer la comparaison des résultats des phases de surveillance et de planification et de la phase d'application.

Utilisez les paramètres suivants pour configurer ce rapport.

#### Paramètres de rapport obligatoires

Les paramètres suivants doivent être spécifiés pour exécuter ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Date de début** | Dans la liste déroulante, sélectionnez la date de début du rapport. |
| **Date de fin** | Dans la liste déroulante, sélectionnez la date de fin du rapport. |
| **Nom du regroupement** | Dans la liste déroulante, sélectionnez un regroupement pour ce rapport. |
| **Type d'appareil** | Dans la liste déroulante, sélectionnez le type d'ordinateur pour lequel vous souhaitez obtenir un rapport. Les valeurs valides sont **Tout** (ordinateurs portables et postes de travail), **Bureau** (postes de travail uniquement) et **Ordinateur portable** (ordinateurs portables uniquement). Ces valeurs sont retournées uniquement pour la période de création de rapports sélectionnée. |

**Paramètres de rapport masqués**

Vous pouvez également indiquer les paramètres masqués suivants pour modifier le comportement de ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Ordinateur de bureau allumé** | Spécifiez la consommation électrique d'un ordinateur de bureau lorsqu'il est allumé. La valeur par défaut est **0,07** kWh. |
| **Ordinateur portable allumé** | Spécifiez la consommation électrique d'un ordinateur portable lorsqu'il est allumé. La valeur par défaut est **0,02** kWh. |
| **Ordinateur de bureau en veille** | Spécifiez la consommation électrique d'un ordinateur de bureau qui est entré en mode veille. La valeur par défaut est **0,003** kWh. |
| **Ordinateur portable en veille** | Spécifiez la consommation électrique d'un ordinateur portable qui est entré en mode veille. La valeur par défaut est **0,001** kWh. |
| **Ordinateur de bureau éteint** | Spécifiez la consommation électrique d'un ordinateur de bureau lorsqu'il est éteint. La valeur par défaut est **0** kWh. |
| **Ordinateur portable éteint** | Spécifiez la consommation électrique d'un ordinateur portable lorsqu'il est éteint. La valeur par défaut est **0** kWh. |
| **Moniteur d'ordinateur de bureau allumé** | Spécifiez la consommation électrique d'un moniteur d'ordinateur de bureau lorsqu'il est allumé. La valeur par défaut est **0,028** kWh. |
| **Moniteur d'ordinateur portable allumé** | Spécifiez la consommation électrique d'un moniteur d'ordinateur portable lorsqu'il est allumé. La valeur par défaut est **0** kWh. |

**Liens de rapports**

Ce rapport n'établit pas de liaison à d'autres rapports de gestion de l'alimentation.

### Rapport Consommation énergétique journalière

Le rapport **Consommation énergétique journalière** affiche les informations suivantes :

- Un graphique indiquant la consommation électrique journalière totale des ordinateurs, exprimée en kilowatts/heure (kWh), dans le regroupement spécifié pour les 31 derniers jours.
- Un graphique indiquant la consommation électrique quotidienne moyenne en kilowatts/heure (kWh) de chaque ordinateur du regroupement spécifié au cours des 31 derniers jours.
- Un tableau indiquant la consommation électrique quotidienne totale en kilowatts/heure (kWh) et la consommation électrique quotidienne moyenne des ordinateurs du regroupement spécifié pour les 31 derniers jours.

  Ces informations peuvent être utilisées pour comprendre les tendances de consommation électrique dans votre environnement. Après avoir appliqué un mode d'alimentation aux ordinateurs du regroupement sélectionné, la consommation électrique des ordinateurs doit diminuer.

> **NOTE**
> Si vous ajoutez ou supprimez des membres dans le regroupement après avoir appliqué un mode d'alimentation, les résultats du rapport **Consommation énergétique** changent et peuvent compliquer la comparaison des résultats des phases de surveillance et de planification et de la phase d'application.

Utilisez les paramètres suivants pour configurer ce rapport.

#### Paramètres de rapport obligatoires

Les paramètres suivants doivent être spécifiés pour exécuter ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Regroupement** | Dans la liste déroulante, sélectionnez un regroupement pour ce rapport. |
| **Device Type** | Dans la liste déroulante, sélectionnez le type d'ordinateur pour lequel vous souhaitez obtenir un rapport. Les valeurs valides sont **Tout** (ordinateurs portables et postes de travail), **Bureau** (postes de travail uniquement) et **Ordinateur portable** (ordinateurs portables uniquement). Ces valeurs sont retournées uniquement pour la période de création de rapports sélectionnée. |

#### Paramètres de rapport masqués

Vous pouvez également indiquer les paramètres masqués suivants pour modifier le comportement de ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Ordinateur de bureau allumé** | Spécifiez la consommation électrique d'un ordinateur de bureau lorsqu'il est allumé. La valeur par défaut est **0,07** kWh. |
| **Ordinateur portable allumé** | Spécifiez la consommation électrique d'un ordinateur portable lorsqu'il est allumé. La valeur par défaut est **0,02** kWh. |

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Ordinateur de bureau en veille** | Spécifiez la consommation électrique d'un ordinateur de bureau qui est entré en mode veille. La valeur par défaut est **0,003** kWh. |
| **Ordinateur portable en veille** | Spécifiez la consommation électrique d'un ordinateur portable qui est entré en mode veille. La valeur par défaut est **0,001** kWh. |
| **Ordinateur de bureau éteint** | Spécifiez la consommation électrique d'un ordinateur de bureau lorsqu'il est éteint. La valeur par défaut est **0** kWh. |
| **Ordinateur portable éteint** | Spécifiez la consommation électrique d'un ordinateur portable lorsqu'il est éteint. La valeur par défaut est **0** kWh. |
| **Moniteur d'ordinateur de bureau allumé** | Spécifiez la consommation électrique d'un moniteur d'ordinateur de bureau lorsqu'il est allumé. La valeur par défaut est **0,028** kWh. |
| **Moniteur d'ordinateur portable allumé** | Spécifiez la consommation électrique d'un moniteur d'ordinateur portable lorsqu'il est allumé. La valeur par défaut est **0** kWh. |

#### Liens de rapports

Ce rapport n'établit pas de liaison à d'autres rapports de gestion de l'alimentation.

### Rapport Coût énergétique

Le rapport **Coût énergétique** affiche les informations suivantes :

- Un graphique indiquant le coût mensuel total d'électricité des ordinateurs du regroupement spécifié pour la période indiquée.
- Un graphique indiquant le coût mensuel moyen d'électricité de chaque ordinateur du regroupement spécifié pour la période indiquée.
- Un tableau affichant le coût mensuel total d'électricité et le coût mensuel moyen d'électricité des ordinateurs du regroupement spécifié au cours des 31 derniers jours.

  Ces informations peuvent être utilisées pour comprendre les tendances de coût d'électricité dans votre environnement. Après avoir appliqué un mode d'alimentation aux ordinateurs du regroupement sélectionné, le coût d'électricité des ordinateurs doit diminuer.

  Utilisez les paramètres suivants pour configurer ce rapport.

#### Paramètres de rapport obligatoires

Les paramètres suivants doivent être spécifiés pour exécuter ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Date de début** | Dans la liste déroulante, sélectionnez la date de début du rapport. |
| **Date de fin** | Dans la liste déroulante, sélectionnez la date de fin du rapport. |

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Coût du kWh** | Spécifiez le coût par kWh d'électricité. La valeur par défaut est **0,09**.<br><br>Vous pouvez modifier la devise utilisée par ce rapport dans la section des paramètres cachés. |
| **Nom du regroupement** | Dans la liste déroulante, sélectionnez le regroupement à utiliser pour ce rapport. |
| **Type d'appareil** | Dans la liste déroulante, sélectionnez le type d'ordinateur pour lequel vous souhaitez obtenir un rapport. Les valeurs valides sont **Tout** (ordinateurs portables et postes de travail), **Bureau** (postes de travail uniquement) et **Ordinateur portable** (ordinateurs portables uniquement). Ces valeurs sont retournées uniquement pour la période de création de rapports sélectionnée. |

**Paramètres de rapport masqués**

Vous pouvez également indiquer les paramètres masqués suivants pour modifier le comportement de ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Ordinateur de bureau allumé** | Spécifiez la consommation électrique d'un ordinateur de bureau lorsqu'il est allumé. La valeur par défaut est **0,07** kWh. |
| **Ordinateur portable allumé** | Spécifiez la consommation électrique d'un ordinateur portable lorsqu'il est allumé. La valeur par défaut est **0,02** kWh. |
| **Ordinateur de bureau en veille** | Spécifiez la consommation électrique d'un ordinateur de bureau qui est entré en mode veille. La valeur par défaut est **0,003** kWh. |
| **Ordinateur portable en veille** | Spécifiez la consommation électrique d'un ordinateur portable qui est entré en mode veille. La valeur par défaut est **0,001** kWh. |
| **Ordinateur de bureau éteint** | Spécifiez la consommation électrique d'un ordinateur de bureau lorsqu'il est éteint. La valeur par défaut est **0** kWh. |
| **Ordinateur portable éteint** | Spécifiez la consommation électrique d'un ordinateur portable lorsqu'il est éteint. La valeur par défaut est **0** kWh. |
| **Moniteur d'ordinateur de bureau allumé** | Spécifiez la consommation électrique d'un moniteur d'ordinateur de bureau lorsqu'il est allumé. La valeur par défaut est **0,028** kWh. |
| **Moniteur d'ordinateur portable allumé** | Spécifiez la consommation électrique d'un moniteur d'ordinateur portable lorsqu'il est allumé. La valeur par défaut est **0** kWh. |

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Devise** | Spécifiez le nom de la devise à utiliser pour ce rapport. La valeur par défaut est **USD ($)**. |

**Liens de rapports**

Ce rapport n'établit pas de liaison à d'autres rapports de gestion de l'alimentation.

### Rapport Coût énergétique journalier

Le rapport **Coût énergétique journalier** affiche les informations suivantes :

- Un graphique indiquant le coût total d'électricité quotidien des ordinateurs du regroupement spécifié pour les 31 derniers jours.
- Un graphique indiquant le coût moyen d'électricité quotidien de chaque ordinateur du regroupement spécifié pour les 31 derniers jours.
- Un tableau affichant le coût total d'électricité quotidien et le coût moyen d'électricité quotidien des ordinateurs du regroupement spécifié pour les 31 derniers jours.

  Ces informations peuvent être utilisées pour comprendre les tendances de coût d'électricité dans votre environnement. Après avoir appliqué un mode d'alimentation aux ordinateurs du regroupement sélectionné, le coût d'électricité des ordinateurs doit diminuer.

  Utilisez les paramètres suivants pour configurer ce rapport.

**Paramètres de rapport obligatoires**

Les paramètres suivants doivent être spécifiés pour exécuter ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Nom du regroupement** | Dans la liste déroulante, sélectionnez le regroupement à utiliser pour ce rapport. |
| **Type d'appareil** | Dans la liste déroulante, sélectionnez le type d'ordinateur pour lequel vous souhaitez obtenir un rapport. Les valeurs valides sont **Tout** (ordinateurs portables et postes de travail), **Bureau** (postes de travail uniquement) et **Ordinateur portable** (ordinateurs portables uniquement). Ces valeurs sont retournées uniquement pour la période de création de rapports sélectionnée. |
| **Coût du kWh** | Spécifiez le coût par kWh d'électricité. La valeur par défaut est **0,09**.<br><br>Vous pouvez modifier la devise utilisée par ce rapport dans la section des paramètres cachés. |

**Paramètres de rapport masqués**

Vous pouvez également indiquer les paramètres masqués suivants pour modifier le comportement de ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Ordinateur de bureau allumé** | Spécifiez la consommation électrique d'un ordinateur de bureau lorsqu'il est allumé. La valeur par défaut est **0,07** kWh. |

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Ordinateur portable allumé** | Spécifiez la consommation électrique d'un ordinateur portable lorsqu'il est allumé. La valeur par défaut est **0,02** kWh. |
| **Ordinateur de bureau en veille** | Spécifiez la consommation électrique d'un ordinateur de bureau qui est entré en mode veille. La valeur par défaut est **0,003** kWh. |
| **Ordinateur portable en veille** | Spécifiez la consommation électrique d'un ordinateur portable qui est entré en mode veille. La valeur par défaut est **0,001** kWh. |
| **Ordinateur de bureau éteint** | Spécifiez la consommation électrique d'un ordinateur de bureau lorsqu'il est éteint. La valeur par défaut est **0** kWh. |
| **Ordinateur portable éteint** | Spécifiez la consommation électrique d'un ordinateur portable lorsqu'il est éteint. La valeur par défaut est **0** kWh. |
| **Moniteur d'ordinateur de bureau allumé** | Spécifiez la consommation électrique d'un moniteur d'ordinateur de bureau lorsqu'il est allumé. La valeur par défaut est **0,028** kWh. |
| **Moniteur d'ordinateur portable allumé** | Spécifiez la consommation électrique d'un moniteur d'ordinateur portable lorsqu'il est allumé. La valeur par défaut est **0** kWh. |
| **Devise** | Spécifiez le nom de la devise à utiliser pour ce rapport. La valeur par défaut est **USD ($)**. |

#### Liens de rapports

Ce rapport n'établit pas de liaison à d'autres rapports de gestion de l'alimentation.

### Rapport Incidence sur l'environnement

Le rapport **Incidence sur l'environnement** affiche les informations suivantes :

- Un graphique indiquant la quantité mensuelle totale de CO2 générée (en tonnes) par les ordinateurs du regroupement spécifié pendant la période indiquée.
- Un graphique indiquant la quantité mensuelle moyenne de CO2 générée (en tonnes) par chaque ordinateur du regroupement spécifié pendant la période indiquée.
- Un tableau indiquant la quantité mensuelle totale de CO2 générée et la quantité mensuelle moyenne de CO2 générée par les ordinateurs du regroupement spécifié pendant la période indiquée.

  Le rapport **Incidence sur l'environnement** calcule la quantité de CO2 générée (en tonnes) en utilisant la durée pendant laquelle un ordinateur ou un moniteur est resté sous tension sur une période de 24 heures.

  Utilisez les paramètres suivants pour configurer ce rapport.

#### Paramètres de rapport obligatoires

Les paramètres suivants doivent être spécifiés pour exécuter ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Date de début du rapport** | Dans la liste déroulante, sélectionnez la date de début du rapport. |
| **Date de fin du rapport** | Dans la liste déroulante, sélectionnez la date de fin du rapport. |
| **Nom du regroupement** | Dans la liste déroulante, sélectionnez un regroupement pour ce rapport. |
| **Type d'appareil** | Dans la liste déroulante, sélectionnez le type d'ordinateur pour lequel vous souhaitez obtenir un rapport. Les valeurs valides sont **Tout** (ordinateurs portables et postes de travail), **Bureau** (postes de travail uniquement) et **Ordinateur portable** (ordinateurs portables uniquement). Ces valeurs sont retournées uniquement pour la période de création de rapports sélectionnée. |

**Paramètres de rapport masqués**

Vous pouvez également indiquer les paramètres masqués suivants pour modifier le comportement de ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Ordinateur de bureau allumé** | Spécifiez la consommation électrique d'un ordinateur de bureau lorsqu'il est allumé. La valeur par défaut est **0,07** kWh. |
| **Ordinateur portable allumé** | Spécifiez la consommation électrique d'un ordinateur portable lorsqu'il est allumé. La valeur par défaut est **0,02** kWh. |
| **Ordinateur de bureau en veille** | Spécifiez la consommation électrique d'un ordinateur de bureau qui est entré en mode veille. La valeur par défaut est **0,003** kWh. |
| **Ordinateur portable en veille** | Spécifiez la consommation électrique d'un ordinateur portable qui est entré en mode veille. La valeur par défaut est **0,001** kWh. |
| **Ordinateur de bureau éteint** | Spécifiez la consommation électrique d'un ordinateur de bureau lorsqu'il est éteint. La valeur par défaut est **0** kWh. |
| **Ordinateur portable éteint** | Spécifiez la consommation électrique d'un ordinateur portable lorsqu'il est éteint. La valeur par défaut est **0** kWh. |
| **Moniteur d'ordinateur de bureau allumé** | Spécifiez la consommation électrique d'un moniteur d'ordinateur de bureau lorsqu'il est allumé. La valeur par défaut est **0,028** kWh. |
| **Moniteur d'ordinateur portable allumé** | Spécifiez la consommation électrique d'un moniteur d'ordinateur portable lorsqu'il est allumé. La valeur par défaut est **0** kWh. |

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Facteur carbone (tonnes/kWh)** (CO2Mix) | Spécifiez la valeur du facteur carbone (en tonnes/kWh) que vous pouvez généralement obtenir auprès de votre compagnie d'électricité. La valeur par défaut est **0,0015** tonne par kWh. |

#### Liens de rapports

Ce rapport n'établit pas de liaison à d'autres rapports de gestion de l'alimentation.

### Rapport Incidence journalière sur l'environnement

Le rapport **Incidence journalière sur l'environnement** affiche les informations suivantes :

- Un graphique indiquant la quantité quotidienne totale de CO2 générée (en tonnes) par les ordinateurs du regroupement spécifié pendant les 31 derniers jours.
- Un graphique indiquant la quantité quotidienne moyenne de CO2 générée (en tonnes) par chaque ordinateur du regroupement spécifié pendant les 31 derniers jours.
- Un tableau indiquant la quantité quotidienne totale de CO2 générée et la quantité quotidienne moyenne de CO2 générée par les ordinateurs du regroupement spécifié pendant les 31 derniers jours.

  Le rapport **Incidence journalière sur l'environnement** calcule la quantité de CO2 générée (en tonnes) en utilisant la durée pendant laquelle un ordinateur ou un moniteur est resté sous tension sur une période de 24 heures.

#### Paramètres de rapport obligatoires

Les paramètres suivants doivent être spécifiés pour exécuter ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Nom du regroupement** | Dans la liste déroulante, sélectionnez un regroupement pour ce rapport. |
| **Type d'appareil** | Dans la liste déroulante, sélectionnez le type d'ordinateur pour lequel vous souhaitez obtenir un rapport. Les valeurs valides sont **Tout** (ordinateurs portables et postes de travail), **Bureau** (postes de travail uniquement) et **Ordinateur portable** (ordinateurs portables uniquement). Ces valeurs sont retournées uniquement pour la période de création de rapports sélectionnée. |

#### Paramètres de rapport masqués

Vous pouvez également indiquer les paramètres masqués suivants pour modifier le comportement de ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Ordinateur de bureau allumé** | Spécifiez la consommation électrique d'un ordinateur de bureau lorsqu'il est allumé. La valeur par défaut est **0,07** kWh. |
| **Ordinateur portable allumé** | Spécifiez la consommation électrique d'un ordinateur portable lorsqu'il est allumé. La valeur par défaut est **0,02** kWh. |

| NOM DU PARAMÈTRE | DESCRIPTION |
| --- | --- |
| **Ordinateur de bureau éteint** | Spécifiez la consommation électrique d'un ordinateur de bureau lorsqu'il est éteint. La valeur par défaut est **0** kWh. |
| **Ordinateur portable éteint** | Spécifiez la consommation électrique d'un ordinateur portable lorsqu'il est éteint. La valeur par défaut est **0** kWh. |
| **Ordinateur de bureau en veille** | Spécifiez la consommation électrique d'un ordinateur de bureau qui est entré en mode veille. La valeur par défaut est **0,003** kWh. |
| **Ordinateur portable en veille** | Spécifiez la consommation électrique d'un ordinateur portable qui est entré en mode veille. La valeur par défaut est **0,001** kWh. |
| **Moniteur d'ordinateur de bureau allumé** | Spécifiez la consommation électrique d'un moniteur d'ordinateur de bureau lorsqu'il est allumé. La valeur par défaut est **0,028** kWh. |
| **Moniteur d'ordinateur portable allumé** | Spécifiez la consommation électrique d'un moniteur d'ordinateur portable lorsqu'il est allumé. La valeur par défaut est **0** kWh. |
| **Facteur carbone (tonnes/kWh)** (CO2Mix) | Spécifiez une valeur pour le facteur carbone (en tonnes/kWh) que vous pouvez généralement obtenir auprès de votre compagnie d'électricité. La valeur par défaut est **0,0015** tonne par kWh. |

#### Liens de rapports

Ce rapport n'établit pas de liaison à d'autres rapports de gestion de l'alimentation.

### Rapport Détails de l'ordinateur non mis en veille

Le rapport **Détails de l'ordinateur non mis en veille** affiche la liste des ordinateurs qui ne se sont pas mis en veille ou en veille prolongée pour une raison donnée pendant une période spécifique. Ce rapport est appelé par le **Rapport sur la non mise en veille** et il n'est pas destiné à être exécuté directement par l'administrateur du site.

Le **rapport de non-mise en veille** indique que les ordinateurs **ne sont pas compatibles avec le mode veille** lorsqu'ils ne peuvent pas se mettre en veille et qu'ils ont été sous tension pendant toute la période de rapport définie. Le rapport affiche un ordinateur comme **Non compatible avec le mode veille prolongée** lorsqu'il ne peut pas se mettre en veille prolongée et qu'il a été sous tension pendant toute la période de rapport définie.

> **NOTE**
> La gestion de l'alimentation peut seulement collecter les causes qui ont empêché les ordinateurs exécutant Windows 7 ou Windows Server 2008 R2 de se mettre en veille ou en veille prolongée.

Utilisez les paramètres suivants pour configurer ce rapport.

#### Paramètres de rapport obligatoires

Les paramètres suivants doivent être spécifiés pour exécuter ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
| --- | --- |
| **Nom du regroupement** | Dans la liste déroulante, sélectionnez le regroupement à utiliser pour ce rapport. |
| **Intervalle du rapport (jours)** | Spécifiez le nombre de jours que doit couvrir le rapport. La valeur par défaut est **7** jours. |
| **Cause de la non mise en veille** | Dans la liste déroulante, sélectionnez une des causes qui peuvent empêcher les ordinateurs d'entrer en mode veille ou veille prolongée. |

**Paramètres de rapport masqués**

Ce rapport n'a aucun paramètre masqué que vous pouvez définir.

**Liens de rapports**

Ce rapport contient des liens vers le rapport suivant qui fournit des informations supplémentaires sur l'élément sélectionné.

| NOM DU RAPPORT | DÉTAILS |
| --- | --- |
| **Détails de l'ordinateur** | Cliquez sur le lien **Cliquez pour obtenir des informations détaillées** pour afficher les fonctions de gestion de l'alimentation, les paramètres d'alimentation et les modes d'alimentation appliqués de l'ordinateur sélectionné.<br><br>Pour plus d'informations, consultez Computer Details Report dans cette rubrique. |

### Insomnia report

Le **Rapport sur la non mise en veille** affiche une liste des causes courantes qui ont empêché les ordinateurs d'entrer en veille ou en veille prolongée et le nombre d'ordinateurs affectés par chaque cause pendant une période spécifique. Un certain nombre de causes peut empêcher un ordinateur d'entrer en veille ou en veille prolongée, notamment le processus en cours d'exécution sur l'ordinateur, une session de bureau à distance ouverte ou l'incapacité pour l'ordinateur d'entrer en veille ou en veille prolongée. À partir de ce rapport, vous pouvez ouvrir le rapport **Détails de l'ordinateur non mis en veille** , qui affiche une liste d'ordinateurs concernés par chaque cause d'ordinateurs qui ne sont pas en veille ou en veille prolongée.

Le rapport de non mise en veille affiche un ordinateur comme **Non compatible avec le mode veille** lorsqu'il ne peut pas se mettre en veille et qu'il a été sous tension pendant toute la période de rapport définie. Le rapport affiche un ordinateur comme **Non compatible avec le mode veille prolongée** lorsqu'il ne peut pas se mettre en veille prolongée et qu'il a été sous tension pendant toute la période de rapport définie.

> **NOTE**
> La gestion de l'alimentation peut seulement collecter les causes qui ont empêché les ordinateurs exécutant Windows 7 ou Windows Server 2008 R2 de se mettre en veille ou en veille prolongée.

Utilisez les paramètres suivants pour configurer ce rapport.

**Paramètres de rapport obligatoires**

Les paramètres suivants doivent être spécifiés pour exécuter ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
| --- | --- |
| **Nom du regroupement** | Dans la liste déroulante, sélectionnez le regroupement à utiliser pour ce rapport. |
| **Intervalle du rapport (jours)** | Spécifiez le nombre de jours que doit couvrir le rapport. La valeur par défaut est **7** jours. La valeur maximale est **365** jours. Spécifiez **0** pour exécuter le rapport pour aujourd'hui. |

**Paramètres de rapport masqués**

Ce rapport n'a aucun paramètre masqué que vous pouvez définir.

**Liens de rapports**

Ce rapport contient des liens vers le rapport suivant qui fournit des informations supplémentaires sur l'élément sélectionné.

| NOM DU RAPPORT | DÉTAILS |
| --- | --- |
| **Détails de l'ordinateur non mis en veille** | Cliquez sur un numéro de la colonne **Ordinateurs affectés** pour afficher une liste des ordinateurs incapables de passer en mode veille ou en mode veille prolongée en raison de la cause sélectionnée.<br><br>Pour plus d'informations, consultez Insomnia Computer Details Report dans cette rubrique. |

### Rapport Fonctions de gestion de l'alimentation

Le rapport **Fonctions de gestion de l'alimentation** affiche les fonctions matérielles de gestion de l'alimentation des ordinateurs dans le regroupement spécifique. Ce rapport est généralement utilisé dans la phase de surveillance de la gestion de l'alimentation pour déterminer les fonctions de gestion de l'alimentation des ordinateurs de votre organisation. Les informations affichées dans le rapport peuvent ensuite être utilisées pour créer des regroupements d'ordinateurs auxquels seront appliqués des modes d'alimentation ou qui seront exclus de la gestion de l'alimentation. Les fonctions de gestion de l'alimentation affichées par ce rapport sont les suivantes :

- **Compatible avec le mode veille** - Indique si l'ordinateur a la possibilité d'entrer en veille s'il est configuré pour ce faire.
- **Compatible avec le mode veille prolongée** – Indique si l'ordinateur peut entrer en veille prolongée s'il est configuré pour ce faire.
- **Compatible avec la sortie de veille** – Indique si l'ordinateur peut sortir du mode veille s'il est configuré pour ce faire.
- **Compatible avec la sortie de veille prolongée** – Indique si l'ordinateur peut sortir du mode veille prolongée s'il est configuré pour ce faire.

  Les valeurs signalées par le rapport **Fonctions de gestion de l'alimentation** indiquent les possibilités de mise en veille et en veille prolongée d'ordinateurs, tels que signalés par Windows. Toutefois, les valeurs signalées ne reflètent pas les cas où les paramètres de BIOS ou de Windows empêchent ces fonctions d'opérer.

  Utilisez les paramètres suivants pour configurer ce rapport.

**Paramètres de rapport obligatoires**

Les paramètres suivants doivent être spécifiés pour exécuter ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
| --- | --- |
| **Regroupement** | Dans la liste déroulante, sélectionnez un regroupement pour ce rapport. |
| **Filtre d'affichage** | Dans la liste déroulante, sélectionnez **Non pris en charge** pour afficher uniquement les ordinateurs du regroupement spécifié qui ne sont pas aptes à être mis en veille, à être mis en veille prolongée, à sortir de veille ou à sortir de veille prolongée. Sélectionnez **Tout afficher** pour afficher tous les ordinateurs du regroupement spécifié. |

#### Paramètres de rapport masqués

Ce rapport n'a aucun paramètre masqué que vous pouvez définir.

#### Liens de rapports

Ce rapport contient des liens vers le rapport suivant qui fournit des informations supplémentaires sur l'élément sélectionné.

| NOM DU RAPPORT | DÉTAILS |
| --- | --- |
| **Détails de l'ordinateur** | Cliquez sur un nom d'ordinateur pour afficher les fonctions de gestion de l'alimentation, les paramètres d'alimentation et les modes de gestion de l'alimentation appliqués à l'ordinateur sélectionné.<br><br>Pour plus d'informations, consultez Computer Details Report dans cette rubrique. |

### Rapport Paramètres d’alimentation

Le rapport **Paramètres d'alimentation** affiche une liste agrégée des paramètres d'alimentation utilisés par les ordinateurs du regroupement spécifié. Pour chaque paramètre d'alimentation, les modes d'alimentation, les valeurs et les unités possibles sont affichés, ainsi que le nombre d'ordinateurs utilisant ces valeurs. Ce rapport peut être utilisé pendant la phase de surveillance de la gestion de l'alimentation pour aider l'administrateur à comprendre les paramètres d'alimentation existants utilisés par les ordinateurs du site et pour faciliter la planification de l'application optimale des paramètres d'alimentation grâce à un mode de gestion de l'alimentation. Ce rapport est également utile lors de la résolution d'erreurs afin de vérifier que ces paramètres d'alimentation ont été correctement appliqués.

> **NOTE**
> Les paramètres affichés sont collectés à partir d'ordinateurs clients pendant l'inventaire matériel. Selon le moment auquel est exécuté l'inventaire matériel, les paramètres des modes d'alimentation appliqués en heures creuses ou en heure de pointe peuvent être collectés.

Utilisez les paramètres suivants pour configurer ce rapport.

#### Paramètres de rapport obligatoires

Les paramètres suivants doivent être spécifiés pour exécuter ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
| --- | --- |
| **Nom du regroupement** | Dans la liste déroulante, sélectionnez un regroupement pour ce rapport. |

#### Paramètres de rapport masqués

Vous pouvez également indiquer les paramètres masqués suivants pour modifier le comportement de ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **numberOfLocalizations** | Spécifiez le nombre de langues dans lesquelles vous souhaitez afficher les noms des paramètres d'alimentation signalés par les ordinateurs clients. Si vous voulez uniquement afficher la langue la plus répandue, conservez ce paramètre à sa valeur par défaut de **1**. Pour afficher toutes les langues, définissez cette valeur sur **0**. |

#### Liens de rapports

Ce rapport contient des liens vers le rapport suivant qui fournit des informations supplémentaires sur l'élément sélectionné.

| NOM DU RAPPORT | DÉTAILS |
|---|---|
| **Détails des paramètres du mode de gestion de l'alimentation** | Cliquez sur le nombre d'ordinateurs dans la colonne **Ordinateurs** pour afficher la liste de tous les ordinateurs qui utilisent les paramètres d'alimentation de cette ligne.<br><br>Pour plus d'informations, consultez Power Settings Details Report dans cette rubrique. |

### Power Settings Details report

Le rapport **Détails des paramètres d'alimentation** affiche d'autres informations sur les ordinateurs sélectionnés dans le rapport **Paramètres d'alimentation** . Ce rapport est appelé par le rapport **Paramètres d'alimentation** et il n'est pas destiné à être exécuté directement par l'administrateur du site.

#### Paramètres de rapport obligatoires

Les paramètres suivants doivent être spécifiés pour exécuter ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
|---|---|
| **Regroupement** | Dans la liste déroulante, sélectionnez le regroupement à utiliser pour ce rapport. |
| **GUID du paramètre d'alimentation** | Dans la liste déroulante, sélectionnez le GUID du paramètre d'alimentation sur lequel vous souhaitez effectuer un rapport. Pour obtenir la liste de tous les paramètres d'alimentation et leurs utilisations, consultez Paramètres du mode de gestion de l'alimentation disponibles dans la rubrique Comment créer et appliquer des modes de gestion de l'alimentation dans System Center Configuration Manager. |
| **Power Mode** | Dans la liste déroulante, sélectionnez le type de paramètres d'alimentation à afficher dans les résultats du rapport. Sélectionnez **Sur secteur** pour afficher les paramètres d'alimentation configurés quand l'ordinateur est branché sur secteur et **Sur batterie** pour afficher les paramètres d'alimentation configurés quand l'ordinateur fonctionne sur batterie. |

| NOM DU PARAMÈTRE | DESCRIPTION |
| --- | --- |
| **Index des paramètres** | Dans la liste déroulante, sélectionnez la valeur pour le nom de paramètre d'alimentation sélectionné pour lequel vous souhaitez produire un rapport. Par exemple, pour afficher tous les ordinateurs dont le paramètre **Arrêter le disque dur après** a la valeur **10** minutes, sélectionnez **Arrêter le disque dur après** pour **Nom du paramètre d'alimentation** et **10** pour **Index des paramètres**. |

**Paramètres de rapport masqués**

Vous pouvez également indiquer les paramètres masqués suivants pour modifier le comportement de ce rapport.

| NOM DU PARAMÈTRE | DESCRIPTION |
| --- | --- |
| **numberOfLocalizations** | Spécifiez le nombre de langues dans lesquelles vous souhaitez afficher les noms des paramètres d'alimentation signalés par les ordinateurs clients. Si vous voulez uniquement afficher la langue la plus répandue, conservez ce paramètre à sa valeur par défaut de **1**. Pour afficher toutes les langues, définissez cette valeur sur **0**. |

**Liens de rapports**

Ce rapport contient des liens vers le rapport suivant qui fournit des informations supplémentaires sur l'élément sélectionné.

| NOM DU RAPPORT | DÉTAILS |
| --- | --- |
| **Détails de l'ordinateur** | Cliquez sur un nom d'ordinateur pour afficher les fonctions de gestion de l'alimentation, les paramètres d'alimentation et les modes de gestion de l'alimentation appliqués à l'ordinateur sélectionné.<br><br>Pour plus d'informations, consultez Computer Details Report dans cette rubrique. |

# Sécurité et confidentialité pour la gestion de l'alimentation dans System Center Configuration Manager

22/06/2018 • 2 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Cette section contient des informations de sécurité et de confidentialité pour la gestion de l'alimentation dans System Center Configuration Manager.

## Meilleures pratiques de sécurité pour la gestion de l'alimentation

Il n'existe aucune meilleure pratique liée à la sécurité pour la gestion de l'alimentation.

## Informations de confidentialité pour la gestion de l'alimentation

Gestion de l'alimentation utilise des fonctionnalités qui sont intégrées à Windows pour surveiller la consommation d'énergie et pour appliquer les paramètres d'alimentation aux ordinateurs pendant les heures de bureau et les heures creuses. Configuration Manager collecte des informations sur la consommation d'énergie auprès des ordinateurs, incluant des données sur périodes d'utilisation des ordinateurs par les utilisateurs. Bien que Configuration Manager surveille la consommation d'énergie pour un regroupement plutôt que pour chaque ordinateur, un regroupement peut contenir un seul ordinateur. La gestion de l'alimentation n'est pas activée par défaut et doit être configurée par un administrateur.

Les informations sur la consommation d'énergie sont stockées dans la base de données Configuration Manager et ne sont pas envoyées à Microsoft. Les informations détaillées sont conservées dans la base de données pendant 31 jours et les informations résumées sont conservées pendant 13 mois. Vous ne pouvez pas configurer l'intervalle de suppression.

Avant de configurer la gestion de l'alimentation, pensez à vos besoins en matière de confidentialité.

# Mettre à niveau les clients dans System Center Configuration Manager

22/06/2018 • 7 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez utiliser différentes méthodes pour mettre à niveau le logiciel client System Center Configuration Manager sur les ordinateurs Windows, les serveurs UNIX et Linux ainsi que les ordinateurs Mac. Les avantages et les inconvénients de chaque méthode sont présentés ci-dessous.

> **TIP**
> Si vous mettez à niveau votre infrastructure de serveur à partir d'une version précédente de Configuration Manager (comme Configuration Manager 2007 ou System Center 2012 Configuration Manager), nous vous recommandons d'effectuer les mises à niveau du serveur, dont l'installation de toutes les mises à jour de Current Branch, avant la mise à niveau des clients. De cette façon, vous disposez également de la version la plus récente du logiciel client.

## Installation via la stratégie de groupe

**Plateforme cliente prise en charge :** Windows

**Avantages**

- N'exige pas la découverte des ordinateurs préalablement à la mise à niveau du client.
- Peut être utilisée pour l'installation de nouveaux clients ou pour les mises à niveau.
- Les ordinateurs peuvent lire les propriétés de l'installation du client ayant été publiées dans les services de domaine Active Directory.
- Ne nécessite pas de configuration ni la présence d'un compte d'installation pour l'ordinateur client choisi.

**Inconvénients**

- Peut occasionner un trafic réseau intense si vous effectuez la mise à niveau d'un grand nombre de clients.
- Si le schéma Active Directory n'est pas étendu pour Configuration Manager, vous devez utiliser les paramètres de stratégie de groupe pour ajouter les propriétés d'installation du client aux ordinateurs de votre site.

## Installation via un script d'ouverture de session

**Plateforme cliente prise en charge :** Windows

**Avantages**

- N'exige pas la découverte des ordinateurs avant l'installation du client.
- Peut être utilisée pour l'installation de nouveaux clients ou pour les mises à niveau.
- Prend en charge les propriétés de ligne de commande de CCMSetup.

**Inconvénients**

- Peut occasionner un trafic réseau intense si vous effectuez la mise à niveau d'un grand nombre de clients sur une courte période.
- La mise à niveau de tous les ordinateurs clients peut prendre beaucoup de temps si les utilisateurs ne se connectent pas souvent au réseau.

  Pour plus d'informations, consultez Comment installer des clients Configuration Manager à l'aide de scripts de connexion.

## Installation manuelle

**Plateformes clientes prises en charge :** Windows, UNIX/Linux, Mac OS X

**Avantages**

- N'exige pas la découverte des ordinateurs préalablement à la mise à niveau du client.
- Peut être utile dans le cadre de tests.
- Prend en charge les propriétés de ligne de commande de CCMSetup.

**Inconvénients**

- Aucune automatisation, peut prendre du temps.

Pour plus d'informations, consultez les rubriques suivantes :

- Guide pratique pour installer manuellement des clients Configuration Manager
- Guide pratique pour mettre à niveau les clients pour des serveurs Linux et UNIX dans System Center Configuration Manager
- Guide pratique pour mettre à niveau les clients sur des ordinateurs Mac dans System Center Configuration Manager

## Mettre à niveau l'installation (gestion des applications)

**Plateforme cliente prise en charge :** Windows

> **NOTE**
> Vous ne pouvez pas mettre à niveau des clients Configuration Manager 2007 avec cette méthode. Dans ces circonstances, vous pouvez déployer le client Configuration Manager comme un package à partir du site Configuration Manager 2007 ou vous pouvez utiliser la mise à niveau automatique du client, qui crée et déploie automatiquement un package contenant la dernière version du client.

**Avantages**

- Prend en charge les propriétés de ligne de commande de CCMSetup.

**Inconvénients**

- Peut occasionner un trafic réseau intense si vous distribuez le client vers des regroupements volumineux.
- Peut être utilisée uniquement pour mettre à niveau le logiciel client sur les ordinateurs ayant été découverts et attribués au site.

  Pour plus d'informations, consultez Comment installer les clients Configuration Manager à l'aide d'un package et d'un programme.

## Mise à niveau automatique du client

> **NOTE**
> Peut être utilisée pour mettre à niveau les clients Configuration Manager 2007 vers des clients System Center Configuration Manager. Un client Configuration Manager 2007 peut être attribué à un site Configuration Manager, mais ne peut effectuer aucune action en dehors de la mise à niveau automatique du client.

**Plateforme cliente prise en charge :** Windows

**Avantages**

- Peut être utilisée pour que les clients du site disposent automatiquement de la dernière version.
- Nécessite une administration minimale.

**Inconvénients**

- Ne peut être utilisée que pour mettre le logiciel client à niveau et ne peut pas être utilisée pour installer un nouveau client.
- N'est pas compatible avec la mise à niveau simultanée de plusieurs clients.
- S'applique à tous les clients de la hiérarchie affectés à un site. Ne peut pas être étendue par regroupement.
- Options de planification limitées.

Pour plus d'informations, consultez Comment mettre à niveau les clients pour les ordinateurs Windows dans System Center Configuration Manager.

## Test du client

**Plateforme cliente prise en charge :** Windows

**Avantages**

- Permet de tester les nouvelles versions du client dans un regroupement de préproduction plus petit.
- Une fois le test terminé, les clients en préproduction sont promus en production et automatiquement mis à niveau à l'échelle du site Configuration Manager.

**Inconvénients**

- Ne peut être utilisée que pour mettre le logiciel client à niveau et ne peut pas être utilisée pour installer un nouveau client.

Comment tester les mises à niveau du client dans un regroupement de préproduction dans System Center Configuration Manager

# Comment tester les mises à niveau du client dans un regroupement de préproduction dans System Center Configuration Manager

22/06/2018 • 7 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez tester une nouvelle version du client Configuration Manager dans un regroupement de préproduction avant de mettre à niveau le reste du site vers cette version. Quand vous procédez ainsi, seuls les appareils qui font partie du regroupement de test sont mis à niveau. Une fois que vous avez pu tester le client, vous pouvez le promouvoir, ce qui rend la nouvelle version du logiciel client disponible pour le reste du site.

> **NOTE**
> Pour promouvoir un client de test en production, vous devez être connecté tant qu'utilisateur avec le rôle de sécurité **Administrateur complet** et une étendue de sécurité de **Tout**. Pour plus d'informations, consultez Principes de base de l'administration basée sur des rôles. Vous devez également être connecté à un serveur connecté au site d'administration centrale ou à un site principal autonome du plus haut niveau.

Il existe 3 étapes de base pour tester des clients en préproduction.

1. Configurez les mises à jour automatiques du client pour utiliser un regroupement de préproduction.
2. Installez une mise à jour de Configuration Manager qui inclut une nouvelle version du client.
3. Promouvez le nouveau client en production.

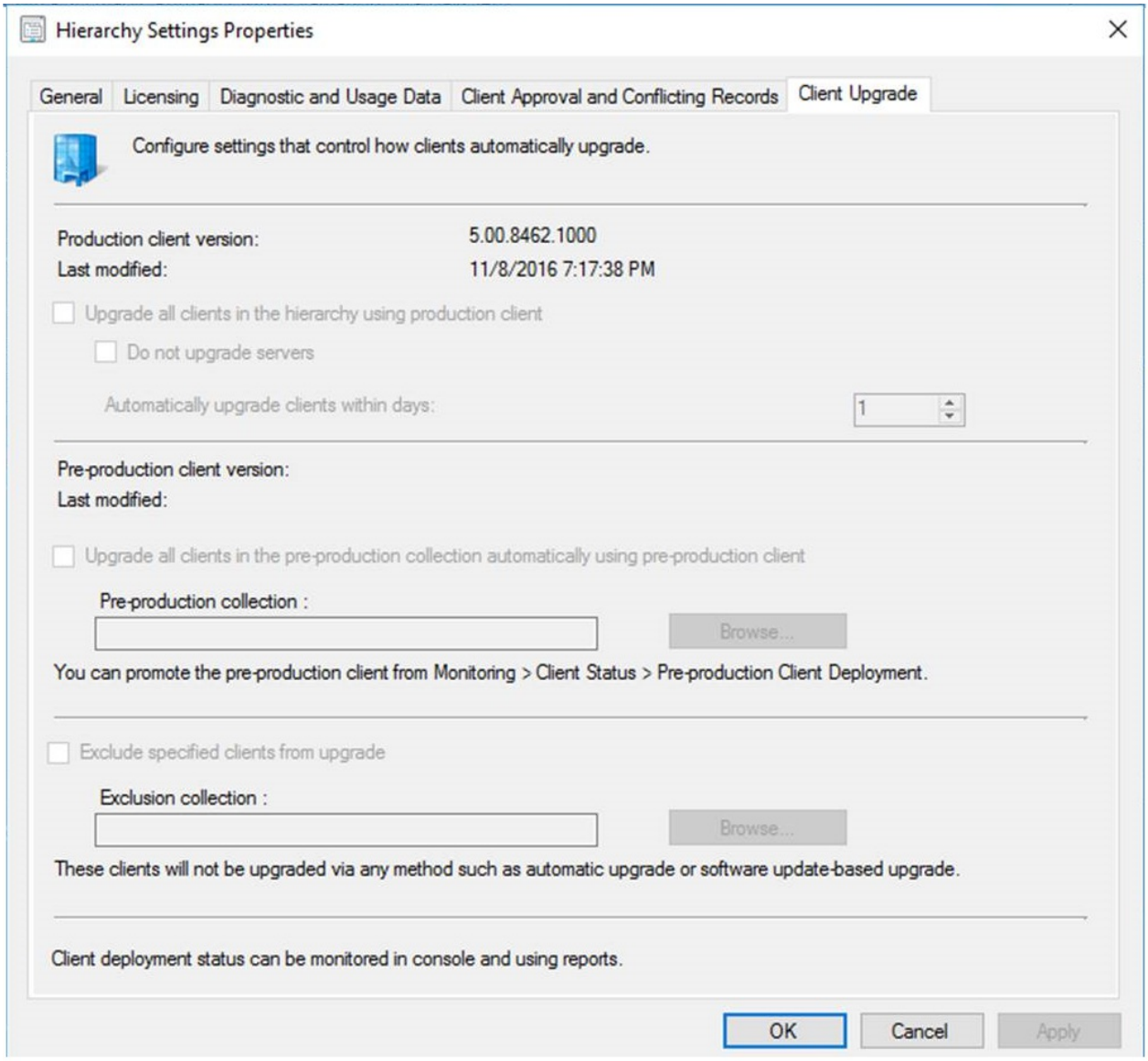
## Pour configurer les mises à jour automatiques du client pour utiliser un regroupement de préproduction

> **IMPORTANT**
> Le déploiement du client de préproduction n'est pas pris en charge pour les ordinateurs de groupe de travail. Ils ne peuvent pas utiliser l'authentification nécessaire pour permettre au point de distribution d'accéder au package du client de préproduction. Ils recevront la dernière version du client quand il sera promu client de production.

1. Configurez un regroupement contenant les ordinateurs sur lesquels vous voulez déployer le client de préproduction.
2. Dans la console Configuration Manager, ouvrez **Administration** > **Configuration du site** > **Sites**, puis choisissez **Paramètres de hiérarchie**.

   Sous l'onglet **Mise à niveau des clients** des **Propriétés des paramètres de hiérarchie**:

   - Sélectionnez **Mettre à niveau automatiquement tous les clients du regroupement de préproduction en utilisant un client de préproduction**.
   - Entrez le nom d'un regroupement à utiliser comme regroupement de préproduction.




**NOTE**

Pour modifier ces paramètres, votre compte doit être un membre du rôle de sécurité **Administrateur complet** et de l'étendue de sécurité **Tous**.

## Pour installer une mise à jour de Configuration Manager qui inclut une nouvelle version du client

1. Dans la console Configuration Manager, ouvrez **Administration** > **Mises à jour et services**, sélectionnez une mise à jour avec l'indication **Disponible**, puis choisissez **Installer le pack de mise à jour**. (Avant la version 1702, les mises à jour et la maintenance s'effectuaient via le menu **Administration** > **Services cloud**.)

   Pour plus d'informations sur l'installation des mises à jour, consultez Mises à jour pour System Center Configuration Manager

2. Lors de l'installation de la mise à jour, dans la page **Options du client** de l'Assistant, sélectionnez **Tester dans le regroupement de préproduction**.

3. Déroulez le reste de l'Assistant et installez le pack de mise à jour.

   Une fois l'Assistant terminé, les clients inclus dans le regroupement de préproduction commencent à déployer le client mis à jour. Vous pouvez surveiller le déploiement de clients mis à niveau en accédant à

**Surveillance** > **État du client** > **Déploiement des clients en préproduction**. Pour plus d'informations, consultez Comment surveiller l'état du déploiement des clients dans System Center Configuration Manager.

> **NOTE**
> L'état du déploiement sur les ordinateurs hébergeant des rôles de système de site dans un regroupement de préproduction peut être signalé comme **Non conforme**, même quand le client a été correctement déployé. Lors de la promotion du client en production, l'état du déploiement est correctement signalé.

## Pour promouvoir le nouveau client en production

1. Dans la console Configuration Manager, ouvrez **Administration** > **Mises à jour et maintenance**, puis choisissez **Promouvoir le client de préproduction**. (Avant la version 1702, les mises à jour et la maintenance s'effectuaient via le menu **Administration** > **Services cloud**.)

   > **TIP**
   > Le bouton **Promouvoir le client de préproduction** est également disponible quand vous surveillez les déploiements de clients dans la console en utilisant **Surveillance** > **État du client** > **Déploiement des clients en préproduction**.

2. Examinez les versions du client en production et préproduction, vérifiez que le regroupement de préproduction approprié est spécifié, et cliquez sur **Promouvoir**, puis sur **Oui**.

3. Une fois la boîte de dialogue fermée, la version du client mise à jour remplace la version du client en cours d'utilisation dans votre hiérarchie. Vous pouvez ensuite mettre à niveau les clients pour l'ensemble du site. Pour plus d'informations, consultez Comment mettre à niveau les clients pour les ordinateurs Windows dans System Center Configuration Manager.

> **NOTE**
> Pour activer le client de pré-production ou promouvoir un client de pré-production en client de production, votre compte doit être membre du rôle de sécurité avec les autorisations de **lecture** et de **modification** pour l'objet **Packages de mise à jour**. Les mises à niveau des clients respectent les fenêtres de maintenance Configuration Manager que vous avez configurées.

# Guide pratique pour empêcher la mise à niveau de clients sur des ordinateurs Windows dans System Center Configuration Manager

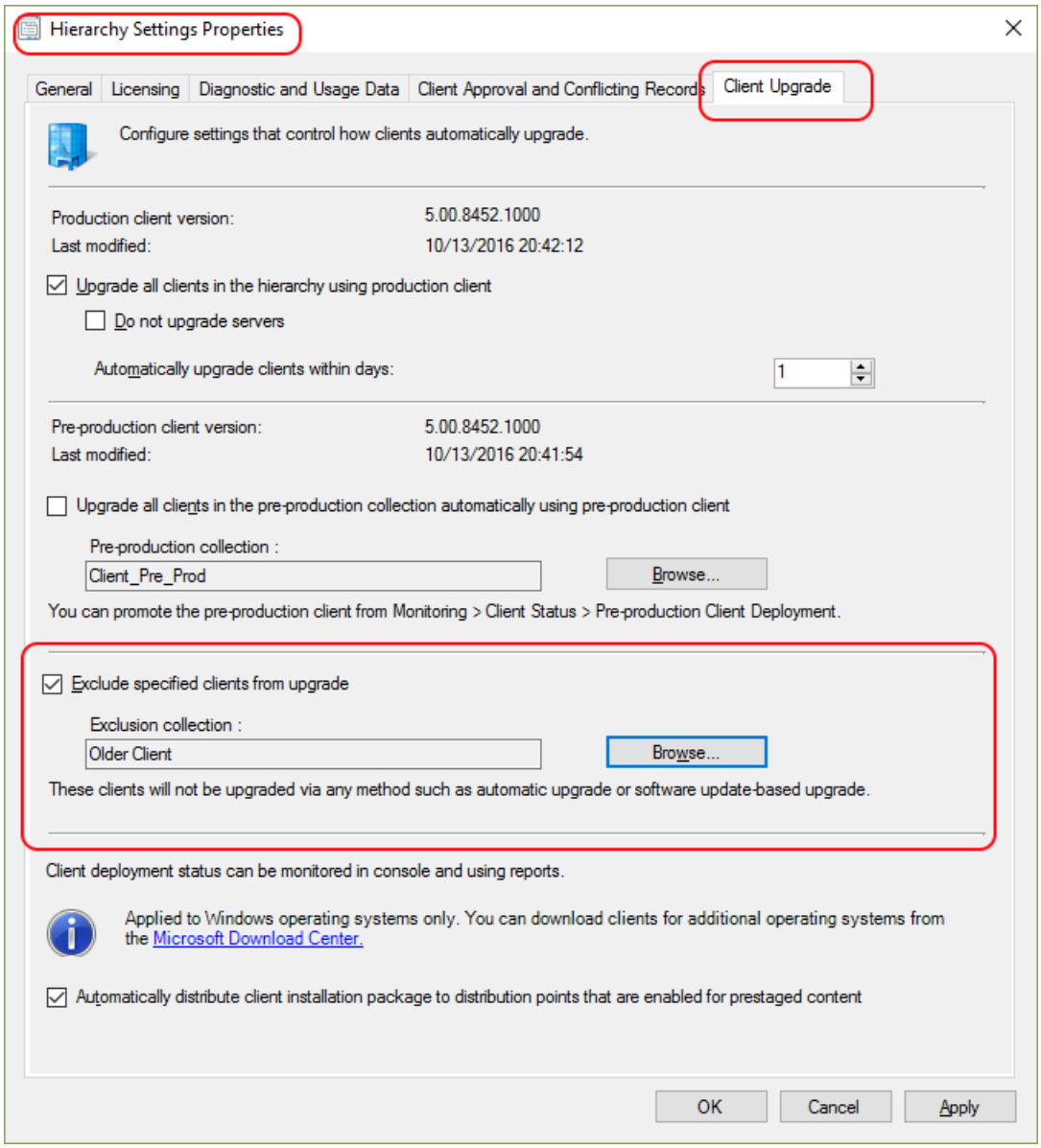
22/06/2018 • 4 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

À partir de la version 1610, vous pouvez empêcher un regroupement de clients d'installer automatiquement les versions mises à jour du client. Cela s'applique à la mise à niveau automatique ainsi qu'à d'autres méthodes, telles que la mise à niveau de logiciels basée sur la mise à jour, les scripts d'ouverture de session et la stratégie de groupe. Vous pouvez utiliser cette fonctionnalité pour un regroupement d'ordinateurs dont la mise à niveau du client nécessite plus d'attention. Un client qui se trouve dans un regroupement exclu ignore les demandes d'installation du logiciel client mis à jour.

## Configurer l'exclusion des mises à niveau automatiques

1. Dans la console Configuration Manager, accédez à **Administration** > **Configuration du site** > **Sites**, puis cliquez sur **Paramètres de hiérarchie**.
2. Cliquez sur l'onglet **Mise à niveau des clients**.
3. Cochez la case **Exclure les clients spécifiés de la mise à niveau**, puis pour Regroupement à exclure, sélectionnez le regroupement à exclure. Vous pouvez sélectionner un seul regroupement à exclure.
4. Cliquez sur **OK** pour fermer et enregistrer la configuration. Ensuite, une fois que les clients ont mis à jour la stratégie, les clients figurant dans le regroupement exclu n'installent plus automatiquement les mises à jour du logiciel client. Pour plus d'informations, consultez Guide pratique pour mettre à niveau des clients sur les ordinateurs Windows.




**NOTE**

Même si l'interface utilisateur indique que les clients ne seront pas mis à niveau, quelle que soit la méthode, il existe deux méthodes que vous pouvez utiliser pour remplacer ces paramètres. L'installation Push du client et une installation manuelle du client peuvent être utilisées pour remplacer cette configuration. Pour plus d'informations, consultez la section suivante.

## Guide pratique pour mettre à niveau un client figurant dans un regroupement exclu

Quand un regroupement est configuré comme exclu, les membres de ce regroupement peuvent mettre à niveau leur logiciel client par seulement deux méthodes, qui ont priorité sur l'exclusion :

- **Installation Push du client** : Vous pouvez utiliser l'installation Push du client pour mettre à niveau un client figurant dans un regroupement exclu. Cela est autorisé, car cela est considéré comme l'intention de l'administrateur et vous permet de mettre à niveau les clients sans retirer le regroupement complet de l'exclusion.

- **Installation manuelle du client** : Vous pouvez mettre à niveau manuellement les clients qui se trouvent dans un regroupement exclu en utilisant le commutateur de ligne de commande suivant avec ccmsetup : ***/ignoreskipupgrade***

  Si vous tentez de mettre à niveau manuellement un client qui est membre du regroupement exclu et que

vous n'utilisez pas ce commutateur, le client n'installe pas le nouveau logiciel client. Pour plus d'informations, consultez Comment installer les clients Configuration Manager manuellement.

Pour plus d'informations sur les méthodes d'installation de client, consultez Comment déployer des clients sur des ordinateurs Windows dans System Center Configuration Manager.

# Comment mettre à niveau les clients pour les ordinateurs Windows dans System Center Configuration Manager

22/06/2018 • 10 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Pour mettre à niveau le client sur des ordinateurs Windows, vous pouvez utiliser les méthodes d'installation de clients ou les fonctionnalités de mise à niveau automatique de clients de Configuration Manager. Les méthodes d'installation de clients présentées ci-dessous sont tout à fait indiquées pour mettre à niveau des logiciels clients sur les ordinateurs Windows :

- Installation via la stratégie de groupe
- Installation via un script d'ouverture de session
- Installation manuelle
- Installation de type mise à niveau

  Si vous voulez mettre à niveau le client en employant l'une des méthodes d'installation de clients, vous trouverez plus d'informations sur l'utilisation de ces méthodes dans Comment déployer des clients sur des ordinateurs Windows dans System Center Configuration Manager.

  À partir de la version 1610, vous pouvez empêcher la mise à niveau de clients en spécifiant un groupe d'exclusion. Pour plus d'informations, consultez Guide pratique pour empêcher la mise à niveau de clients sur les ordinateurs Windows.

**TIP**

Si vous mettez à niveau votre infrastructure de serveur à partir d'une version précédente de Configuration Manager (comme Configuration Manager 2007 ou System Center 2012 Configuration Manager), nous vous recommandons d'effectuer les mises à niveau du serveur, dont l'installation de toutes les mises à jour de Current Branch, avant la mise à niveau des clients. La dernière mise à jour de Current Branch contenant la dernière version du client, il est préférable d'effectuer les mises à niveau des clients après avoir installé toutes les mises à jour de Configuration Manager que vous souhaitez utiliser.

**NOTE**

Si vous voulez réattribuer le site pour les clients pendant la mise à niveau, vous pouvez spécifier le nouveau site à l'aide de la propriété SMSSITECODE client.msi. Si vous utilisez AUTO pour SMSSITECODE, vous devez également spécifier SITEREASSIGN=TRUE pour autoriser la réattribution automatique du site pendant la mise à niveau. Pour plus d'informations, consultez SMSSITECODE.

## Utiliser la mise à niveau automatique du client

Vous pouvez également configurer Configuration Manager pour mettre automatiquement à niveau le logiciel client vers la dernière version du client Configuration Manager quand Configuration Manager détecte qu'un client affecté à la hiérarchie Configuration Manager est antérieur à la version utilisée dans la hiérarchie. Ce scénario inclut la mise à niveau du client vers la dernière version quand il essaie de s'affecter à un site

Configuration Manager.

Un client peut être mis automatiquement à niveau dans les scénarios suivants :

- La version du client est inférieure à la version utilisée dans la hiérarchie.
- Le client du site d'administration centrale dispose d'un module linguistique, mais pas le client existant.
- La hiérarchie impose une version différente de celle installée sur le client.
- Un ou plusieurs fichiers d'installation du client sont d'une version différente.

> **NOTE**
> Vous pouvez exécuter le rapport **Nombre de clients de Configuration Manager par versions de client** dans le dossier du rapport **Site - Informations client** pour identifier les différentes versions du client Configuration Manager dans votre hiérarchie.

Configuration Manager crée un package de mise à niveau par défaut qui est automatiquement envoyé à tous les points de distribution de la hiérarchie. Si vous apportez des modifications au package du client sur le site d'administration centrale, par exemple, en ajoutant un module linguistique client, Configuration Manager met automatiquement à jour le package et le distribue à tous les points de distribution de la hiérarchie. Si la mise à niveau automatique des clients est activée, chaque client installe automatiquement le nouveau module linguistique client.

> **NOTE**
> Configuration Manager n'envoie pas automatiquement le package de mise à niveau du client aux points de distribution cloud Configuration Manager.

Nous vous recommandons d'activer les mises à niveau automatiques des clients dans votre hiérarchie. De cette façon, vos clients sont mis à jour avec une surcharge administrative minimale.

Utilisez la procédure suivante pour configurer la mise à niveau automatique des clients. La mise à niveau automatique des clients doit être configurée sur un site d'administration centrale. Cette configuration s'applique alors à tous les clients de votre hiérarchie.

**Pour configurer les mises à niveau automatiques du client**

1. Dans la console Configuration Manager, cliquez sur **Administration**.
2. Dans l'espace de travail **Administration** , développez **Configuration du site**, puis cliquez sur **Sites**.
3. Dans l'onglet **Accueil** , dans le groupe **Sites** , cliquez sur **Paramètres de hiérarchie**.
4. Sous l'onglet **Mise à niveau des clients** de la boîte de dialogue **Propriétés des paramètres de hiérarchie** , examinez la version et la date du client de production et vérifiez qu'il s'agit bien de la version que vous voulez utiliser pour mettre à niveau les ordinateurs Windows. Si ce n'est pas la version du client que vous attendiez, vous serez peut-être amené à promouvoir le client de préproduction en production. Pour plus d'informations, consultez Guide pratique pour tester les mises à niveau du client dans un regroupement de préproduction dans System Center Configuration Manager.
5. Cliquez sur **Mettre à niveau tous les clients de la hiérarchie en utilisant un client de production** et sur **OK** dans la boîte de dialogue de confirmation.
6. Si vous ne voulez pas que les mises à niveau du client s'appliquent aux serveurs, cliquez sur **Ne pas mettre à niveau les serveurs**.

7. Spécifiez le délai (en jours) dont disposent les ordinateurs pour mettre à niveau le client après avoir reçu la stratégie client. Le client sera mis à niveau dans un intervalle aléatoire, compris dans ce délai. Cela évite les scénarios où un grand nombre d'ordinateurs clients est mis à niveau simultanément.

   > **NOTE**
   >
   > Un ordinateur doit être en cours d'exécution pour mettre à niveau le client. Si un ordinateur n'est pas en cours d'exécution au moment où la réception de la mise à niveau est planifiée, cette dernière n'a pas lieu. En revanche, dès que l'ordinateur est redémarré, une autre mise à niveau est planifiée à un moment aléatoire pendant le nombre de jours autorisé. Si le redémarrage se produit alors que le délai de la mise à niveau a expiré, celle-ci est planifiée pour se produire à une heure aléatoire dans un délai de 24 heures après le redémarrage de l'ordinateur.
   >
   > En raison de ce comportement, les ordinateurs régulièrement arrêtés en fin de journée de travail risquent d'avoir besoin de plus de temps que prévu pour se mettre à niveau si l'heure de mise à niveau planifiée de façon aléatoire ne tombe pas dans les heures de travail.

8. À compter de la version 1610, si vous ne voulez pas que des clients soient mis à niveau, cliquez sur **Exclure les clients spécifiés de la mise à niveau** et spécifiez le regroupement à exclure.

9. Si vous souhaitez que le package d'installation du client soit copié sur des points de distribution activés pour le contenu préparé, cliquez sur **Distribuer automatiquement le package d'installation du client aux points de distribution activés pour le contenu préparé**.

10. Cliquez sur **OK** pour enregistrer les paramètres et fermer la boîte de dialogue **Propriétés des paramètres de hiérarchie** . Les clients recevront ces paramètres lors de leur prochain téléchargement de la stratégie.

> **NOTE**
>
> Les mises à niveau des clients respectent les fenêtres de maintenance Configuration Manager configurées.

# Comment mettre à niveau les clients pour des serveurs Linux et UNIX dans System Center Configuration Manager

22/06/2018 • 8 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Vous pouvez mettre à niveau la version du client pour Linux et UNIX vers une version plus récente du client sans désinstaller au préalable le client actuel. Pour cela, installez le nouveau package d'installation du client sur l'ordinateur en utilisant la propriété de ligne de commande **-keepdb**. Quand le client pour Linux et UNIX est installé, il remplace les données du client existantes par les nouveaux fichiers du client. Toutefois, la propriété de ligne de commande **-keepdb** demande au processus d'installation de conserver l'identificateur unique (GUID) du client, la base de données locale d'informations et le magasin de certificats. Ces informations sont ensuite utilisées par la nouvelle installation du client.

Par exemple, vous avez un ordinateur RHEL5 x64 qui exécute le client à partir de la version d'origine du client Configuration Manager pour Linux et UNIX. Pour mettre à niveau ce client avec la version du client disponible dans la mise à jour cumulative 1, exécutez manuellement le script **install** pour installer le package du client approprié à partir de la mise à jour cumulative 1, en ajoutant le commutateur de ligne de commande **-keepdb**. Consultez l'exemple de ligne de commande suivante :

```
./install -mp <hostname\> -sitecode <code\> -keepdb ccm-Universal-x64.<build\>.tar
```

## Comment utiliser un déploiement de logiciels pour mettre à niveau le client sur des serveurs Linux et UNIX

Vous pouvez utiliser un déploiement de logiciels pour mettre à niveau le client sur des serveurs Linux et UNIX vers une nouvelle version du client. Toutefois, le client Configuration Manager ne peut pas exécuter directement le script d'installation pour installer le nouveau client, car l'installation d'un nouveau client doit d'abord désinstaller le client actuel. Cette action entraînerait l'arrêt du processus client Configuration Manager qui exécute le script d'installation avant que l'installation du nouveau client ne commence. Pour pouvoir utiliser un déploiement de logiciels pour installer le nouveau client, vous devez planifier l'installation pour qu'elle commence plus tard et qu'elle soit exécutée par les fonctionnalités de planification intégrées du système d'exploitation.

Utilisez un déploiement de logiciels pour d'abord copier les fichiers du nouveau package d'installation de client sur l'ordinateur client. Déployez et exécutez ensuite un script destiné à planifier le processus d'installation du client. Le script utilise la commande **at** intégrée du système d'exploitation pour retarder son démarrage. Quand le script s'exécute, son fonctionnement est géré par le système d'exploitation du client, et non par le client Configuration Manager sur l'ordinateur. Ce comportement permet à la ligne de commande appelée par le script de d'abord désinstaller le client Configuration Manager, puis d'installer le nouveau client. Ces actions terminent le processus de mise à niveau du client sur l'ordinateur UNIX ou Linux. Une fois la mise à niveau terminée, le client mis à niveau continue à être géré par Configuration Manager.

Utilisez la procédure suivante pour configurer un déploiement de logiciels destiné à mettre à niveau le client pour Linux et UNIX. Les étapes et exemples suivants mettent à niveau un ordinateur RHEL5 x64 qui exécute la version initiale du client vers la version du client disponible dans la mise à jour cumulative 1.

**Pour utiliser un déploiement de logiciels destiné à mettre à niveau le client sur des serveurs Linux et UNIX**

1. Copiez le nouveau package d'installation du client sur l'ordinateur qui exécute le client Configuration

Manager à mettre à niveau.

Par exemple, placez le package d'installation du client et le script d'installation de la mise à jour cumulative 1 dans l'emplacement suivant sur l'ordinateur client : **/tmp/PATCH**

2. Créez un script pour gérer la mise à niveau du client Configuration Manager. Placez ensuite une copie de ce script dans le même dossier sur l'ordinateur client que les fichiers d'installation du client de l'étape 1.

   Le script ne doit pas obligatoirement porter un nom spécifique. Il doit contenir les lignes de commande nécessaires pour utiliser les fichiers d'installation du client à partir d'un dossier local sur l'ordinateur client et installer le package d'installation du client à l'aide de la propriété de ligne de commande **-keepdb**. Utilisez la propriété de ligne de commande **-keepdb** pour conserver l'identificateur unique du client actuel afin qu'il soit utilisé par le nouveau client que vous installez.

   Par exemple, créez un script nommé **upgrade.sh** contenant les lignes suivantes :

   ```
   #!/bin/sh
   #
   /tmp/PATCH/install -sitecode <code> -mp <hostname> -keepdb /tmp/PATCH/ccm-Universal-x64.<build>.tar
   ```

   Copiez-le ensuite dans le dossier **/tmp/PATCH** sur l'ordinateur client.

3. Utilisez le déploiement de logiciels pour que chaque client utilise la commande **at** intégrée de l'ordinateur pour exécuter le script **upgrade.sh** avec un court délai avant l'exécution du script.

   Par exemple, utilisez la ligne de commande suivante pour exécuter le script : **at -f /tmp/upgrade.sh -m now + 5 minutes**

   Une fois que le client a correctement planifié l'exécution du script **upgrade.sh** , le client envoie un message d'état indiquant que le déploiement de logiciels s'est terminé avec succès. Toutefois, l'installation du client actuel est ensuite gérée par l'ordinateur, une fois le délai écoulé. Une fois la mise à niveau du client terminée, validez l'installation en consultant le fichier **/var/opt/microsoft/scxcm.log** sur l'ordinateur client. Vérifiez que le client est installé et qu'il communique avec le site en affichant les détails relatifs au client dans le nœud **Appareils** de l'espace de travail **Ressources et Conformité** dans la console Configuration Manager.

# Comment mettre à niveau les clients sur les ordinateurs Mac dans System Center Configuration Manager

10/07/2018 • 7 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Suivez les étapes générales décrites ci-dessous pour mettre à niveau le client pour des ordinateurs Mac à l'aide d'une application System Center Configuration Manager. Vous pouvez également télécharger le fichier d'installation du client Mac, le copier dans un emplacement réseau partagé ou un dossier local sur l'ordinateur Mac puis demander aux utilisateurs d'exécuter l'installation manuellement.

> **NOTE**
> Avant d'effectuer ces étapes, assurez-vous que votre ordinateur Mac dispose de la configuration requise. Consultez Systèmes d'exploitation pris en charge pour les ordinateurs Mac.

## Étape 1 : Télécharger le dernier fichier d'installation du client Mac à partir du Centre de téléchargement Microsoft

Le client Mac pour Configuration Manager n'est pas fourni sur le support d'installation de Configuration Manager et doit être téléchargé à partir du Centre de téléchargement Microsoft. Les fichiers d'installation du client Mac sont contenus dans un fichier Windows Installer nommé ConfigmgrMacClient.msi.

Vous pouvez télécharger ce fichier à partir du Centre de téléchargement Microsoft.

## Étape 2 : Exécuter le fichier d'installation téléchargé pour créer le fichier d'installation du client Mac

Sur un ordinateur exécutant Windows, exécutez **ConfigmgrMacClient.msi** que vous avez téléchargé pour décompresser le fichier d'installation du client Mac, nommé **Macclient.dmg**. Ce fichier est disponible, par défaut, dans le dossier **C:\Program Files (x86)\Microsoft\System Center 2012 Configuration Manager Mac Client** sur l'ordinateur Windows une fois que vous avez décompressé les fichiers.

## Étape 3 : Extraire les fichiers d'installation du client

Copiez le fichier Macclient.dmg dans un partage réseau ou dans un dossier local sur un ordinateur Mac. Puis, sur l'ordinateur Mac, montez et ouvrez le fichier Macclient.dmg et copiez les fichiers dans un dossier sur l'ordinateur Mac.

## Étape 4 : Créer un fichier .cmmac pouvant être utilisé pour créer une application

1. Utilisez l'outil **CMAppUtil** (disponible dans le dossier **Outils** des fichiers d'installation du client Mac) pour créer un fichier .cmmac à partir du package d'installation du client. Ce fichier sera utilisé pour créer l'application Configuration Manager.

2. Copiez le nouveau fichier **CMClient.pkg.cmmac** dans un emplacement disponible pour l'ordinateur qui

exécute la console Configuration Manager.

Pour plus d'informations, consultez Procédures supplémentaires de création et de déploiement d'applications pour ordinateurs Mac.

## **Étape 5 :** Créer et déployer une application contenant les fichiers du client Mac

1. Dans la console Configuration Manager, créez une application à partir du fichier **CMClient.pkg.cmmac** qui contient les fichiers d'installation du client.
2. Déployez cette application sur les ordinateurs Mac de votre hiérarchie.

   Pour plus d'informations, consultez Création d'applications pour ordinateurs Mac avec System Center Configuration Manager.

## Step 6 : Les utilisateurs installent la dernière version du client

Les utilisateurs de clients Mac seront informés qu'une mise à jour du client Configuration Manager est disponible et qu'elle doit être installée. Une fois que les utilisateurs installent le client, ils doivent redémarrer leur ordinateur Mac.

Après le redémarrage de l'ordinateur, l'Assistant Inscription d'ordinateur s'exécute automatiquement pour demander un nouveau certificat d'utilisateur. L'Assistant Inscription d'ordinateur sera automatiquement exécuté uniquement lors de la première installation du client SCCM. Et il ne sera pas réexécuté si vous essayez de mettre à jour le client avec un nouveau programme d'installation ultérieurement dans la mesure où il a déjà un certificat utilisateur valide.

Si vous n'utilisez pas l'inscription Configuration Manager, mais que vous installez le certificat client indépendamment de Configuration Manager, consultez Configurer le client mis à niveau pour qu'il utilise un certificat existant.

## Configure the upgraded client to use an existing certificate

Exécutez la procédure suivante pour empêcher l'exécution de l'Assistant Inscription ordinateur et pour configurer le client mis à niveau afin qu'il utilise un certificat client existant.

- Dans la console Configuration Manager, créez un élément de configuration du type **Mac OS X**.
- Ajoutez un paramètre à cet élément de configuration avec le type de paramètre **Script**.
- Ajoutez le script suivant au paramètre :

```
#!/bin/sh
echo "Starting script\n"
echo "Changing directory to MAC Client\n"
cd /Users/Administrator/Desktop/'MAC Client'/
echo "Import root cert\n"
/usr/bin/sudo /usr/bin/security import /Users/Administrator/Desktop/'MAC Client'/Root.pfx -A -k
/Library/Keychains/System.Keychain -P ROOT
echo "Using openssl to convert pfx to a crt\n"
/usr/bin/sudo openssl pkcs12 -in /Users/Administrator/Desktop/'MAC Client'/Root.pfx -out Root1.crt -
nokeys -clcerts -passin pass:ROOT
echo "Adding trust to root cert\n"
/usr/bin/sudo /usr/bin/security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.Keychain
Root1.crt
echo "Import client cert\n"
/usr/bin/sudo /usr/bin/security import /Users/Administrator/Desktop/'MAC Client'/MacClient.pfx -A -k
/Library/Keychains/System.Keychain -P MAC
echo "Executing ccmclient with MP\n"
sudo ./ccmsetup -MP https://SCCM34387.SCCM34387DOM.NET/omadm/cimhandler.ashx
echo "Editing Plist file\n"
sudo /usr/libexec/Plistbuddy -c 'Add:SubjectName string CMMAC003L' /Library/'Application
Support'/Microsoft/CCM/ccmclient.plist
echo "Changing directory to CCM\n"
cd /Library/'Application Support'/Microsoft/CCM/
echo "Making connection to the server\n"
sudo open ./CCMClient
echo "Ending Script\n"
exit
```

- Ajoutez l'élément de configuration à une base de référence de configuration, puis déployez cette dernière sur tous les ordinateurs Mac qui installent un certificat indépendamment de Configuration Manager.

  Pour plus d'informations sur la création et le déploiement d'éléments de configuration pour des ordinateurs Mac, consultez Comment créer des éléments de configuration pour des appareils Mac OS X gérés avec le client System Center Configuration Manager et Comment déployer des bases de référence de configuration dans System Center Configuration Manager.

# Intégrer Upgrade Readiness à System Center Configuration Manager

02/07/2018 • 10 minutes to read • Edit Online

*S'applique à : System Center Configuration Manager (Current Branch)*

Upgrade Readiness (anciennement Upgrade Analytics) fait partie de Windows Analytics qui vous permet d'évaluer et d'analyser l'état de préparation des appareils de votre environnement pour une mise à niveau vers Windows 10. Vous pouvez configurer la version spécifique. Vous pouvez intégrer Upgrade Readiness à Configuration Manager pour accéder aux données de compatibilité de mise à niveau du client dans la console d'administration de Configuration Manager. Vous êtes en mesure de cibler des appareils pour des mises à niveau ou mises à jour à l'aide de regroupements dynamiques créés en fonction de ces données.

Upgrade Readiness est une solution qui s'exécute sur Operations Management Suite (OMS). Pour en savoir plus sur Upgrade Readiness, consultez Gérer les mises à niveau de Windows avec Upgrade Readiness.

## Configurer des clients

Upgrade Readiness, comme toutes les solutions Windows Analytics, s'appuie sur les données de télémétrie Windows. Pour qu'Upgrade Readiness reçoive suffisamment de données de télémétrie, les prérequis suivants doivent être satisfaits :

- Tous les clients doivent être configurés avec une **clé d'ID commercial**.
- Le niveau de base de la télémétrie doit au minimum être configuré pour les clients Windows 10.
- Les clients exécutant des versions antérieures sur Windows doivent installer des bases de connaissances spécifiques comme décrit dans Prise en main d'Upgrade Readiness. Ils doivent également avoir activer la télémétrie dans les **paramètres client**.

La clé d'ID commercial et la télémétrie Windows peuvent être configurées dans les **paramètres client**. Pour en savoir plus, consultez Utiliser Windows Analytics avec Configuration Manager.

> **NOTE**
> Si Upgrade Readiness ne reçoit pas comme prévu les données de télémétrie envoyées par les appareils de votre environnement, vous pouvez traiter certains de ces problèmes à l'aide du script de déploiement Upgrade Readiness. Toutefois, dans la plupart des environnements, le déploiement des bases de connaissances appropriées, ainsi que la configuration de la clé d'ID commercial et de la télémétrie dans les **Paramètres client** devraient suffire.

## Connecter Configuration Manager à Upgrade Readiness

À compter de Current Branch version 1706, l'Assistant Services Azure est utilisé pour simplifier le processus de configuration des services Azure que vous utilisez avec Configuration Manager. Pour connecter Configuration Manager à Upgrade Readiness, une inscription d'application Azure AD de type *application web/API* doit être créée dans le portail Azure. Pour en savoir plus sur la création d'une inscription d'application, consultez Inscrire votre application avec un client Azure Active Directory. Dans le **portail Azure**, vous devez également donner à votre application web tout juste inscrite des autorisations de *contributeur* sur le groupe de ressources qui contient l'espace de travail OMS qui héberge vos données Upgrade Readiness. L'**Assistant Services Azure** utilise cette inscription d'application pour permettre à Configuration Manager de communiquer en toute sécurité avec Azure AD et de connecter votre infrastructure à vos données Upgrade Readiness.

**IMPORTANT**

Les autorisations de *contributeur* doivent être accordées à l'application elle-même, contrairement à une identité d'utilisateur Azure AD. En effet, c'est l'application inscrite et non un utilisateur Azure AD qui accède aux données pour le compte de votre infrastructure Configuration Manager. Pour accorder les autorisations, vous devez rechercher le nom de l'inscription d'application dans la zone **Ajouter des utilisateurs** au moment d'attribuer l'autorisation. Il s'agit du même processus que celui à suivre pour accorder à Configuration Manager les autorisations d'accès à OMS pour les connexions à Log Analytics. Ces étapes doivent être effectuées avant d'importer l'inscription d'application dans Configuration Manager avec l'*Assistant Services Azure*.

**Utiliser l'Assistant Azure pour créer la connexion**

Suivez les instructions données dans Configurer les services Azure à utiliser avec Configuration Manager pour créer une connexion à Upgrade Readiness en important l'inscription d'application web créée ci-dessus.

Dans la page *Configuration*, les valeurs suivantes sont préremplies si l'importation d'application web a réussi et si les autorisations appropriées sont affectées dans le **portail Azure**.

- Abonnements Azure
- Groupe de ressources Azure
- Espace de travail Windows Analytics

Plusieurs groupes de ressources ou espaces de travail sont disponibles uniquement si l'application web Azure AD inscrite dispose d'autorisations de *contributeur* sur plusieurs groupes de ressources ou si le groupe de ressources sélectionné comprend plusieurs espaces de travail OMS.

## Afficher et utiliser les informations Upgrade Readiness dans Configuration Manager

Une fois que vous avez intégré Upgrade Readiness à Configuration Manager, vous pouvez afficher l'analyse de la préparation de vos clients pour la mise à niveau.

1. Dans la console Configuration Manager, choisissez **Surveillance** > **Vue d'ensemble** > **Upgrade Readiness**.
2. Passez en revue les données, notamment l'état de préparation à la mise à niveau et le pourcentage d'appareils Windows qui envoient des données de télémétrie.
3. Vous pouvez filtrer le tableau de bord pour afficher les données d'appareils dans des regroupements spécifiques.
4. Vous pouvez afficher les appareils dans un état de préparation particulier et créer un regroupement dynamique pour ces derniers afin de pouvoir les mettre à niveau s'ils sont prêts ou effectuer les actions nécessaires pour corriger les appareils dont la mise à niveau est bloquée.

## Utilisation du connecteur Upgrade Readiness (versions 1702 et antérieures)

Dans Configuration Manager version 1702 ou antérieure, une autre série d'étapes et d'exigences est nécessaire pour créer une connexion à Upgrade Readiness.

**Prérequis**

- Pour ajouter la connexion, votre environnement Configuration Manager doit d'abord configurer un point de connexion de service dans un mode en ligne. Quand vous ajoutez la connexion à votre environnement, Microsoft Monitoring Agent est également installé sur l'ordinateur exécutant ce rôle de système de site.
- Inscrivez Configuration Manager comme outil de gestion « Application web et/ou API web » et obtenez l'ID de client résultant de cette inscription.
- Créer une clé de client pour l'outil de gestion inscrit dans Azure Active Directory.

- Dans le portail Azure, autorisez l'application web inscrite à accéder à OMS en suivant les étapes décrites dans Accorder à Configuration Manager les autorisations d'accès à OMS.

> **IMPORTANT**
> Quand vous configurez l'autorisation d'accès à OMS, choisissez le rôle **Collaborateur** et accordez-lui les autorisations sur le groupe de ressources de l'application inscrite.

**Créer la connexion**

1. Dans la console Configuration Manager, choisissez **Administration** > **Services cloud** > **Connecteur Upgrade Readiness** > **Créer une connexion à Upgrade Analytics** pour démarrer l'**Assistant Ajout d'une connexion Upgrade Analytics**.
2. Dans l'écran **Azure Active Directory**, indiquez les valeurs de **Locataire**, **ID de client** et **Clé secrète du client**, puis sélectionnez **Suivant**.
3. Dans l'écran **Upgrade Readiness**, définissez vos paramètres de connexion en renseignant les champs **Abonnement Azure**, **Groupe de ressources Azure** et **Espace de travail Operations Management Suite**.
4. Vérifiez vos paramètres de connexion dans l'écran **Résumé**, puis sélectionnez **Suivant**.

> **NOTE**
> Vous devez connecter Upgrade Readiness au site de niveau supérieur de votre hiérarchie. Si vous connectez Upgrade Readiness à un site principal autonome et que vous ajoutez ensuite un site d'administration centrale à votre environnement, vous devez supprimer et recréer la connexion OMS au sein de la nouvelle hiérarchie.