# Installation de VMware Horizon View

Présentation 5.2
Présentation Manager 5.2
Présentation Composer 5.2

Ce document prend en charge la version de chacun des produits répertoriés, ainsi que toutes les versions publiées par la suite jusqu'au remplacement dudit document par une nouvelle édition. Pour rechercher des éditions plus récentes de ce document, rendez-vous sur : http://www.vmware.com/fr/support/pubs.

FR-001020-00

vmware®

Vous trouverez la documentation technique la plus récente sur le site Web de VMware à l'adresse :

http://www.vmware.com/fr/support/

Le site Web de VMware propose également les dernières mises à jour des produits.

N'hésitez pas à nous transmettre tous vos commentaires concernant cette documentation à l'adresse suivante :

docfeedback@vmware.com



**VMware, Inc.**
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

**VMware, Inc.**
100-101 Quartier Boieldieu
92042 Paris La Défense
France
www.vmware.com/fr

# Table des matières

# Installation de VMware Horizon View

Le document *Installation de VMware Horizon View* explique comment installer les composants serveur et client VMware® Horizon View™.

## Public cible

Ces informations sont destinées à toute personne souhaitant installer VMware Horizon View. Les informations sont destinées aux administrateurs système Windows ou Linux expérimentés qui connaissent bien le fonctionnement des datacenters et de la technologie des machines virtuelles.

# Configuration requise pour les composants serveur 1

Les hôtes exécutant des composants serveur VMware Horizon View doivent satisfaire des exigences matérielles et logicielles spécifiques.

Ce chapitre aborde les rubriques suivantes :



## Exigences de View Connection Server

View Connection Server agit comme un broker pour les connexions client en authentifiant et en dirigeant les demandes entrantes d'utilisateur vers le poste de travail View approprié. View Connection Server a des exigences matérielles, de système d'exploitation, d'installation et de logiciels pris en charge spécifiques.

- Exigences matérielles de Serveur de connexion View page 8

  Vous devez installer tous les types d'installations de Serveur de connexion View, notamment les installations standard, de réplica et de serveur de sécurité, sur une machine physique ou virtuelle dédiée ayant la configuration matérielle requise.

- Systèmes d'exploitation pris en charge pour Serveur de connexion View page 8

  Vous devez installer Serveur de connexion View sur un système d'exploitation Windows Server 2008 R2.

- Exigences de logiciel de virtualisation pour le serveur de connexion View page 8

  Serveur de connexion View requiert certaines versions du logiciel de virtualisation VMware.

- Exigences de réseau pour des instances répliquées de Serveur de connexion View page 9

  Si vous installez des instances répliquées de Serveur de connexion View, configurez les instances dans le même emplacement et connectez-les sur un réseau LAN haute performance.

## Exigences matérielles de Serveur de connexion View

Vous devez installer tous les types d'installations de Serveur de connexion View, notamment les installations standard, de réplica et de serveur de sécurité, sur une machine physique ou virtuelle dédiée ayant la configuration matérielle requise.

**Tableau 1-1.** Exigences matérielles de Serveur de connexion View

| Composant matériel | Requis | Recommandé |
|---|---|---|
| Processeur | Processeur Pentium IV 2 GHz ou plus | 4 CPU |
| Réseau | Une ou plusieurs cartes réseau de 10/100 Mbits/s | Des cartes réseau de 1 Gbit/s |
| Mémoire<br>Windows Server 2008 64 bits | RAM de 4 Go ou plus | Au moins RAM de 10 Go pour les déploiements de 50 postes de travail View ou plus |

Ces exigences s'appliquent également à des instances de Serveur de connexion View de réplica et de serveur de sécurité que vous installez pour une disponibilité élevée ou un accès externe.

**IMPORTANT** La machine physique ou virtuelle qui héberge Serveur de connexion View doit utiliser une adresse IP statique.

## Systèmes d'exploitation pris en charge pour Serveur de connexion View

Vous devez installer Serveur de connexion View sur un système d'exploitation Windows Server 2008 R2.

Les systèmes d'exploitation suivants prennent en charge tous les types d'installations de Serveur de connexion View, y compris les installations standard, de réplica et de serveur de sécurité.

**Tableau 1-2.** Prise en charge de système d'exploitation pour Serveur de connexion View

| Système d'exploitation | Version | Édition |
|---|---|---|
| Windows Server 2008 R2 | 64 bits | Standard<br>Enterprise |
| Windows Server 2008 R2 SP1 | 64 bits | Standard<br>Enterprise |

## Exigences de logiciel de virtualisation pour le serveur de connexion View

Serveur de connexion View requiert certaines versions du logiciel de virtualisation VMware.

Si vous utilisez vSphere, vous devez utiliser une version prise en charge des hôtes de vSphere ESX/ESXi et de vCenter Server.

Pour plus d'informations sur les versions d'Horizon View compatibles avec les versions de vCenter Server et ESX/ESXi, consultez la matrice d'interopérabilité des produits VMware à l'adresse http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

### Exigences de réseau pour des instances répliquées de Serveur de connexion View

Si vous installez des instances répliquées de Serveur de connexion View, configurez les instances dans le même emplacement et connectez-les sur un réseau LAN haute performance.

Lorsque vous installez des instances répliquées de Serveur de connexion View, vous devez configurer les instances dans le même emplacement physique et les connecter sur un réseau LAN haute performance. N'utilisez pas un réseau WAN, un réseau MAN (Metropolitan Area Network) ou autre réseau non LAN pour connecter des instances répliquées de Serveur de connexion View.

Même un réseau WAN, MAN ou autre réseau non LAN haute performance avec une latence faible et un débit élevé peut connaître des périodes pendant lesquelles le réseau ne peut pas fournir les caractéristiques de performance nécessaires pour que des instances de Serveur de connexion View préservent la cohérence.

Si les configurations View LDAP sur des instances de Serveur de connexion View deviennent incohérentes, les utilisateurs peuvent ne pas être capables d'accéder à leurs postes de travail. L'accès d'un utilisateur peut être refusé lors de la connexion à une instance de Serveur de connexion View avec une configuration périmée.

## Exigences de View Administrator

Des administrateurs utilisent View Administrator pour configurer Serveur de connexion View, déployer et gérer des postes de travail, contrôler l'authentification utilisateur, initier et examiner des événements système et effectuer des activités analytiques. Les systèmes client qui exécutent View Administrator doivent satisfaire un certain nombre d'exigences.

View Administrator est une application Web installée lorsque vous installez Serveur de connexion View. Vous pouvez accéder et utiliser View Administrator avec les navigateurs Web suivants :

- Internet Explorer 8
- Internet Explorer 9
- Internet Explorer 10 (sur un système Windows 8 en mode Bureau)
- Firefox 6 et versions supérieures

Pour utiliser View Administrator avec votre navigateur Web, vous devez installer Adobe Flash Player 10 ou supérieur. Votre système client doit avoir un accès à Internet pour permettre l'installation d'Adobe Flash Player.

L'ordinateur sur lequel vous lancez View Administrator doit approuver les certificats racine et intermédiaires du serveur qui héberge Serveur de connexion View. Les navigateurs pris en charge contiennent déjà des certificats pour toutes les autorités de certification reconnues. Si vos certificats proviennent d'une autorité de certification qui n'est pas reconnue, vous devez suivre les instructions du document *Installation de VMware Horizon View* sur l'importation des certificats racine et intermédiaires.

Pour afficher le texte correctement, View Administrator requiert des polices spécifiques de Microsoft. Si votre navigateur Web s'exécute sur un système d'exploitation autre que Windows, tel que Linux, UNIX ou Mac OS X, assurez-vous que des polices Microsoft sont installées sur votre ordinateur.

Actuellement, le site Web Microsoft ne distribue pas de polices Microsoft, mais vous pouvez les télécharger sur des sites Web indépendants.

# Exigences de View Composer

View Manager utilise View Composer pour déployer plusieurs postes de travail de clone lié à partir d'une image de base centrale unique. View Composer a des exigences d'installation et de stockage spécifiques.

- Systèmes d'exploitation pris en charge pour View Composer page 10

  View Composer prend en charge les systèmes d'exploitation 64 bits avec des exigences et des limites spécifiques. Vous pouvez installer View Composer sur la même machine physique ou virtuelle que vCenter Server ou sur un serveur distinct.

- Exigences matérielles de View Composer autonome page 10

  Avec View 5.1 et versions supérieures, View Composer n'a plus besoin d'être installé sur la même machine physique ou virtuelle que vCenter Server. Si vous installez View Composer sur un serveur séparé, vous devez utiliser une machine physique ou virtuelle dédiée qui satisfait des exigences matérielles spécifiques.

- Exigences de base de données pour View Composer page 11

  View Composer requiert une base de données SQL pour stocker des données. La base de données View Composer doit résider sur, ou être disponible pour, l'hôte du serveur View Composer.

## Systèmes d'exploitation pris en charge pour View Composer

View Composer prend en charge les systèmes d'exploitation 64 bits avec des exigences et des limites spécifiques. Vous pouvez installer View Composer sur la même machine physique ou virtuelle que vCenter Server ou sur un serveur distinct.

**Tableau 1-3.** Support de système d'exploitation pour View Composer

| Système d'exploitation | Version | Édition |
|---|---|---|
| Windows Server 2008 R2 | 64 bits | Standard<br>Enterprise |
| Windows Server 2008 R2 SP1 | 64 bits | Standard<br>Enterprise |

Si vous envisagez d'installer View Composer sur une machine physique ou virtuelle différente de celle de vCenter Server, voir « Exigences matérielles de View Composer autonome », page 10.

## Exigences matérielles de View Composer autonome

Avec View 5.1 et versions supérieures, View Composer n'a plus besoin d'être installé sur la même machine physique ou virtuelle que vCenter Server. Si vous installez View Composer sur un serveur séparé, vous devez utiliser une machine physique ou virtuelle dédiée qui satisfait des exigences matérielles spécifiques.

Une installation de View Composer autonome fonctionne avec vCenter Server installé sur un ordinateur Windows Server et avec vCenter Server Appliance basé sur Linux. VMware recommande d'avoir un mappage un-à-un entre chaque service View Composer et instance de vCenter Server.

**Tableau 1-4.** Exigences matérielles de View Composer

| Composant matériel | Requise | Recommandé |
|---|---|---|
| Processeur | Processeur Intel 64 ou AMD 64 1,4 GHz ou plus avec 2 CPU | 2 GHz ou plus et 4 CPU |
| Réseau | Une ou plusieurs cartes réseau de 10/100 Mbits/s | Des cartes réseau de 1 Gbit/s |

**Tableau 1-4.** Exigences matérielles de View Composer (suite)

| Composant matériel | Requise | Recommandé |
|---|---|---|
| Mémoire | RAM de 4 Go ou plus | RAM de 8 Go ou plus pour des déploiements de 50 postes de travail View ou plus |
| Espace disque | 40 Go | 60 Go |

**IMPORTANT** La machine physique ou virtuelle qui héberge View Composer doit utiliser une adresse IP statique.

## Exigences de base de données pour View Composer

View Composer requiert une base de données SQL pour stocker des données. La base de données View Composer doit résider sur, ou être disponible pour, l'hôte du serveur View Composer.

Si un serveur de base de données existe déjà pour vCenter Server, View Composer peut utiliser ce serveur s'il s'agit d'une version répertoriée dans le Tableau 1-5. Par exemple, View Composer peut utiliser l'instance de Microsoft SQL Server 2005 ou 2008 Express fournie avec vCenter Server. Si aucun serveur de base de données n'existe, vous devez en installer un.

View Composer prend en charge un sous-ensemble des serveurs de base de données que vCenter Server prend en charge. Si vous utilisez déjà vCenter Server avec un serveur de base de données qui n'est pas pris en charge par View Composer, continuez à utiliser ce serveur de base de données pour vCenter Server et installez un serveur de base de données séparé à utiliser pour des événements de base de données View Composer et View Manager.

**IMPORTANT** Si vous créez la base de données View Composer sur la même instance de SQL Server que vCenter Server, ne remplacez pas la base de données vCenter Server.

Tableau 1-5 répertorie les serveurs de base de données pris en charge et leurs versions. Pour voir une liste complète des versions de base de données prises en charge avec vCenter Server, consultez les *matrices de compatibilité de VMware vSphere* sur le site Web de documentation de VMware vSphere.

Les versions de vCenter Server répertoriées dans les titres de colonne de tableau sont générales. Pour voir les versions de mise à jour prises en charge spécifiques de chaque version de vCenter Server, consultez les *Matrices de compatibilité de VMware vSphere* dans la documentation présente sur le site Web de VMware vSphere.

**Tableau 1-5.** Serveurs de base de données pris en charge pour View Composer

| Base de données | vCenter Server 5.1 | vCenter Server 5,0 | vCenter Server 4.1 | vCenter Server 4,0 |
|---|---|---|---|---|
| Microsoft SQL Server 2005 (SP4), Standard, Enterprise et Datacenter (32 et 64 bits) | Oui | Oui | Standard uniquement | Standard uniquement |
| Microsoft SQL Server 2008 Express (R2 SP1) (64 bits) | Oui | Oui | Non | Non |
| Microsoft SQL Server 2008 (SP2), Standard, Enterprise et Datacenter (32 et 64 bits) | Oui | Oui | Oui | Oui |
| Microsoft SQL Server 2008 (R2), Standard et Enterprise (32 et 64 bits) | Oui | Oui | Oui | Oui |

**Tableau 1-5.** Serveurs de base de données pris en charge pour View Composer (suite)

| Base de données | vCenter Server 5.1 | vCenter Server 5,0 | vCenter Server 4.1 | vCenter Server 4,0 |
|---|---|---|---|---|
| Oracle 10g Release 2, Standard, Standard ONE et Enterprise [10.2.0.4]<br>(32 et 64 bits) | Oui | Oui | Oui | Oui |
| Oracle 11g Release 2, Standard, Standard ONE et Enterprise [11.2.0.1]<br>avec Patch 5<br>(32 et 64 bits) | Oui | Oui | Oui | Oui |

**Remarque** Si vous utilisez une base de données Oracle 11g R2, vous devez installer Oracle 11.2.0.1 Patch 5. Ce correctif s'applique aux versions 32 et 64 bits.

# Exigences de View Transfer Server

View Transfer Server est un composant facultatif de View Manager qui prend en charge la restitution, l'emprunt et la réplication de postes de travail exécutés en mode local. View Transfer Server a des exigences d'installation, de système d'exploitation et de stockage spécifiques.

- Exigences d'installation et de mise à niveau du serveur de transfert View page 12

  Vous devez installer Serveur de transfert View comme application Windows dans une machine virtuelle qui satisfait des exigences spécifiques.

- Systèmes d'exploitation pris en charge pour Serveur de transfert View page 13

  Vous devez installer Serveur de transfert View sur un système d'exploitation pris en charge avec au moins la quantité minimale requise de RAM.

- Exigences de stockage pour View Transfer Server page 13

  View Transfer Server transfère du contenu statique vers et depuis le référentiel de Transfer Server et du contenu dynamique entre des postes de travail locaux et des postes de travail distants dans le datacenter. View Transfer Server a des exigences de stockage spécifiques.

## Exigences d'installation et de mise à niveau du serveur de transfert View

Vous devez installer Serveur de transfert View comme application Windows dans une machine virtuelle qui satisfait des exigences spécifiques.

**Important** Si des utilisateurs vont emprunter des postes de travail locaux qui utilisent le format de disque fragmenté à optimisation d'espace (SE-Flex), disponible à partir de vSphere 5.1, Serveur de transfert View doit être hébergé sur une machine virtuelle vSphere 5.1 ou supérieur (version matérielle virtuelle 9). Le format de disque fragmenté à optimisation d'espace permet de récupérer des données périmées ou supprimées dans un système d'exploitation client avec un processus d'effacement et de réduction.

Pour utiliser la fonction de récupération d'espace, vous devez vérifier que vos hôtes de vCenter Server sont à la version 5.1 avec le correctif de téléchargement ESXi 5.1 ESXi510-201212001 ou supérieur. Dans un cluster ESXi, vérifiez que tous les hôtes sont à la version 5.1 avec le correctif de téléchargement ESXi510-201212001 ou supérieur.

La machine virtuelle qui héberge Serveur de transfert View doit satisfaire plusieurs exigences concernant la connectivité réseau :

- Il doit être géré par la même instance de vCenter Server que les postes de travail locaux qu'il gérera.
- Elle ne doit pas faire partie d'un domaine.
- Elle doit utiliser une adresse IP statique.

Le logiciel Serveur de transfert View ne peut pas coexister sur la même machine virtuelle avec tout autre composant logiciel View Manager, notamment Serveur de connexion View.

N'ajoutez ou ne supprimez pas manuellement des périphériques PCI sur la machine virtuelle qui héberge Serveur de transfert View. Si vous ajoutez ou supprimez des périphériques PCI, View peut être incapable de découvrir des périphériques ajoutés à chaud, ce qui peut entraîner l'échec des opérations de transfert des données.

Vous pouvez installer plusieurs instances de Serveur de transfert View pour une haute disponibilité et une évolutivité.

## Systèmes d'exploitation pris en charge pour Serveur de transfert View

Vous devez installer Serveur de transfert View sur un système d'exploitation pris en charge avec au moins la quantité minimale requise de RAM.

**Tableau 1-6.** Prise en charge de systèmes d'exploitation pour Serveur de transfert View

| Système d'exploitation | Version | Édition | RAM minimale |
|---|---|---|---|
| Windows Server 2008 R2 | 64 bits | Standard<br>Enterprise | 4 Go |
| Windows Server 2008 R2 SP1 | 64 bits | Standard<br>Enterprise | 4 Go |

**IMPORTANT** Configurez deux CPU virtuelles pour les machines virtuelles qui hébergent Serveur de transfert View.

## Exigences de stockage pour View Transfer Server

View Transfer Server transfère du contenu statique vers et depuis le référentiel de Transfer Server et du contenu dynamique entre des postes de travail locaux et des postes de travail distants dans le datacenter. View Transfer Server a des exigences de stockage spécifiques.

- Le disque dur sur lequel vous configurez le référentiel de Transfer Server doit comporter suffisamment d'espace pour stocker vos fichiers d'image statique. Les fichiers d'image sont des images de base View Composer.
- View Transfer Server doit avoir accès aux magasins de données qui stockent les disques de poste de travail à transférer. Les magasins de données doivent être accessibles depuis l'hôte ESX/ESXi sur lequel la machine virtuelle View Transfer Server est exécutée.
- Le nombre maximum recommandé de transferts de disque simultanés que View Transfer Server peut prendre en charge est 20.

  Lors d'une opération de transfert, le disque virtuel d'un poste de travail local est monté sur View Transfer Server. La machine virtuelle View Transfer Server a quatre contrôleurs SCSI. Cette configuration permet de lier plusieurs disques à la machine virtuelle à la fois.
- Comme les postes de travail locaux peuvent contenir des données utilisateur sensibles, assurez-vous que les données sont cryptées lors de leur transfert sur le réseau.

  Dans View Administrator, vous pouvez configurer des options de sécurité pour le transfert des données sur chaque instance de View Connection Server. Pour configurer ces options dans View Administrator, cliquez sur **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** , sélectionnez une instance de View Connection Server et cliquez sur **[Edit (Modifier)]** .
- Lorsque View Transfer Server est ajouté à View Manager, sa stratégie d'automatisation DRS (Distributed Resource Scheduler) est définie sur Manual (Manuel), ce qui désactive efficacement DRS.

Pour migrer une instance de View Transfer Server sur un autre hôte ESX ou magasin de données, vous devez placer l'instance en mode de maintenance avant de commencer la migration.

Lorsque View Transfer Server est supprimé de View Manager, la règle d'automatisation DRS est réinitialisée à la valeur qu'elle avait avant l'ajout de View Transfer Server à View Manager.

# Configuration requise pour les systèmes d'exploitation client 2

Les systèmes exécutant View Agent ou View Persona Management autonome doivent satisfaire certaines exigences matérielles et logicielles.

Ce chapitre aborde les rubriques suivantes :



## Systèmes d'exploitation pris en charge pour View Agent

Le composant View Agent facilite la gestion des sessions, l'ouverture de session unique et la redirection de périphérique. Vous devez installer View Agent sur l'ensemble des machines virtuelles, des systèmes physiques et des serveurs Terminal Server qui seront gérés par View Manager.

**Tableau 2-1.** Prise en charge de systèmes d'exploitation pour View Agent

| Système d'exploitation client | Version | Édition | Service Pack |
|---|---|---|---|
| Windows 8 | 64 bits et 32 bits | Enterprise et Professional | S/O |
| Windows 7 | 64 bits et 32 bits | Enterprise et Professional | Aucun et SP1 |
| Windows Vista | 32 bits | Business et Enterprise | SP1 et SP2 |
| Windows XP | 32 bits | Professional | SP3 |
| Windows 2008 R2 Terminal Server | 64 bits | Standard | SP1 |
| Windows 2008 Terminal Server | 64 bits | Standard | SP2 |

Pour utiliser l'option de configuration de View Persona Management avec View Agent, vous devez installer View Agent sur des machines virtuelles Windows 8, Windows 7, Windows Vista ou Windows XP. Cette option ne fonctionne pas sur des ordinateurs physiques ou sur des serveurs Microsoft Terminal Server.

Vous pouvez installer la version autonome de View Persona Management sur des ordinateurs physiques. Reportez-vous à la section « Systèmes d'exploitation pris en charge pour View Persona Management autonome », page 16.

# Systèmes d'exploitation pris en charge pour View Persona Management autonome

Le logiciel View Persona Management autonome fournit la gestion de persona pour les ordinateurs physiques et les machines virtuelles autonomes sur lesquels View Agent 5.*x* n'est pas installé. Lorsque des utilisateurs se connectent, leurs profils sont téléchargés dynamiquement depuis un référentiel de profils distant vers leurs systèmes autonomes.

**Remarque** Pour configurer View Persona Management pour les postes de travail View, installez View Agent avec l'option de configuration **[View Persona Management]**. Le logiciel View Persona Management autonome est conçu uniquement pour les systèmes non View.

La section Tableau 2-2 répertorie les systèmes d'exploitation pris en charge pour le logiciel View Persona Management autonome.

**Tableau 2-2.** Systèmes d'exploitation pris en charge pour View Persona Management autonome

| Guest Operating System | Version | Édition | Service Pack |
|---|---|---|---|
| Windows 8 | 64 bits et 32 bits | Pro - Desktop et Enterprise - Desktop | S/O |
| Windows 7 | 64 bits et 32 bits | Enterprise et Professional | Aucun et SP1 |
| Windows Vista | 32 bits | Business et Enterprise | SP1 et SP2 |
| Windows XP | 32 bits | Professional | SP3 |

Le logiciel View Persona Management autonome n'est pas pris en charge sur les Services Terminal Server Microsoft ou les Services Bureau à distance Microsoft.

# Prise en charge du protocole d'affichage à distance et logicielle

Les protocoles d'affichage à distance et logicielles fournissent un accès aux postes de travail d'ordinateurs distants sur une connexion réseau. View Client prend en charge le protocole RDP (Remote Desktop Protocol) de Microsoft et PCoIP de VMware.

- Horizon View avec PCoIP page 16

  PCoIP offre une utilisation optimisée du poste de travail pour délivrer l'intégralité de l'environnement de poste de travail, y compris des applications, des images, du contenu audio et vidéo, à un grand nombre d'utilisateurs sur le réseau LAN ou sur le réseau WAN. PCoIP peut compenser une augmentation de la latence ou une réduction de la bande passante, et garantir ainsi que les utilisateurs finaux peuvent rester productifs quelles que soient les conditions du réseau.

- Microsoft RDP page 18

  Remote Desktop Protocol est le même protocole multicanal que de nombreuses personnes utilisent déjà pour accéder à leur ordinateur professionnel depuis leur ordinateur à domicile. La Connexion Bureau à distance Microsoft utilise RDP pour transmettre des données.

## Horizon View avec PCoIP

PCoIP offre une utilisation optimisée du poste de travail pour délivrer l'intégralité de l'environnement de poste de travail, y compris des applications, des images, du contenu audio et vidéo, à un grand nombre d'utilisateurs sur le réseau LAN ou sur le réseau WAN. PCoIP peut compenser une augmentation de la latence ou une réduction de la bande passante, et garantir ainsi que les utilisateurs finaux peuvent rester productifs quelles que soient les conditions du réseau.

PCoIP est pris en charge comme protocole d'affichage pour les postes de travail View avec des machines virtuelles et des machines physiques qui contiennent des cartes d'hôte Teradici.

## Fonctions de PCoIP

Les fonctions clés de PCoIP incluent :

- Les utilisateurs à l'extérieur du pare-feu d'entreprise peuvent utiliser ce protocole avec le réseau privé virtuel (VPN) de votre entreprise, ou bien ils peuvent établir une connexion cryptée et sécurisée avec un serveur de sécurité View dans la zone DMZ de l'entreprise.
- Le cryptage AES (Advanced Encryption Standard) 128 bits est pris en charge et est activé par défaut. Toutefois, vous pouvez modifier le chiffrement de clé de cryptage sur AES-192 ou AES-256.
- Les connexions à des postes de travail Windows avec des versions de système d'exploitation View Agent répertoriées dans la section « Systèmes d'exploitation pris en charge pour View Agent », page 15 sont prises en charge.
- Les connexions de tous les types de clients View.
- La redirection MMR est prise en charge pour certains systèmes d'exploitation client Windows et certains systèmes d'exploitation de poste de travail View (agent). Consultez la « Matrice de prise en charge des fonctions » dans le document *Planification de l'architecture de VMware Horizon View*.
- La redirection USB est prise en charge pour certains types de client.
- La redirection audio avec le réglage dynamique de la qualité audio pour les réseaux LAN et WAN est prise en charge.
- Les contrôles d'optimisation pour la réduction de l'utilisation de bande passante sur les réseaux LAN et WAN.
- Plusieurs écrans sont pris en charge pour certains types de client. Par exemple, sur des clients Windows, vous pouvez utiliser jusqu'à quatre écrans et régler la résolution de chaque écran séparément, avec une résolution de 2560 x 1600 maximum par écran. La rotation d'affichage et l'ajustement automatique sont également pris en charge.

  Lorsque la fonction 3D est activée, jusqu'à 2 écrans sont pris en charge avec une résolution de 1920 x 1200 maximum.
- Les couleurs 32 bits sont prises en charge pour les affichages virtuels.
- Les polices ClearType sont prises en charge.
- Les opérations copier et coller du texte et des images entre un système d'exploitation client Windows et un poste de travail View sont prises en charge, jusqu'à 1 Mo maximum. Les formats de fichier pris en charge incluent le texte, les images et RTF (Rich Text Format). Vous ne pouvez pas copier et coller des objets système comme des dossiers et des fichiers entre des systèmes.

Pour plus d'informations sur les périphériques client prenant en charge des fonctions PCoIP spécifiques, allez sur https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

## Paramètres de système d'exploitation client recommandés

Les paramètres de système d'exploitation client recommandés incluent :

- Pour les postes de travail Windows XP : 768 Mo ou plus de RAM et un seul CPU.
- Pour les postes de travail Windows 7 ou 8 : 1 Go ou plus de RAM et un CPU double sont recommandés pour lire des vidéos haute définition, en mode plein écran ou formatées à 720p ou plus.

### Exigences de qualité vidéo

**Vidéo formatée à 480p**

Vous pouvez lire une vidéo à 480p ou moins à des résolutions natives lorsque le poste de travail View a une seule CPU virtuelle. Si le système d'exploitation est Windows 7 ou supérieur et que vous voulez lire la vidéo en Flash haute définition ou en mode plein écran, le poste de travail requiert une CPU virtuelle double. Même avec un poste de travail de CPU virtuel double, les vidéos formatées à 360p lues en mode plein écran peuvent être décalées par rapport au son, en particulier sur les clients Windows.

**Vidéo formatée à 720p**

Vous pouvez lire une vidéo à 720p à des résolutions natives lorsque le poste de travail View a une CPU virtuelle double. Les performances peuvent être affectées si vous lisez des vidéos à 720p en haute définition ou en mode plein écran.

**Vidéo formatée à 1 080p**

Si le poste de travail View a une CPU virtuelle double, vous pouvez lire une vidéo formatée à 1 080p, bien que la taille d'écran du lecteur média puisse être diminuée.

**3D**

Si vous utilisez VMware vSphere 5.1 ou supérieur, vous pouvez configurer des postes de travail View afin qu'ils utilisent l'affichage graphique accéléré logiciellement ou matériellement.

- Avec vSGA (Virtual Shared Graphics Acceleration), une fonction de vSphere 5.1 qui utilise des cartes graphiques physiques installées sur les hôtes ESXi, vous pouvez utiliser des applications 3D pour la conception, la modélisation et le multimédia.
- Avec la fonction d'affichage graphique accéléré logiciellement, disponible avec vSphere 5.0 et supérieur, vous pouvez utiliser des applications 3D moins gourmandes, telles que les thèmes Windows Aero, Microsoft Office 2010 et Google Earth.

  Cette fonction d'affichage graphique accéléré non matériel vous permet d'exécuter des applications DirectX 9 et OpenGL 2.1 sans nécessiter de GPU physique.

Pour les applications 3D, 2 écrans maximum sont pris en charge, et la résolution d'écran maximale est 1920 x 1200. Le système d'exploitation client sur les postes de travail View doit être Windows 7 ou supérieur.

### Exigences matérielles des systèmes client

Pour plus d'informations sur les exigences de processeur et de mémoire, consultez le document « Utilisation de VMware Horizon View Client » pour le type spécifique de poste de travail ou de périphérique client mobile. Allez sur https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

## Microsoft RDP

Remote Desktop Protocol est le même protocole multicanal que de nombreuses personnes utilisent déjà pour accéder à leur ordinateur professionnel depuis leur ordinateur à domicile. La Connexion Bureau à distance Microsoft utilise RDP pour transmettre des données.

Microsoft RDP fournit les fonctions suivantes :

- Avec RDP 6, vous pouvez utiliser plusieurs écrans en mode étendu. RDP 7 offre une prise en charge de plusieurs écrans, pour 16 écrans maximum.

- Vous pouvez copier et coller du texte et des objets système, tels que des dossiers et des fichiers, entre le système local et le poste de travail View.
- Les couleurs 32 bits sont prises en charge pour les affichages virtuels.
- RDP prend en charge le cryptage 128 bits.
- Les utilisateurs à l'extérieur du pare-feu d'entreprise peuvent utiliser ce protocole avec le réseau privé virtuel (VPN) de votre entreprise, ou bien ils peuvent établir une connexion cryptée et sécurisée avec un serveur de sécurité View dans la zone DMZ de l'entreprise.

**Remarque** Pour les machines virtuelles de poste de travail Windows XP, vous devez installer les correctifs RDP répertoriés dans les articles 323497 et 884020 de la Base de connaissances de Microsoft. Si vous n'installez pas les correctifs RDP, le message `Échec des sockets Windows` risque de s'afficher sur le client.

## Exigences matérielles des systèmes client

Pour plus d'informations sur les exigences de processeur et de mémoire, consultez le document « Utilisation de VMware Horizon View Client » pour le type spécifique de système client. Allez sur https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

**Remarque** Les périphériques client iOS et Android utilisent uniquement le protocole d'affichage PCoIP.

# Préparation d'Active Directory 3

View utilise votre infrastructure Microsoft Active Directory existante pour l'authentification et la gestion des utilisateurs. Vous devez exécuter certaines tâches pour préparer Active Directory à l'utilisation avec View.

View prend en charge les versions suivantes d'Active Directory :

- Windows 2003 Active Directory
- Windows 2008 Active Directory

Ce chapitre aborde les rubriques suivantes :



## Configuration de domaines et de relations d'approbation

Vous devez associer chaque hôte de View Connection Server à un domaine Active Directory. L'hôte ne doit pas être un contrôleur de domaine. Vous placez des postes de travail View dans le même domaine que l'hôte de View Connection Server ou dans un domaine qui a une relation d'approbation bidirectionnelle avec le domaine de l'hôte de View Connection Server.

Vous pouvez autoriser des utilisateurs et des groupes dans le domaine de l'hôte de View Connection vers des postes de travail et des pools View. Vous pouvez également sélectionner des utilisateurs et des groupes du domaine de l'hôte de View Connection Server pour qu'ils soient des administrateurs dans View Administrator. Pour autoriser ou sélectionner des utilisateurs et des groupes dans un domaine différent, vous devez établir une relation d'approbation bidirectionnelle entre ce domaine et le domaine de l'hôte de View Connection Server.

Les utilisateurs sont authentifiés par Active Directory pour le domaine de l'hôte de View Connection Server et par des domaines d'utilisateurs supplémentaires avec lesquels un accord d'approbation existe.

**Remarque** Comme les serveurs de sécurité n'accèdent à aucun référentiel d'authentification, y compris Active Directory, ils n'ont pas besoin de résider dans un domaine Active Directory.

### Relations d'approbation et filtrage de domaine

Pour déterminer les domaines auxquels elle peut accéder, une instance de Serveur de connexion View traverse des relations d'approbation en commençant par son propre domaine.

Pour un petit ensemble de domaines bien connectés, Serveur de connexion View peut déterminer rapidement la liste complète de domaines, mais le temps que cela prend augmente car le nombre de domaines accroît ou car la connectivité entre les domaines diminue. La liste peut également inclure des domaines que vous ne souhaitez pas proposer aux utilisateurs lorsqu'ils ouvrent une session sur leurs postes de travail View.

Vous pouvez utiliser la commande `vdmadmin` pour configurer le filtrage de domaine pour limiter les domaines qu'une instance de Serveur de connexion View recherche et qu'elle affiche aux utilisateurs. Pour plus d'informations, consultez le document *Administration de VMware Horizon View*.

## Création d'une UO pour des postes de travail View

Vous devez créer une unité d'organisation (UO) spécifiquement pour vos postes de travail View. Une UO est une sous-division dans Active Directory contenant des utilisateurs, des groupes, des ordinateurs ou d'autres UO.

Pour empêcher l'application de paramètres de stratégie de groupe sur d'autres serveurs ou stations de travail Windows dans le même domaine que vos postes de travail, vous pouvez créer un GPO pour vos stratégies de groupe de View et le lier à l'UO qui contient vos postes de travail View. Vous pouvez également déléguer le contrôle de l'UO à des groupes subordonnés tels que des opérateurs de serveur ou des utilisateurs individuels.

Si vous utilisez View Composer, vous devez créer un conteneur Active Directory séparé pour des postes de travail de clone lié basé sur l'UO pour vos postes de travail View. Les administrateurs de View qui ont des privilèges d'administrateur d'UO dans Active Directory peuvent approvisionner des postes de travail de clone lié sans privilèges d'administrateur de domaine. Si vous modifiez les informations d'identification d'administrateur dans Active Directory, vous devez également mettre à jour les informations d'identification dans View Composer.

## Création d'UO et de groupes pour des comptes de client en mode kiosque

Un client en mode kiosque est un client léger ou un PC verrouillé qui exécute View Client pour se connecter à une instance de Serveur de connexion View et lancer une session de poste de travail à distance. Si vous configurez des clients en mode kiosque, vous devez créer des UO et des groupes dédiés dans Active Directory pour des comptes de client en mode kiosque.

La création d'UO et de groupes dédiés pour des comptes de client en mode kiosque protège les systèmes client contre les intrusions injustifiées et simplifie la configuration et l'administration du client.

Pour plus d'informations, consultez le document *Administration de VMware Horizon View*.

## Création de groupes pour les utilisateurs de View

Vous devez créer des groupes pour différents types d'utilisateurs de View dans Active Directory. Par exemple, vous pouvez créer un groupe nommé Utilisateurs de VMware Horizon View pour vos utilisateurs de postes de travail View et un autre groupe nommé Administrateurs de VMware Horizon View pour les utilisateurs qui administreront des postes de travail View.

## Création d'un compte d'utilisateur pour vCenter Server

Vous devez créer un compte d'utilisateur dans Active Directory à utiliser avec vCenter Server. Vous spécifiez ce compte d'utilisateur lorsque vous ajoutez une instance de vCenter Server dans View Administrator.

Le compte d'utilisateur doit se trouver dans le même domaine que votre hôte de View Connection Server ou dans un domaine approuvé. Si vous utilisez View Composer, vous devez ajouter le compte d'utilisateur dans le groupe d'administrateurs local sur l'ordinateur vCenter Server.

Vous devez accorder au compte d'utilisateur les privilèges pour effectuer certaines opérations dans vCenter Server. Si vous utilisez View Composer, vous devez accorder au compte d'utilisateur des privilèges supplémentaires. Reportez-vous à la section « Configuration de comptes d'utilisateur pour vCenter Server et View Composer », page 95 pour plus d'informations sur la configuration de ces privilèges.

## Créer un compte d'utilisateur pour View Composer

Si vous utilisez View Composer, vous devez créer un compte d'utilisateur dans Active Directory pour l'utiliser avec View Composer. View Composer a besoin de ce compte pour associer des postes de travail de clone lié à votre domaine Active Directory.

Pour garantir la sécurité, vous devez créer un compte d'utilisateur séparé à utiliser avec View Composer. En créant un compte séparé, vous pouvez garantir qu'il n'a pas de privilèges supplémentaires définis pour une autre raison. Vous pouvez donner au compte les privilèges minimum dont il a besoin pour créer et supprimer des objets ordinateur dans un conteneur Active Directory spécifié. Par exemple, le compte View Composer ne requiert pas de privilèges d'administrateur de domaine.

### Procédure

1 Dans Active Directory, créez un compte d'utilisateur dans le même domaine que votre hôte de Serveur de connexion View ou dans un domaine approuvé.

2 Ajoutez les autorisations **[Créer des objets ordinateur]** , **[Supprimer des objets ordinateur]** et **[Écrire toutes les propriétés]** au compte dans le conteneur Active Directory dans lequel les comptes d'ordinateur de clone lié sont créés ou vers lequel les comptes d'ordinateur de clone lié sont déplacés.

   La liste suivante montre toutes les autorisations requises pour le compte d'utilisateur, y compris les autorisations affectées par défaut :

   - Contenu de la liste
   - Lire toutes les propriétés
   - Écrire toutes les propriétés
   - Lire les autorisations
   - Réinitialiser le mot de passe
   - Créer des objets ordinateur

- Supprimer des objets ordinateur

**Remarque** Si vous sélectionnez le paramètre **[Autoriser la réutilisation de comptes d'ordinateur pré-existants]** pour un pool de postes de travail, vous avez seulement besoin d'ajouter les autorisations suivantes :

- Contenu de la liste
- Lire toutes les propriétés
- Lire les autorisations
- Réinitialiser le mot de passe

3 Assurez-vous que les autorisations du compte d'utilisateur s'appliquent au conteneur Active Directory et à tous les objets enfants du conteneur.

### Suivant

Spécifiez le compte dans View Administrator lorsque vous configurez View Composer pour vCenter Server et quand vous configurez et déployez des pools de postes de travail de clone lié.

## Configurer la stratégie Groupes restreints

Pour ouvrir une session sur un poste de travail View, les utilisateurs doivent appartenir au groupe Utilisateurs du Bureau à distance local du poste de travail View. Vous pouvez utiliser la stratégie Groupes restreints dans Active Directory pour ajouter des utilisateurs ou des groupes au groupe Utilisateurs du Bureau à distance local de chaque poste de travail View associé à votre domaine.

La stratégie Groupes restreints définit l'appartenance du groupe local d'ordinateurs dans le domaine pour correspondre aux paramètres de la liste d'appartenance définie dans la stratégie Groupes restreints. Les membres de votre groupe d'utilisateurs de poste de travail View sont toujours ajoutés au groupe Utilisateurs du Bureau à distance local de chaque poste de travail View associé à votre domaine. Lors de l'ajout de nouveaux utilisateurs, vous ne devez les ajouter qu'à votre groupe d'utilisateurs de poste de travail View.

### Prérequis

Créez un groupe pour les utilisateurs de poste de travail View dans votre domaine dans Active Directory.

### Procédure

1 Sur le serveur Active Directory, naviguez vers le plug-in de gestion de stratégie de groupe.

| Version d'AD | Chemin de navigation |
|---|---|
| **Windows 2003** | a Sélectionnez **[Démarrer] > [Tous les programmes] > [Outils d'administration] > [Utilisateurs et ordinateurs Active Directory]** .<br>b Cliquez avec le bouton droit sur votre domaine et cliquez sur **[Propriétés]** .<br>c Sur l'onglet **[Stratégie de groupe]** , cliquez sur **[Ouvrir]** pour ouvrir le plug-in de Gestion de stratégie de groupe.<br>d Cliquez avec le bouton droit sur **[Stratégie de domaine par défaut]** et cliquez sur **[Modifier]** . |
| **Windows 2008** | a Sélectionnez **[Démarrer] > [Outils d'administration] > [Gestion de stratégie de groupe]** .<br>b Développez votre domaine, cliquez avec le bouton droit sur **[Stratégie de domaine par défaut]** et cliquez sur **[Modifier]** . |

2 Développez la section **[Computer Configuration (Configuration ordinateur)]** et ouvrez **[Windows Settings (Paramètres Windows)\Security Settings (Paramètres de sécurité)]** .

3 Cliquez avec le bouton droit sur **[Restricted Groups (Groupes restreints)]** , sélectionnez **[Add Group (Ajouter un groupe)]** , puis ajoutez le groupe Utilisateurs du Bureau à distance.

4 Cliquez avec le bouton droit sur le nouveau groupe Utilisateurs du Bureau à distance restreint et ajoutez votre groupe d'utilisateurs de poste de travail View à la liste d'appartenance au groupe.

5 Cliquez sur **[OK]** pour enregistrer vos modifications.

# Utilisation de fichiers de modèle d'administration de stratégie de groupe de View

View comporte plusieurs fichiers de modèle d'administration de stratégie de groupe spécifiques à un composant.

Lors de l'installation de Serveur de connexion View, les fichiers de modèle d'administration de View sont installés dans le répertoire *install_directory*`\VMware\VMware View\Server\Extras\GroupPolicyFiles` sur votre hôte de Serveur de connexion View. Vous devez copier ces fichiers vers un répertoire de votre serveur Active Directory.

Vous pouvez optimiser et sécuriser des postes de travail View en ajoutant les paramètres de stratégie dans ces fichiers à un nouveau GPO ou un GPO existant dans Active Directory puis en liant ce GPO à l'UO qui contient vos postes de travail View.

Pour plus d'informations sur les paramètres de stratégie de groupe de View, consultez le document *Administration de VMware Horizon View*.

# Préparer Active Directory pour l'authentification par carte à puce

Vous devrez peut-être effectuer certaines tâches dans Active Directory lors de l'implémentation de l'authentification par carte à puce.

- Ajouter des UPN pour des utilisateurs de carte à puce page 26

  Comme les ouvertures de session par carte à puce reposent sur des noms d'utilisateur principaux (UPN), les comptes d'utilisateurs Active Directory qui utilisent des cartes à puce pour s'authentifier dans View doivent avoir un UPN valide.

- Ajouter le certificat racine à des autorités de certification racine de confiance page 27

  Si vous utilisez une autorité de certification pour émettre des certificats d'ouverture de session par carte à puce ou de contrôleur de domaine, vous devez ajouter le certificat racine à la stratégie de groupe Trusted Root Certification Authorities (Autorités de certification racine de confiance) dans Active Directory. Vous n'avez pas à effectuer cette procédure si le contrôleur de domaine Windows agit en tant qu'autorité de certification racine.

- Ajouter un certificat intermédiaire à des autorités de certification intermédiaires page 28

  Si vous utilisez une autorité de certification intermédiaire pour émettre des certificats d'ouverture de session par carte à puce ou de contrôleur de domaine, vous devez ajouter le certificat intermédiaire à la stratégie de groupe Intermediate Certification Authorities (Autorités de certification intermédiaires) dans Active Directory.

- Ajouter le certificat racine au magasin Enterprise NTAuth page 28

  Si vous utilisez une autorité de certification pour émettre des certificats d'ouverture de session par carte à puce ou de contrôleur de domaine, vous devez ajouter le certificat racine au magasin Enterprise NTAuth dans Active Directory. Vous n'avez pas à effectuer cette procédure si le contrôleur de domaine Windows agit en tant qu'autorité de certification racine.

## Ajouter des UPN pour des utilisateurs de carte à puce

Comme les ouvertures de session par carte à puce reposent sur des noms d'utilisateur principaux (UPN), les comptes d'utilisateurs Active Directory qui utilisent des cartes à puce pour s'authentifier dans View doivent avoir un UPN valide.

Si le domaine sur lequel réside un utilisateur de carte à puce est différent du domaine à partir duquel est émis votre certificat racine, vous devez définir l'UPN de l'utilisateur sur l'autre nom de l'objet (SAN) contenu dans le certificat racine de l'autorité de certification approuvée. Si votre certificat racine est émis à partir d'un serveur dans le domaine actuel de l'utilisateur de carte à puce, vous n'avez pas à modifier l'UPN de l'utilisateur.

---

**Remarque** Vous devrez peut-être définir l'UPN pour les comptes Active Directory intégrés, même si le certificat est émis à partir du même domaine. Aucun UPN n'est défini par défaut pour les comptes intégrés, y compris Administrateur.

---

### Prérequis

- Obtenez le SAN contenu dans le certificat racine de l'autorité de certification approuvée en affichant les propriétés du certificat.
- Si l'utilitaire Éditeur ADSI n'est pas présent sur votre serveur Active Directory, téléchargez et installez les outils de support Windows appropriés sur le site Web Microsoft.

### Procédure

1. Sur votre serveur Active Directory, démarrez l'utilitaire Éditeur ADSI.
2. Dans le volet de gauche, développez le domaine dans lequel se trouve l'utilisateur et double-cliquez sur `CN=Users`.
3. Dans le volet de droite, cliquez avec le bouton droit sur l'utilisateur et cliquez sur **[Properties (Propriétés)]** .
4. Double-cliquez sur l'attribut `userPrincipalName` et saisissez la valeur SAN du certificat de l'autorité de certification approuvée.
5. Cliquez sur **[OK]** pour enregistrer le paramètre d'attribut.

## Ajouter le certificat racine à des autorités de certification racine de confiance

Si vous utilisez une autorité de certification pour émettre des certificats d'ouverture de session par carte à puce ou de contrôleur de domaine, vous devez ajouter le certificat racine à la stratégie de groupe Trusted Root Certification Authorities (Autorités de certification racine de confiance) dans Active Directory. Vous n'avez pas à effectuer cette procédure si le contrôleur de domaine Windows agit en tant qu'autorité de certification racine.

### Procédure

1 Sur le serveur Active Directory, naviguez vers le plug-in de gestion de stratégie de groupe.

| Version d'AD | Chemin de navigation |
|---|---|
| **Windows 2003** | a Sélectionnez **[Démarrer] > [Tous les programmes] > [Outils d'administration] > [Utilisateurs et ordinateurs Active Directory]** .<br>b Cliquez avec le bouton droit sur votre domaine et cliquez sur **[Propriétés]** .<br>c Sur l'onglet **[Stratégie de groupe]** , cliquez sur **[Ouvrir]** pour ouvrir le plug-in de Gestion de stratégie de groupe.<br>d Cliquez avec le bouton droit sur **[Stratégie de domaine par défaut]** et cliquez sur **[Modifier]** . |
| **Windows 2008** | a Sélectionnez **[Démarrer] > [Outils d'administration] > [Gestion de stratégie de groupe]** .<br>b Développez votre domaine, cliquez avec le bouton droit sur **[Stratégie de domaine par défaut]** et cliquez sur **[Modifier]** . |

2 Développez la section **[Computer Configuration (Configuration ordinateur)]** et ouvrez le dossier **[Windows Settings (Paramètres Windows)\Security Settings (Paramètres de sécurité)\Public Key (Clé publique)]** .

3 Cliquez avec le bouton droit sur **[Trusted Root Certification Authorities (Autorités de certification racine de confiance)]** et sélectionnez **[Import (Importer)]** .

4 Suivez les invites de l'assistant pour importer le certificat racine (par exemple, `rootCA.cer`) et cliquez sur **[OK]** .

5 Fermez la fenêtre Group Policy (Stratégie de groupe).

Tous les systèmes du domaine contiennent maintenant une copie du certificat racine dans leur magasin racine approuvé.

### Suivant

Si une autorité de certification intermédiaire émet vos certificats d'ouverture de session par carte à puce ou de contrôleur de domaine, ajoutez le certificat intermédiaire à la stratégie de groupe Intermediate Certification Authorities (Autorités de certification intermédiaires) dans Active Directory. Reportez-vous à la section « Ajouter un certificat intermédiaire à des autorités de certification intermédiaires », page 28.

## Ajouter un certificat intermédiaire à des autorités de certification intermédiaires

Si vous utilisez une autorité de certification intermédiaire pour émettre des certificats d'ouverture de session par carte à puce ou de contrôleur de domaine, vous devez ajouter le certificat intermédiaire à la stratégie de groupe Intermediate Certification Authorities (Autorités de certification intermédiaires) dans Active Directory.

### Procédure

1 Sur le serveur Active Directory, naviguez vers le plug-in de gestion de stratégie de groupe.

| Version d'AD | Chemin de navigation |
|---|---|
| **Windows 2003** | a Sélectionnez **[Démarrer] > [Tous les programmes] > [Outils d'administration] > [Utilisateurs et ordinateurs Active Directory]** .<br>b Cliquez avec le bouton droit sur votre domaine et cliquez sur **[Propriétés]** .<br>c Sur l'onglet **[Stratégie de groupe]** , cliquez sur **[Ouvrir]** pour ouvrir le plug-in de Gestion de stratégie de groupe.<br>d Cliquez avec le bouton droit sur **[Stratégie de domaine par défaut]** et cliquez sur **[Modifier]** . |
| **Windows 2008** | a Sélectionnez **[Démarrer] > [Outils d'administration] > [Gestion de stratégie de groupe]** .<br>b Développez votre domaine, cliquez avec le bouton droit sur **[Stratégie de domaine par défaut]** et cliquez sur **[Modifier]** . |

2 Développez la section **[Computer Configuration (Configuration ordinateur)]** et ouvrez la stratégie de **[Windows Settings\Security Settings\Public Key (Paramètres Windows\Paramètres de sécurité\Clé publique)]** .

3 Cliquez avec le bouton droit sur **[Intermediate Certification Authorities (Autorités de certification intermédiaires)]** et sélectionnez **[Import (Importer)]** .

4 Suivez les invites de l'assistant pour importer le certificat intermédiaire (par exemple, `intermediateCA.cer`) et cliquez sur **[OK]** .

5 Fermez la fenêtre Groupe Policy (Stratégie de groupe).

Tous les systèmes du domaine contiennent maintenant une copie du certificat intermédiaire dans leur magasin d'autorité de certification intermédiaire approuvé.

## Ajouter le certificat racine au magasin Enterprise NTAuth

Si vous utilisez une autorité de certification pour émettre des certificats d'ouverture de session par carte à puce ou de contrôleur de domaine, vous devez ajouter le certificat racine au magasin Enterprise NTAuth dans Active Directory. Vous n'avez pas à effectuer cette procédure si le contrôleur de domaine Windows agit en tant qu'autorité de certification racine.

### Procédure

- Sur votre serveur Active Directory, utilisez la commande `certutil` pour publier le certificat dans le magasin Enterprise NTAuth.

  Par exemple : **`certutil –dspublish –f`** ***`path_to_root_CA_cert`*** **`NTAuthCA`**

L'autorité de certification est désormais approuvée pour émettre des certificats de ce type.

# Installation de View Composer 4

Pour utiliser View Composer, vous créez une base de données View Composer, installez le service View Composer et optimisez votre infrastructure View pour prendre en charge View Composer. Vous pouvez installer le service View Composer sur le même hôte que vCenter Server ou sur un hôte distinct.

View Composer est une fonction facultative. Installez View Composer si vous prévoyez de déployer des pools de postes de travail de clone lié.

Vous devez posséder une licence pour installer et utiliser la fonction View Composer.

Ce chapitre aborde les rubriques suivantes :



## Préparer une base de données View Composer

Vous devez créer une base de données et un nom de source de données (DSN) pour stocker des données View Composer.

Le service View Composer n'inclut pas de base de données. Si aucune instance de base de données n'existe dans l'environnement réseau, vous devez en installer une. Après avoir installé une instance de base de données, vous ajoutez la base de données View Composer à l'instance.

Vous pouvez ajouter la base de données View Composer à l'instance sur laquelle se trouve la base de données vCenter Server. Vous pouvez configurer la base de données localement ou à distance sur un ordinateur Linux, UNIX ou Windows Server connecté au réseau.

La base de données View Composer stocke des informations sur les connexions et les composants utilisés par View Composer :

- les connexions vCenter Server ;
- les connexions Active Directory ;
- les postes de travail de clone lié déployés par View Composer ;
- les réplicas créés par View Composer.

Chaque instance du service View Composer doit posséder sa propre base de données View Composer. Plusieurs services View Composer ne peuvent pas partager une base de données View Composer.

Pour voir une liste des versions de base de données prises en charge, reportez-vous à la section « Exigences de base de données pour View Composer », page 11.

Pour ajouter une base de données View Composer à une instance de base de données installée, choisissez l'une de ces procédures.

- Créer une base de données SQL Server pour View Composer page 30

  View Composer peut stocker des informations de poste de travail de clone lié dans une base de données SQL Server. Vous créez une base de données View Composer en l'ajoutant à SQL Server et en configurant une source de données ODBC pour elle.

- Créer une base de données Oracle pour View Composer page 32

  View Composer peut stocker des informations de poste de travail de clone lié dans une base de données Oracle 11g ou 10g. Vous créez une base de données View Composer en l'ajoutant à une instance d'Oracle existante et en configurant une source de données ODBC pour elle. Vous pouvez ajouter une nouvelle base de données View Composer en utilisant l'assistant de configuration de base de données Oracle ou en exécutant une instruction SQL.

## Créer une base de données SQL Server pour View Composer

View Composer peut stocker des informations de poste de travail de clone lié dans une base de données SQL Server. Vous créez une base de données View Composer en l'ajoutant à SQL Server et en configurant une source de données ODBC pour elle.

### Ajouter une base de données View Composer à SQL Server

Vous pouvez ajouter une nouvelle base de données View Composer à une instance de Microsoft SQL Server existante pour stocker des données de clone lié pour View Composer.

Si la base de données réside localement, vous pouvez utiliser le modèle de sécurité Authentification Windows intégrée sur le système sur lequel vous allez installer View Composer. Si la base de données réside sur un système distant, vous ne pouvez pas utiliser cette méthode d'authentification.

#### Prérequis

- Vérifiez qu'une version prise en charge de SQL Server est installée sur l'ordinateur où vous allez installer View Composer ou dans votre environnement de réseau. Pour plus d'informations, reportez-vous à la section « Exigences de base de données pour View Composer », page 11.
- Vérifiez que vous utilisez SQL Server Management Studio ou SQL Server Management Studio Express pour créer et administrer la source de données. Vous pouvez télécharger et installer SQL Server Management Studio Express depuis le site Web suivant.

  http://www.microsoft.com/downloadS/details.aspx?familyid=C243A5AE-4BD1-4E3D-94B8-5A0F62BF7796

#### Procédure

1. Sur l'ordinateur View Composer, sélectionnez **[Start (Démarrer)] > [All Programs (Tous les programmes)] > [Microsoft SQL Server 2008]** ou **[Microsoft SQL Server 2005]** .
2. Sélectionnez **[SQL Server Management Studio Express]** et connectez-vous à l'instance de SQL Server existante pour vSphere Management.
3. Dans le volet Object Explorer (Explorateur d'objets), cliquez avec le bouton droit sur l'entrée Databases (Bases de données) et sélectionnez **[New Database (Nouvelle base de données)]** .
4. Dans la boîte de dialogue New Database (Nouvelle base de données), saisissez un nom dans la zone de texte Database name (Nom de base de données).

   Par exemple : **`viewComposer`**

5 Cliquez sur **[OK]** .

SQL Server Management Studio Express ajoute votre base de données à l'entrée Databases (Bases de données) dans le volet Object Explorer (Explorateur d'objets).

6 Quittez Microsoft SQL Server Management Studio Express.

### Suivant

Suivez les instructions de la section « Ajouter une source de données ODBC à SQL Server », page 31.

## Ajouter une source de données ODBC à SQL Server

Lorsque vous avez ajouté une base de données View Composer à SQL Server, vous devez configurer une connexion ODBC à la nouvelle base de données pour que cette source de données soit visible pour le service View Composer.

Lorsque vous configurez un nom de source de données (DSN) ODBC pour View Composer, définissez pour la connexion de base de données sous-jacente un niveau de sécurité adapté à votre environnement. Pour plus d'informations sur la sécurisation des connexions de base de données, voir la documentation SQL Server.

Si la connexion de base de données sous-jacente utilise le chiffrement SSL, il est recommandé de configurer les serveurs de base de données avec des certificats SSL signés par une autorité de certification (CA) de confiance. Si vous utilisez des certificats autosignés, les connexions de base de données peuvent être l'objet d'attaques d'intercepteur. .

### Prérequis

Effectuez les étapes décrites dans la section « Ajouter une base de données View Composer à SQL Server », page 30.

### Procédure

1 Sur l'ordinateur sur lequel View Composer doit être installé, sélectionnez **[Start (Démarrer)] > [Administrative Tools (Outils d'administration)] > [Data Source (ODBC) (Source de données (ODBC))]** .

2 Sélectionnez l'onglet **[System DSN (Nom DSN système)]** .

3 Cliquez sur **[Add (Ajouter)]** et sélectionnez **[SQL Native Client]** dans la liste.

4 Cliquez sur **[Finish (Terminer)]** .

5 Dans l'assistant d'installation Create a New Data Source to SQL Server (Créer une nouvelle source de données vers SQL Server), saisissez un nom et la description de la base de données View Composer.

Par exemple : **`ViewComposer`**

6 Dans la zone de texte Server (Serveur), saisissez le nom de la base de données SQL Server.

Utilisez la forme *host_name**server_name*, où *host_name* est le nom de l'ordinateur et *server_name* correspond à l'instance de SQL Server.

Par exemple : **`VCHOST1\VIM_SQLEXP`**

7 Cliquez sur **[Next (Suivant)]** .

8 Assurez-vous que la case **[Connect to SQL Server to obtain default settings for the additional configuration options (Se connecter à SQL Server pour obtenir les paramètres par défaut pour les options de configuration supplémentaires)]** est cochée et sélectionnez une option d'authentification.

| Option | Description |
|---|---|
| **Windows NT authentication (Authentification Windows NT)** | Sélectionnez cette option si vous utilisez une instance locale de SQL Server. Cette option est aussi connue sous le nom d'authentification approuvée. L'authentification Windows NT est prise en charge uniquement si SQL Server est exécuté sur l'ordinateur local. |
| **SQL Server authentication (Authentification SQL Server)** | Sélectionnez cette option si vous utilisez une instance distante de SQL Server. L'authentification Windows NT n'est pas prise en charge sur les SQL Server distants. |

9 Cliquez sur **[Next (Suivant)]** .

10 Cochez la case **[Change the default database to (Changer la base de données par défaut par :)]** et sélectionnez le nom de la base de données View Composer dans la liste.

Par exemple : `ViewComposer`

11 Si la connexion SQL Server est configurée avec SSL, accédez à la page de configuration du nom de source de données (DSN) Microsoft SQL Server et sélectionnez **[Use strong encryption for data (Utiliser le cryptage renforcé pour les données)]** .

12 Effectuez et fermez l'assistant Microsoft ODBC Data Source Administrator (Administrateur de sources de données ODBC de Microsoft).

### Suivant

Installez le nouveau service View Composer. Reportez-vous à la section « Installer le service View Composer », page 36.

## Créer une base de données Oracle pour View Composer

View Composer peut stocker des informations de poste de travail de clone lié dans une base de données Oracle 11g ou 10g. Vous créez une base de données View Composer en l'ajoutant à une instance d'Oracle existante et en configurant une source de données ODBC pour elle. Vous pouvez ajouter une nouvelle base de données View Composer en utilisant l'assistant de configuration de base de données Oracle ou en exécutant une instruction SQL.

- Ajouter une base de données View Composer à Oracle 11g ou 10g page 33

  Vous pouvez utiliser l'assistant de configuration de base de données Oracle pour ajouter une nouvelle base de données View Composer sur une instance d'Oracle 11g ou 10g existante.

- Utiliser une instruction SQL pour ajouter une base de données View Composer à une instance d'Oracle page 34

  La base de données View Composer doit posséder certains espaces et privilèges de table. Vous pouvez utiliser une instruction SQL pour créer la base de données View Composer dans une instance de base de données Oracle 11g ou 10g.

- Configurer un utilisateur de base de données Oracle pour View Composer page 34

  Par défaut, l'utilisateur de base de données qui exécute la base de données View Composer dispose d'autorisations d'administrateur système Oracle. Pour limiter les autorisations de sécurité pour l'utilisateur exécutant la base de données View Composer, vous devez configurer un utilisateur de base de données Oracle avec des autorisations spécifiques.

- Ajouter une source de données ODBC à Oracle 11g ou 10g page 35

  Lorsque vous avez ajouté une base de données View Composer à une instance d'Oracle 11g ou 10g, vous devez configurer une connexion ODBC à la nouvelle base de données pour rendre cette source de données visible pour le service View Composer.

## Ajouter une base de données View Composer à Oracle 11g ou 10g

Vous pouvez utiliser l'assistant de configuration de base de données Oracle pour ajouter une nouvelle base de données View Composer sur une instance d'Oracle 11g ou 10g existante.

### Prérequis

Vérifiez qu'une version prise en charge d'Oracle 11g ou 10g est installée sur l'ordinateur local ou distant. Reportez-vous à la section « Exigences de base de données pour View Composer », page 11.

### Procédure

1 Démarrez **[Database Configuration Assistant (Assistant de configuration de base de données)]** sur l'ordinateur où vous ajoutez la base de données View Composer.

| Version de base de données | Action |
|---|---|
| **Oracle 11g** | Sélectionnez **[Start (Démarrer)] > [All Programs (Tous les programmes)] > [Oracle-OraDb11g_home] > [Configuration and Migration Tools (Outils de configuration et de migration)] > [Database Configuration Assistant (Assistant de configuration de base de données)]** . |
| **Oracle 10g** | Sélectionnez **[Start (Démarrer)] > [All Programs (Tous les programmes)] > [Oracle-OraDb10g_home] > [Configuration and Migration Tools (Outils de configuration et de migration)] > [Database Configuration Assistant (Assistant de configuration de base de données)]** . |

2 Sur la page Operations (Opérations), sélectionnez **[Create a database (Créer une base de données)]** .

3 Sur la page Database Templates (Modèles de base de données), sélectionnez le modèle **[General Purpose or Transaction Processing (Général ou traitement transactionnel)]** .

4 Sur la page Database Identification (Identification de la base de données), saisissez un nom global de base de données et un préfixe d'Identificateur système (SID) Oracle.

  Pour des raisons de facilité, utilisez la même valeur pour les deux éléments.

5 Sur la page Management Options (Options de gestion), cliquez sur **[Next (Suivant)]** pour accepter les réglages par défaut.

6 Sur la page Database Credentials (Informations d'identification de la base de données), sélectionnez **[Use the Same Administrative Passwords for All Accounts (Utiliser les mêmes mots de passe administratifs pour tous les comptes)]** et saisissez un mot de passe.

7 Sur les pages de configuration restantes, cliquez sur **[Next (Suivant)]** pour accepter les réglages par défaut.

8 Sur la page Creation Options (Options de création), vérifiez que **[Create Database (Créer une base de données)]** est sélectionné et cliquez sur **[Finish (Terminer)]** .

9 Sur la page Confirmation, examinez les options et cliquez sur **[OK]** .

  L'outil de configuration crée la base de données.

10 Sur la page Database Creation Complete (Création de la base de données terminée), cliquez sur **[OK]** .

### Suivant

Suivez les instructions de la section « Ajouter une source de données ODBC à Oracle 11g ou 10g », page 35.

## Utiliser une instruction SQL pour ajouter une base de données View Composer à une instance d'Oracle

La base de données View Composer doit posséder certains espaces et privilèges de table. Vous pouvez utiliser une instruction SQL pour créer la base de données View Composer dans une instance de base de données Oracle 11g ou 10g.

Lorsque vous créez la base de données, vous pouvez personnaliser l'emplacement des données et des fichiers journaux.

### Prérequis

Vérifiez qu'une version prise en charge d'Oracle 11g ou 10g est installée sur l'ordinateur local ou distant. Pour plus d'informations, reportez-vous à la section « Exigences de base de données pour View Composer », page 11.

### Procédure

1 Ouvrez une session SQL*Plus avec le compte système.

2 Exécutez l'instruction SQL suivante pour créer la base de données.

```
CREATE SMALLFILE TABLESPACE "VCMP" DATAFILE '/u01/app/oracle/oradata/vcdb/vcmp01.dbf'
SIZE 512M AUTOEXTEND ON NEXT 10M MAXSIZE UNLIMITED LOGGING EXTENT MANAGEMENT LOCAL SEGMENT
SPACE MANAGEMENT AUTO;
```

Dans cet exemple, `VCMP` est le nom d'exemple de la base de données View Composer et `vcmp01.dbf` est le nom du fichier de base de données.

Pour une installation Windows, utilisez les conventions Windows dans le chemin du répertoire vers le fichier `vcmp01.dbf`.

### Suivant

Si vous voulez exécuter la base de données View Composer avec des autorisations de sécurité spécifiques, suivez les instructions de la section « Configurer un utilisateur de base de données Oracle pour View Composer », page 34.

Suivez les instructions de la section « Ajouter une source de données ODBC à Oracle 11g ou 10g », page 35

## Configurer un utilisateur de base de données Oracle pour View Composer

Par défaut, l'utilisateur de base de données qui exécute la base de données View Composer dispose d'autorisations d'administrateur système Oracle. Pour limiter les autorisations de sécurité pour l'utilisateur exécutant la base de données View Composer, vous devez configurer un utilisateur de base de données Oracle avec des autorisations spécifiques.

### Prérequis

Vérifiez qu'une base de données View Composer a été créée dans une instance d'Oracle 11g ou 10g.

### Procédure

1 Ouvrez une session SQL*Plus avec le compte système.

2 Exécutez la commande SQL suivante pour créer un utilisateur de base de données View Composer avec les autorisations correctes.

```
CREATE USER "VCMPADMIN" PROFILE "DEFAULT" IDENTIFIED BY "oracle" DEFAULT TABLESPACE

"VCMP" ACCOUNT UNLOCK;
   grant connect to VCMPADMIN;
```

```
grant resource to VCMPADMIN;
grant create view to VCMPADMIN;
grant create sequence to VCMPADMIN;
grant create table to VCMPADMIN;
grant create materialized view to VCMPADMIN;
grant execute on dbms_lock to VCMPADMIN;
grant execute on dbms_job to VCMPADMIN;
grant unlimited tablespace to VCMPADMIN;
```

Dans cet exemple, le nom d'utilisateur est `VCMPADMIN` et le nom de la base de données View Composer est `VCMP`.

Par défaut, les privilèges `create procedure`, `create table` et `create sequence` sont affectés au rôle `resource`. Si le rôle `resource` ne possède pas ces privilèges, accordez-les explicitement à l'utilisateur de base de données View Composer.

## Ajouter une source de données ODBC à Oracle 11g ou 10g

Lorsque vous avez ajouté une base de données View Composer à une instance d'Oracle 11g ou 10g, vous devez configurer une connexion ODBC à la nouvelle base de données pour rendre cette source de données visible pour le service View Composer.

Lorsque vous configurez un nom de source de données (DSN) ODBC pour View Composer, définissez pour la connexion de base de données sous-jacente un niveau de sécurité adapté à votre environnement. Pour plus d'informations sur la sécurisation des connexions de base de données, voir la documentation de la base de données Oracle.

Si la connexion de base de données sous-jacente utilise le chiffrement SSL, il est recommandé de configurer les serveurs de base de données avec des certificats SSL signés par une autorité de certification (CA) de confiance. Si vous utilisez des certificats autosignés, les connexions de base de données peuvent être l'objet d'attaques d'intercepteur. .

### Prérequis

Vérifiez que vous avez effectué les étapes décrites dans la section « Ajouter une base de données View Composer à Oracle 11g ou 10g », page 33 ou « Utiliser une instruction SQL pour ajouter une base de données View Composer à une instance d'Oracle », page 34.

### Procédure

1 Sur l'ordinateur de la base de données View Composer, sélectionnez **[Start (Démarrer)] > [Administrative Tools (Outils d'administration)] > [Data Source (ODBC) (Source de données (ODBC))]** .

2 Dans l'assistant Microsoft ODBC Data Source Administrator (Administrateur de sources de données ODBC de Microsoft), sélectionnez l'onglet **[System DSN (Nom DNS système)]** .

3 Cliquez sur **[Add (Ajouter)]** et sélectionnez le pilote Oracle approprié dans la liste.

Par exemple : **`OraDb11g_home`**

4 Cliquez sur **[Finish (Terminer)]** .

5 Dans la boîte de dialogue Oracle ODBC Driver Configuration (Configuration du pilote Oracle ODBC), saisissez un DSN à utiliser avec View Composer, une description de la source de données et un ID d'utilisateur pour vous connecter à la base de données.

Si vous avez configuré un ID d'utilisateur de base de données Oracle avec des autorisations de sécurité spécifiques, spécifiez cet ID d'utilisateur.

**REMARQUE** Vous utilisez le nom DNS lorsque vous installez le service View Composer.

6 Spécifiez un **[TNS Service Name (Nom du service TNS)]** en sélectionnant le nom global de base de données dans le menu déroulant.

L'assistant de configuration de base de données Oracle spécifie le nom global de base de données.

7 Pour vérifier la source de données, cliquez sur **[Test Connection (Tester la connexion)]** et sur **[OK]** .

### Suivant

Installez le nouveau service View Composer. Reportez-vous à la section « Installer le service View Composer », page 36.

## Configuration d'un certificat SSL pour View Composer

Par défaut, un certificat auto-signé est installé avec View Composer. Vous pouvez utiliser le certificat par défaut à des fins de test. Mais, à des fins de production, vous devez le remplacer par un certificat signé par une autorité de certification.

Vous pouvez configurer un certificat avant ou après avoir installé View Composer. Dans View 5.1 et versions supérieures, vous configurez un certificat en l'important dans le magasin de certificats de l'ordinateur local Windows sur l'ordinateur Windows Server sur lequel View Composer est, ou sera, installé.

- Si vous importez un certificat signé par une autorité de certification avant d'installer View Composer, vous pouvez sélectionner le certificat signé lors de l'installation de View Composer. Cette approche évite d'avoir à remplacer manuellement le certificat par défaut après l'installation.
- Si vous prévoyez de remplacer un certificat existant ou le certificat auto-signé par défaut par un nouveau certificat après avoir installé View Composer, vous devez importer le nouveau certificat et exécuter l'utilitaire `SviConfig ReplaceCertificate` pour lier votre nouveau certificat sur le port utilisé par View Composer.

Pour plus d'informations sur la configuration des certificats SSL et l'utilisation de l'utilitaire `SviConfig ReplaceCertificate`, reportez-vous à la section Chapitre 7, « Configuration de certificats SSL pour des View Servers », page 75.

Si vous installez vCenter Server et View Composer sur le même ordinateur Windows Server, ils peuvent utiliser le même certificat SSL, mais vous devez configurer le certificat séparément pour chaque composant.

## Installer le service View Composer

Pour utiliser View Composer, vous devez installer le service View Composer. View Manager utilise View Composer pour créer et déployer des postes de travail de clone lié dans vCenter Server.

Vous installez le service View Composer sur l'ordinateur Windows Server sur lequel vCenter Server est installé ou sur un ordinateur Windows Server séparé. Une installation de View Composer autonome fonctionne avec vCenter Server installé sur un ordinateur Windows Server et avec vCenter Server Appliance basé sur Linux.

Le logiciel View Composer ne peut pas coexister sur la même machine virtuelle ou physique avec d'autres composants logiciels de View Manager, y compris un serveur réplica, un serveur de sécurité, Serveur de connexion View, View Agent, View Client ou Serveur de transfert View.

### Prérequis

- Vérifiez que votre installation satisfait les exigences de View Composer décrites dans la section « Exigences de View Composer », page 10.
- Vérifiez que vous possédez une licence pour installer et utiliser View Composer.
- Vérifiez que vous possédez le DSN, le nom d'utilisateur d'administrateur de domaine et le mot de passe que vous avez fournis dans l'assistant Administrateur de sources de données ODBC. Vous saisissez ces informations lorsque vous installez le service View Composer.

- Si vous prévoyez de configurer un certificat SSL signé par une autorité de certification pour View Composer lors de l'installation, vérifiez que votre certificat est importé dans le magasin de certificats de l'ordinateur local Windows. Reportez-vous à la section Chapitre 7, « Configuration de certificats SSL pour des View Servers », page 75.
- Vérifiez qu'aucune application exécutée sur l'ordinateur View Composer n'utilise de bibliothèques Windows SSL qui requièrent la version 2 de SSL (SSLv2) fournie via le package de sécurité Microsoft Secure Channel (Schannel). Le programme d'installation de View Composer désactive SSLv2 sur Microsoft Schannel. Des applications telles que Tomcat, qui utilise Java SSL, ou Apache, qui utilise OpenSSL, ne sont pas affectées par cette contrainte.
- Pour exécuter le programme d'installation de View Composer, vous devez être un utilisateur de domaine avec des privilèges d'administrateur sur le système.

### Procédure

1 Téléchargez le fichier du programme d'installation View Composer sur la page de produits VMware à l'adresse http://www.vmware.com/fr/products/ sur l'ordinateur Windows Server.

Le nom de fichier du programme d'installation est `VMware-viewcomposer-y.y.y-xxxxxx.exe`, où *xxxxxx* est le numéro de build et *y.y.y* est le numéro de version. Le fichier du programme d'installation installe le service View Composer sur des systèmes d'exploitation Windows Server 64 bits.

2 Pour démarrer le programme d'installation de View Composer, cliquez avec le bouton droit sur le fichier du programme d'installation et sélectionnez **[Exécuter en tant qu'administrateur]** .

3 Acceptez les termes de licence VMware.

4 Acceptez ou modifiez le dossier de destination.

5 Saisissez le DSN pour la base de données View Composer que vous avez fourni dans l'assistant Administrateur de sources de données ODBC Microsoft ou Oracle.

Par exemple : **`VMware View Composer`**

**Remarque** Si vous n'avez pas configuré un DSN pour la base de données View Composer, cliquez sur **[Configurer un DSN ODBC]** pour configurer un nom maintenant.

6 Saisissez le nom d'utilisateur et le mot de passe d'administrateur de domaine que vous avez fournis dans l'assistant Administrateur de sources de données ODBC.

Si vous avez configuré un utilisateur de base de données Oracle avec des autorisations de sécurité spécifiques, spécifiez ce nom d'utilisateur.

7 Saisissez un numéro de port ou acceptez la valeur par défaut.

Serveur de connexion View utilise ce port pour communiquer avec le service View Composer.

8 Fournissez un certificat SSL.

| Option | Action |
|---|---|
| **Créer un certificat SSL par défaut** | Sélectionnez ce bouton radio pour créer un certificat SSL par défaut pour le service View Composer.<br>Après l'installation, vous pouvez remplacer le certificat par défaut par un certificat SSL signé par une autorité de certification. |
| **Utiliser un certificat SSL existant** | Sélectionnez ce bouton radio si vous avez installé un certificat SSL signé que vous voulez utiliser pour le service View Composer. Sélectionnez un certificat SSL dans la liste. |

9 Cliquez sur **[Installer]** et **[Terminer]** pour terminer l'installation du service View Composer.

Le service VMware View Composer démarre.

View Composer utilise les suites de chiffrement qui sont fournies par le système d'exploitation Windows Server. Vous devez suivre les recommandations de votre entreprise concernant la gestion des suites de chiffrement sur les systèmes Windows Server. Si votre entreprise ne fournit aucune recommandation, VMware vous conseille de désactiver les suites de chiffrement faible sur le serveur View Composer afin d'améliorer la sécurité de votre environnement View. Pour plus d'informations sur la gestion des suites de chiffrement, consultez votre documentation Microsoft.

# Configuration de votre infrastructure pour View Composer

Vous pouvez profiter des fonctions de vSphere, vCenter Server, Active Directory et d'autres composants de votre infrastructure afin d'optimiser les performances, la disponibilité et la fiabilité de View Composer.

## Configuration de l'environnement vSphere pour View Composer

Pour prendre en charge View Composer, vous devez suivre certaines meilleures pratiques lorsque vous installez et configurez vCenter Server, ESX/ESXi et d'autres composants vSphere.

Ces meilleures pratiques permettent à View Composer de fonctionner efficacement dans l'environnement vSphere.

- Lorsque vous avez créé les informations sur le chemin d'accès et le dossier pour les machines virtuelles de clone lié, ne modifiez pas les informations dans vCenter Server. Utilisez plutôt View Administrator pour modifier les informations de dossier.

  Si vous modifiez ces informations dans vCenter Server, View Manager ne peut pas rechercher correctement les machines virtuelles dans vCenter Server.

- Assurez-vous que les paramètres de vSwitch sur l'hôte ESX/ESXi sont configurés avec suffisamment de ports pour prendre en charge toutes les cartes réseau virtuelles qui sont configurées sur les machines virtuelles de clone lié exécutées sur l'hôte ESX/ESXi.

- Lorsque vous déployez des postes de travail de clone lié dans un pool de ressources, assurez-vous que votre environnement vSphere contient assez de CPU et de mémoire pour héberger le nombre de postes de travail dont vous avez besoin. Utilisez vSphere Client pour contrôler l'utilisation de CPU et de mémoire dans les pools de ressources.

- Dans vSphere 5.1 et supérieur, un cluster utilisé pour des clones liés View Composer peut contenir plus de 8 hôtes ESX/ESXi si les disques de réplica sont stockés sur des magasins de données VMFS5 ou supérieur ou sur des magasins de données NFS. Si vous stockez les réplicas sur une version VMFS antérieure à VMFS5, un cluster peut contenir 8 hôtes au maximum.

  Dans vSphere 5.0, vous pouvez sélectionner un cluster avec plus de 8 hôtes ESXi si les réplicas sont stockés sur des magasins de données NFS. Si vous stockez les réplicas sur des magasins de données VMFS, un cluster peut contenir au maximum 8 hôtes.

- Utilisez vSphere DRS. DRS distribue efficacement des machines virtuelles de clone lié à vos hôtes.

**REMARQUE** Storage vMotion n'est pas pris en charge pour des postes de travail de clone lié.

## Meilleures pratiques supplémentaires pour View Composer

Pour vous assurer que View Composer fonctionne efficacement, vérifiez que votre DNS (Dynamic Name Service) fonctionne correctement et exécutez des analyses de logiciel antivirus à des heures décalées.

En vous assurant que la résolution DNS fonctionne correctement, vous pouvez résoudre des problèmes intermittents causés par des erreurs DNS. Le service View Composer repose sur la résolution de nom dynamique pour communiquer avec d'autres ordinateurs. Pour tester le fonctionnement de DNS, effectuez un test Ping sur les ordinateurs Active Directory et View Connection Server par nom.

Si vous décalez les heures d'exécution de votre logiciel antivirus, les performances des postes de travail de clone lié ne sont pas affectées. Si le logiciel antivirus s'exécute dans tous les clones liés à la même heure, des opérations d'E/S par seconde (IOPS) excessives se produisent pour votre sous-système de stockage. Cette activité excessive peut affecter les performances des postes de travail de clone lié.

# Installation de View Connection Server 5

Pour utiliser View Connection Server, vous installez le logiciel sur des ordinateurs pris en charge, configurez les composants requis et, de façon facultative, optimisez les composants.

Ce chapitre aborde les rubriques suivantes :



## Installation du logiciel View Connection Server

En fonction des besoins en termes de performances, de disponibilité et de sécurité de votre déploiement de View, vous pouvez installer une instance unique de View Connection Server, des instances répliquées de View Connection Server et des serveurs de sécurité. Vous devez installer au moins une instance de View Connection Server.

Lorsque vous installez View Connection Server, vous sélectionnez un type d'installation.

| | |
|---|---|
| **Installation standard** | Génère une instance de View Connection Server avec une nouvelle configuration View LDAP. |
| **Installation de réplica** | Génère une instance de View Connection Server avec une configuration View LDAP copiée depuis une instance existante. |
| **Installation de serveur de sécurité** | Génère une instance de View Connection Server qui ajoute une couche supplémentaire de sécurité entre Internet et votre réseau interne. |

# Conditions préalables d'installation pour Serveur de connexion View

Avant d'installer Serveur de connexion View, vous devez vérifier que votre environnement d'installation satisfait des conditions préalables spécifiques.

- Serveur de connexion View nécessite une clé de licence valide pour View Manager. Les clés de licence suivantes sont disponibles :
  - View Manager
  - View Manager avec View Composer et mode local
- Vous devez associer l'hôte de Serveur de connexion View à un domaine Active Directory. Serveur de connexion View prend en charge les versions suivantes d'Active Directory :
  - Windows 2003 Active Directory
  - Windows 2008 Active Directory

  L'hôte de Serveur de connexion View ne doit pas être un contrôleur de domaine.

  **REMARQUE** Serveur de connexion View ne fait ni ne requiert de mises à jour de schéma ou de configuration pour Active Directory.
- N'installez pas Serveur de connexion View sur des systèmes sur lesquels le rôle Windows Terminal Server est installé. Vous devez supprimer le rôle Windows Terminal Server du système sur lequel vous installez Serveur de connexion View.
- N'installez pas Serveur de connexion View sur un système qui effectue d'autres fonctions ou rôles. Par exemple, n'utilisez pas le même système pour héberger vCenter Server.
- Le système sur lequel vous installez Serveur de connexion View doit avoir une adresse IP statique.
- Pour exécuter le programme d'installation de Serveur de connexion View, vous devez utiliser un compte d'utilisateur de domaine avec des privilèges d'administrateur sur le système.
- Lorsque vous installez Serveur de connexion View, vous autorisez un compte d'administrateur View. Vous pouvez spécifier le groupe d'administrateurs local ou un compte d'utilisateur ou de groupe de domaine. View affecte des droits d'administration de View complets, y compris le droit d'installer des instances répliquées du serveur de connexion View, à ce compte uniquement. Si vous spécifiez un utilisateur ou un groupe de domaine, vous devez créer le compte dans Active Directory avant d'exécuter le programme d'installation.

# Installer Serveur de connexion View avec une nouvelle configuration

Pour installer Serveur de connexion View en tant que serveur unique ou en tant que première instance d'un groupe d'instances de Serveur de connexion View répliquées, vous utilisez l'option d'installation standard.

Lorsque vous sélectionnez l'option d'installation standard, l'installation crée une nouvelle configuration View LDAP locale. L'installation charge les définitions de schémas, la définition de DIT (Directory Information Tree) et des ACL et initialise les données.

Après l'installation, vous gérez la plupart des données de configuration View LDAP à l'aide de View Administrator. Serveur de connexion View conserve automatiquement certaines entrées de View LDAP.

Le logiciel Serveur de connexion View ne peut pas coexister sur la même machine virtuelle ou physique avec d'autres composants logiciels de View Manager, y compris un serveur réplica, un serveur de sécurité, View Composer, View Agent, View Client ou Serveur de transfert View.

Lorsque vous installez Serveur de connexion View avec une nouvelle configuration, vous pouvez participer à un programme d'amélioration de l'expérience utilisateur. VMware collecte des données anonymes sur votre déploiement afin d'améliorer la réponse de VMware aux exigences des utilisateurs. Aucune donnée identifiant votre entreprise n'est collectée. Vous pouvez choisir de ne pas participer en désélectionnant cette option lors

de l'installation. Si vous changez d'avis quant à la participation après l'installation, vous pouvez participer ou vous retirer du programme en modifiant la page Licence produit et utilisation dans View Administrator. Pour consulter la liste des champs dont les données sont collectées, y compris les champs qui restent anonymes, consultez la section « Informations collectées par le programme d'amélioration de l'expérience utilisateur » dans le document *Administration de VMware Horizon View*.

### Prérequis

- Vérifiez que vous pouvez ouvrir une session en tant qu'utilisateur de domaine avec des privilèges d'administrateur sur l'ordinateur Windows Server sur lequel vous installez Serveur de connexion View.
- Vérifiez que votre installation satisfait les exigences décrites dans la section « Exigences de View Connection Server », page 7.
- Préparez votre environnement pour l'installation. Reportez-vous à la section « Conditions préalables d'installation pour Serveur de connexion View », page 42.
- Si vous prévoyez d'autoriser un utilisateur ou un groupe de domaine en tant que compte de View Administrators, vérifiez que vous avez créé le compte de domaine dans Active Directory.
- Si vous utilisez l'authentification MIT Kerberos pour vous connecter à un ordinateur Windows Server 2008 R2 sur lequel vous installez Serveur de connexion View, installez le correctif Microsoft décrit dans l'article 978116 de la base de connaissances à l'adresse http://support.microsoft.com/kb/978116.
- Préparez un mot de passe de récupération de données. Lorsque vous sauvegardez Serveur de connexion View, la configuration View LDAP est exportée sous forme de données LDIF cryptées. Pour restaurer la configuration View de sauvegarde cryptée, vous devez fournir le mot de passe de récupération de données. Le mot de passe doit contenir entre 1 et 128 caractères. Suivez les meilleures pratiques de votre entreprise concernant la génération de mots de passe sécurisés.

  **Important** Vous aurez besoin du mot de passe de récupération de données pour laisser View en fonctionnement et éviter les temps d'arrêt dans un scénario de continuité d'activité et de récupération d'urgence (BC/DR). Vous pouvez fournir un rappel de mot de passe avec le mot de passe lorsque vous installez Serveur de connexion View.

- Familiarisez-vous avec les ports réseau qui doivent être ouverts sur le Pare-feu Windows pour les instances de Serveur de connexion View. Reportez-vous à la section « Règles de pare-feu pour le serveur de connexion View », page 61.
- Si vous prévoyez de coupler un serveur de sécurité avec cette instance du serveur de connexion View, vérifiez que le Pare-feu Windows avec sécurité avancée est défini sur **[activé]** dans les profils actifs. Il vous est recommandé de régler ce paramètre sur **[activé]** pour tous les profils. Par défaut, des règles IPsec régissent les connexions entre le serveur de sécurité et le serveur de connexion View et requièrent que le Pare-feu Windows avec sécurité avancée soit activé.
- Si votre topologie de réseau inclut un pare-feu principal entre un serveur de sécurité et l'instance de Serveur de connexion View, vous devez configurer le pare-feu pour qu'il prenne en charge IPsec. Reportez-vous à la section « Configuration d'un pare-feu principal pour prendre en charge IPsec », page 62.

### Procédure

1 Téléchargez le fichier du programme d'installation de Serveur de connexion View sur la page de produits VMware à l'adresse http://www.vmware.com/fr/products/ sur l'ordinateur Windows Server.

  Le nom de fichier du programme d'installation est `VMware-viewconnectionserver-x86_64-`*`y.y.y-xxxxxx`*`.exe`, où *xxxxxx* est le numéro de build et *y.y.y* le numéro de version.

2 Pour démarrer le programme d'installation de Serveur de connexion View, double-cliquez sur le fichier du programme d'installation.

3 Acceptez les termes de licence VMware.

4 Acceptez ou modifiez le dossier de destination.

5 Sélectionnez l'option d'installation **[Serveur standard View]** .

6 Tapez un mot de passe de récupération de données et éventuellement un rappel de mot de passe.

7 Choisissez comment configurer le service Pare-feu Windows.

| Option | Action |
|---|---|
| **Configurer le Pare-feu Windows automatiquement** | Laissez le programme d'installation configurer le Pare-feu Windows pour autoriser les connexions réseau requises. |
| **Ne pas configurer le Pare-feu Windows** | Configurez les règles de pare-feu Windows manuellement.<br>Sélectionnez cette option uniquement si votre entreprise utilise ses propres règles prédéfinies pour la configuration du pare-feu Windows. |

8 Autorisez un compte de View Administrators.

Seuls les membres de ce compte peuvent ouvrir une session sur View Administrator, disposer de droits d'administration View complets et installer des instances répliquées de Serveur de connexion View et d'autres serveurs View.

| Option | Description |
|---|---|
| **Autoriser le groupe d'administrateurs local** | Permet aux utilisateurs dans le groupe d'administrateurs local d'administrer View. |
| **Autoriser un utilisateur ou un groupe de domaine spécifique** | Permet à l'utilisateur ou au groupe de domaine spécifié d'administrer View. |

9 Si vous avez spécifié un compte de View Administrators de domaine, et que vous exécutez le programme d'installation en tant qu'administrateur local ou un autre utilisateur sans accès au compte de domaine, fournissez des informations d'identification pour ouvrir une session sur le domaine avec un nom d'utilisateur et un mot de passe autorisés.

Utilisez le format *domain name**user name* ou le format d'utilisateur principal (UPN). Le format UPN peut être comme suit *user@domain.com*.

10 Choisissez si vous voulez participer au programme d'amélioration de l'expérience utilisateur.

Si vous participez, vous pouvez éventuellement sélectionner le type, la taille et l'adresse de votre entreprise.

11 Effectuez l'assistant d'installation pour terminer l'installation de Serveur de connexion View.

12 Recherchez les nouveaux correctifs sur l'ordinateur Windows Server et exécutez Windows Update, le cas échéant.

Même si vous avez corrigé complètement l'ordinateur Windows Server avant l'installation de Serveur de connexion View, l'installation peut avoir activé des fonctions du système d'exploitation pour la première fois. Dans ce cas, des correctifs supplémentaires peuvent être nécessaires.

Les services View sont installés sur l'ordinateur Windows Server :

- Serveur de connexion View VMware
- Composant de l'infrastructure VMware View
- Composant du bus de message VMware View
- Hôte de script VMware View
- Composant de la passerelle de sécurité VMware View
- VMware View PCoIP Secure Gateway

- VMware View Blast Secure Gateway
- Composant Web VMware View
- VMware VDMDS, qui fournit des services d'annuaire View LDAP

Pour plus d'informations sur ces services, consultez le document *Administration de VMware Horizon View*.

### Suivant

Configurez des certificats de serveur SSL pour Serveur de connexion View. Reportez-vous à la section Chapitre 7, « Configuration de certificats SSL pour des View Servers », page 75.

Effectuez la configuration initiale sur Serveur de connexion View. Reportez-vous à la section Chapitre 8, « Première configuration de View », page 95.

Si vous prévoyez d'inclure des instances de Serveur de connexion View répliquées et des serveurs de sécurité dans votre déploiement, vous devez installer chaque instance de serveur en exécutant le fichier du programme d'installation de Serveur de connexion View.

Si vous réinstallez Serveur de connexion View sur un système d'exploitation Windows Server 2008 et que vous possédez un ensemble de collecteur de données pour analyser les données de performances, arrêtez l'ensemble de collecteur de données et démarrez-le de nouveau.

## Installer Serveur de connexion View en silence

Vous pouvez utiliser la fonction d'installation silencieuse de MSI (Microsoft Windows Installer) pour effectuer une installation standard de Serveur de connexion View sur plusieurs ordinateurs Windows. Dans une installation silencieuse, vous utilisez la ligne de commande et n'avez pas à répondre à des invites d'assistant.

Avec l'installation silencieuse, vous pouvez déployer efficacement des composants View dans une grande entreprise.

### Prérequis

- Vérifiez que vous pouvez ouvrir une session en tant qu'utilisateur de domaine avec des privilèges d'administrateur sur l'ordinateur Windows Server sur lequel vous installez Serveur de connexion View.
- Vérifiez que votre installation satisfait les exigences décrites dans la section « Exigences de View Connection Server », page 7.
- Préparez votre environnement pour l'installation. Reportez-vous à la section « Conditions préalables d'installation pour Serveur de connexion View », page 42.
- Si vous prévoyez d'autoriser un utilisateur ou un groupe de domaine en tant que compte de View Administrators, vérifiez que vous avez créé le compte de domaine dans Active Directory.
- Si vous utilisez l'authentification MIT Kerberos pour vous connecter à un ordinateur Windows Server 2008 R2 sur lequel vous installez Serveur de connexion View, installez le correctif Microsoft décrit dans l'article 978116 de la base de connaissances à l'adresse http://support.microsoft.com/kb/978116.
- Familiarisez-vous avec les ports réseau qui doivent être ouverts sur le Pare-feu Windows pour les instances de Serveur de connexion View. Reportez-vous à la section « Règles de pare-feu pour le serveur de connexion View », page 61.
- Si vous prévoyez de coupler un serveur de sécurité avec cette instance du serveur de connexion View, vérifiez que le Pare-feu Windows avec sécurité avancée est défini sur **[activé]** dans les profils actifs. Il vous est recommandé de régler ce paramètre sur **[activé]** pour tous les profils. Par défaut, des règles IPsec régissent les connexions entre le serveur de sécurité et le serveur de connexion View et requièrent que le Pare-feu Windows avec sécurité avancée soit activé.
- Si votre topologie de réseau inclut un pare-feu principal entre un serveur de sécurité et l'instance de Serveur de connexion View, vous devez configurer le pare-feu pour qu'il prenne en charge IPsec. Reportez-vous à la section « Configuration d'un pare-feu principal pour prendre en charge IPsec », page 62.

- Vérifiez que l'ordinateur Windows sur lequel vous installez Serveur de connexion View a la version 2.0 ou supérieure du moteur runtime MSI. Pour plus d'informations, consultez le site Web Microsoft.
- Familiarisez-vous avec les options de ligne de commande du programme d'installation MSI. Reportez-vous à la section « Options de ligne de commande Microsoft Windows Installer », page 64.
- Familiarisez-vous avec les propriétés d'installation silencieuse disponibles avec une installation standard de Serveur de connexion View. Reportez-vous à la section « Propriétés de l'installation silencieuse pour une installation standard de Serveur de connexion View », page 47.

### Procédure

1 Téléchargez le fichier du programme d'installation de Serveur de connexion View sur la page de produits VMware à l'adresse http://www.vmware.com/fr/products/ sur l'ordinateur Windows Server.

   Le nom de fichier du programme d'installation est `VMware-viewconnectionserver-x86_64-`*`y.y.y-xxxxxx`*`.exe`, où *xxxxxx* est le numéro de build et *y.y.y* le numéro de version.

2 Ouvrez une invite de commande sur l'ordinateur Windows Server.

3 Saisissez la commande d'installation sur une ligne.

   Par exemple : `VMware-viewconnectionserver-`*`y.y.y-xxxxxx`*`.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=1 VDM_INITIAL_ADMIN_SID=S-1-5-32-544 VDM_SERVER_RECOVERY_PWD=mini VDM_SERVER_RECOVERY_PWD_REMINDER=""First car"""`

   **Important** Lorsque vous exécutez une installation silencieuse, l'ensemble de la ligne de commande, y compris le mot de passe de récupération de données, est journalisé dans le fichier `vminst.log` du programme d'installation. À la fin de l'installation, supprimez ce fichier journal ou changez le mot de passe de récupération de données en utilisant View Administrator.

4 Recherchez les nouveaux correctifs sur l'ordinateur Windows Server et exécutez Windows Update, le cas échéant.

   Même si vous avez corrigé complètement l'ordinateur Windows Server avant l'installation de Serveur de connexion View, l'installation peut avoir activé des fonctions du système d'exploitation pour la première fois. Dans ce cas, des correctifs supplémentaires peuvent être nécessaires.

Les services View sont installés sur l'ordinateur Windows Server. Pour plus d'informations, reportez-vous à la section « Installer Serveur de connexion View avec une nouvelle configuration », page 42.

### Suivant

Configurez des certificats de serveur SSL pour Serveur de connexion View. Reportez-vous à la section Chapitre 7, « Configuration de certificats SSL pour des View Servers », page 75.

Si vous configurez View pour la première fois, effectuez la configuration initiale sur Serveur de connexion View. Reportez-vous à la section Chapitre 8, « Première configuration de View », page 95.

### Propriétés de l'installation silencieuse pour une installation standard de Serveur de connexion View

Vous pouvez inclure des propriétés de Serveur de connexion View spécifiques lorsque vous effectuez une installation silencieuse depuis la ligne de commande. Vous devez utiliser un format *PROPERTY=value* pour que Microsoft Windows Installer (MSI) puisse interpréter les propriétés et les valeurs.

**Tableau 5-1.** Propriétés MSI pour l'installation silencieuse de Serveur de connexion View dans une installation standard

| Propriété MSI | Description | Valeur par défaut |
|---|---|---|
| INSTALLDIR | Chemin d'accès et dossier dans lequel le logiciel Serveur de connexion View est installé.<br>Par exemple : `INSTALLDIR=""D:\abc\my folder""`<br>Les jeux de deux guillemets doubles entourant le chemin autorisent le programme d'installation MSI à interpréter l'espace comme étant une partie valide du chemin. | `%ProgramFiles %\VMware\VMware View\Server` |
| VDM_SERVER_ INSTANCE_TYPE | Type d'installation du serveur View :<br>■ **1**. Installation standard<br>■ **2**. Installation de réplica<br>■ **3**. Installation d'un serveur de sécurité<br>■ **4**. Installation de Serveur de transfert View<br>Par exemple, pour effectuer une installation standard, définissez `VDM_SERVER_INSTANCE_TYPE=1` | 1 |
| FWCHOICE | Propriété MSI qui détermine de configurer un pare-feu pour l'instance de Serveur de connexion View.<br>Une valeur de 1 configure un pare-feu. Une valeur de 2 ne configure pas un pare-feu.<br>Par exemple : `FWCHOICE=1` | 1 |
| VDM_INITIAL_ ADMIN_SID | SID de l'utilisateur ou du groupe d'administrateurs View initial qui est autorisé avec des droits d'administration complets dans View.<br>La valeur par défaut est le SID du groupe d'administrateurs local sur l'ordinateur Serveur de connexion View. Vous pouvez spécifier un SID d'un compte d'utilisateur ou de groupe de domaine. | `S-1-5-32-544` |
| VDM_SERVER_ RECOVERY_PWD | Mot de passe de récupération de données. Si aucun mot de passe de récupération de données n'est défini dans View LDAP, cette propriété est obligatoire.<br>Le mot de passe doit contenir entre 1 et 128 caractères. Suivez les meilleures pratiques de votre entreprise concernant la génération de mots de passe sécurisés. | Aucun |
| VDM_SERVER_RECOVERY_ PWD_REMINDER | Rappel du mot de passe de récupération de données. Cette propriété est facultative. | Aucun |

## Installer une instance répliquée de Serveur de connexion View

Pour fournir une disponibilité élevée et un équilibrage de charge, vous pouvez installer une ou plusieurs instances supplémentaires de Serveur de connexion View qui répliquent une instance de Serveur de connexion View existante. Après l'installation de réplica, les instances existantes et les instances venant d'être installées de Serveur de connexion View sont identiques.

Lorsque vous installez une instance répliquée, View Manager copie les données de configuration View LDAP depuis l'instance de Serveur de connexion View existante.

Après l'installation, le logiciel View Manager conserve les données de configuration View LDAP identiques sur toutes les instances de Serveur de connexion View dans le groupe répliqué. Lorsqu'une modification est faite sur une instance, les informations mises à jour sont copiées sur les autres instances.

Si une instance répliquée échoue, les autres instances du groupe continuent de fonctionner. Lorsque l'instance échouée reprend l'activité, sa configuration est mise à jour avec les modifications qui ont eu lieu au cours de la panne.

**Remarque** La fonction de réplication est fournie par View LDAP, qui utilise la même technologie de réplication qu'Active Directory.

Le logiciel du serveur réplica ne peut pas coexister sur la même machine virtuelle ou physique avec d'autres composants logiciels de View Manager, y compris un serveur de sécurité, Serveur de connexion View, View Composer, View Agent, View Client ou Serveur de transfert View.

### Prérequis

- Vérifiez qu'au moins une instance de Serveur de connexion View est installée et configurée sur le réseau.
- Pour installer l'instance répliquée, vous devez ouvrir une session en tant qu'utilisateur avec le rôle View Administrators. Vous spécifiez le compte ou le groupe avec le rôle View Administrators lorsque vous installez la première instance de Serveur de connexion View. Le rôle peut être attribué au groupe d'administrateurs local ou à un utilisateur ou un groupe de domaine. Reportez-vous à la section « Installer Serveur de connexion View avec une nouvelle configuration », page 42.
- Si l'instance de Serveur de connexion View existante se trouve dans un domaine différent de celui de l'instance répliquée, l'utilisateur de domaine doit également disposer de privilèges View Administrator sur l'ordinateur Windows Server sur lequel l'instance existante est installée.
- Si vous utilisez l'authentification MIT Kerberos pour vous connecter à un ordinateur Windows Server 2008 R2 sur lequel vous installez Serveur de connexion View, installez le correctif Microsoft décrit dans l'article 978116 de la base de connaissances à l'adresse http://support.microsoft.com/kb/978116.
- Vérifiez que votre installation satisfait les exigences décrites dans la section « Exigences de View Connection Server », page 7.
- Vérifiez que les ordinateurs sur lesquels vous installez des instances répliquées de Serveur de connexion View sont connectés sur un réseau LAN haute performance. Reportez-vous à la section « Exigences de réseau pour des instances répliquées de Serveur de connexion View », page 9.
- Préparez votre environnement pour l'installation. Reportez-vous à la section « Conditions préalables d'installation pour Serveur de connexion View », page 42.
- Si vous installez une instance de Serveur de connexion View répliquée correspondant à la version View 5.1 ou supérieure et que l'instance de Serveur de connexion View existante que vous répliquez correspond à la version View 5.0.*x* ou antérieure, préparez un mot de passe de récupération de données. Reportez-vous à la section « Installer Serveur de connexion View avec une nouvelle configuration », page 42.
- Familiarisez-vous avec les ports réseau qui doivent être ouverts sur le Pare-feu Windows pour les instances de Serveur de connexion View. Reportez-vous à la section « Règles de pare-feu pour le serveur de connexion View », page 61.
- Si vous prévoyez de coupler un serveur de sécurité avec cette instance du serveur de connexion View, vérifiez que le Pare-feu Windows avec sécurité avancée est défini sur **[activé]** dans les profils actifs. Il vous est recommandé de régler ce paramètre sur **[activé]** pour tous les profils. Par défaut, des règles IPsec régissent les connexions entre le serveur de sécurité et le serveur de connexion View et requièrent que le Pare-feu Windows avec sécurité avancée soit activé.
- Si votre topologie de réseau inclut un pare-feu principal entre un serveur de sécurité et l'instance de Serveur de connexion View, vous devez configurer le pare-feu pour qu'il prenne en charge IPsec. Reportez-vous à la section « Configuration d'un pare-feu principal pour prendre en charge IPsec », page 62.

### Procédure

1 Téléchargez le fichier du programme d'installation de Serveur de connexion View sur la page de produits VMware à l'adresse http://www.vmware.com/fr/products/ sur l'ordinateur Windows Server.

Le nom de fichier du programme d'installation est `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`, où *xxxxxx* est le numéro de build et *y.y.y* le numéro de version.

2 Pour démarrer le programme d'installation de Serveur de connexion View, double-cliquez sur le fichier du programme d'installation.

3 Acceptez les termes de licence VMware.

4 Acceptez ou modifiez le dossier de destination.

5 Sélectionnez l'option d'installation **[View Replica Server]** .

6 Saisissez le nom d'hôte ou l'adresse IP de l'instance de Serveur de connexion View existante que vous répliquez.

7 Tapez un mot de passe de récupération de données et éventuellement un rappel de mot de passe.

Vous êtes invité à fournir un mot de passe de récupération de données uniquement si l'instance de Serveur de connexion View existante que vous répliquez correspond à la version View 5.0.*x* ou antérieure.

8 Choisissez comment configurer le service Pare-feu Windows.

| Option | Action |
|---|---|
| **Configurer le Pare-feu Windows automatiquement** | Laissez le programme d'installation configurer le Pare-feu Windows pour autoriser les connexions réseau requises. |
| **Ne pas configurer le Pare-feu Windows** | Configurez les règles de pare-feu Windows manuellement.<br>Sélectionnez cette option uniquement si votre entreprise utilise ses propres règles prédéfinies pour la configuration du pare-feu Windows. |

9 Effectuez l'assistant d'installation pour terminer l'installation de l'instance répliquée.

10 Recherchez les nouveaux correctifs sur l'ordinateur Windows Server et exécutez Windows Update, le cas échéant.

Même si vous avez corrigé complètement l'ordinateur Windows Server avant l'installation de Serveur de connexion View, l'installation peut avoir activé des fonctions du système d'exploitation pour la première fois. Dans ce cas, des correctifs supplémentaires peuvent être nécessaires.

Les services View sont installés sur l'ordinateur Windows Server :

- Serveur de connexion View VMware
- Composant de l'infrastructure VMware View
- Composant du bus de message VMware View
- Hôte de script VMware View
- Composant de la passerelle de sécurité VMware View
- VMware View PCoIP Secure Gateway
- VMware View Blast Secure Gateway
- Composant Web VMware View
- VMware VDMDS, qui fournit des services d'annuaire View LDAP

Pour plus d'informations sur ces services, consultez le document *Administration de VMware Horizon View*.

### Suivant

Configurez un certificat de serveur SSL pour l'instance de Serveur de connexion View. Reportez-vous à la section Chapitre 7, « Configuration de certificats SSL pour des View Servers », page 75.

Vous n'avez pas à effectuer une configuration View initiale sur une instance répliquée de Serveur de connexion View. L'instance répliquée hérite de sa configuration depuis l'instance de Serveur de connexion View existante.

Toutefois, il peut être nécessaire de configurer des paramètres de connexion client pour cette instance de Serveur de connexion View, et vous pouvez optimiser les paramètres Windows Server pour prendre en charge un déploiement de grande envergure. Reportez-vous aux sections « Configuration de connexions View Client », page 112 et « Dimensionnement de paramètres de Windows Server pour prendre en charge votre déploiement », page 122.

Si vous réinstallez Serveur de connexion View sur un système d'exploitation Windows Server 2008 et que vous possédez un ensemble de collecteur de données pour analyser les données de performances, arrêtez l'ensemble de collecteur de données et démarrez-le de nouveau.

## Installer une instance répliquée de Serveur de connexion View en silence

Vous pouvez utiliser la fonction d'installation silencieuse de MSI (Microsoft Windows Installer) pour installer une instance répliquée de Serveur de connexion View sur plusieurs ordinateurs Windows. Dans une installation silencieuse, vous utilisez la ligne de commande et n'avez pas à répondre à des invites d'assistant.

Avec l'installation silencieuse, vous pouvez déployer efficacement des composants View dans une grande entreprise.

### Prérequis

- Vérifiez qu'au moins une instance de Serveur de connexion View est installée et configurée sur le réseau.
- Pour installer l'instance répliquée, vous devez ouvrir une session en tant qu'utilisateur avec des informations d'identification pour accéder au compte de View Administrators. Vous spécifiez le compte de View Administrators lorsque vous installez la première instance de Serveur de connexion View. Le compte peut être le groupe d'administrateurs local ou un compte d'utilisateur ou de groupe de domaine. Reportez-vous à la section « Installer Serveur de connexion View avec une nouvelle configuration », page 42.
- Si l'instance de Serveur de connexion View existante se trouve dans un domaine différent de celui de l'instance répliquée, l'utilisateur de domaine doit également disposer de privilèges View Administrator sur l'ordinateur Windows Server sur lequel l'instance existante est installée.
- Si vous utilisez l'authentification MIT Kerberos pour vous connecter à un ordinateur Windows Server 2008 R2 sur lequel vous installez Serveur de connexion View, installez le correctif Microsoft décrit dans l'article 978116 de la base de connaissances à l'adresse http://support.microsoft.com/kb/978116.
- Vérifiez que votre installation satisfait les exigences décrites dans la section « Exigences de View Connection Server », page 7.
- Vérifiez que les ordinateurs sur lesquels vous installez des instances répliquées de Serveur de connexion View sont connectés sur un réseau LAN haute performance. Reportez-vous à la section « Exigences de réseau pour des instances répliquées de Serveur de connexion View », page 9.
- Préparez votre environnement pour l'installation. Reportez-vous à la section « Conditions préalables d'installation pour Serveur de connexion View », page 42.
- Familiarisez-vous avec les ports réseau qui doivent être ouverts sur le Pare-feu Windows pour les instances de Serveur de connexion View. Reportez-vous à la section « Règles de pare-feu pour le serveur de connexion View », page 61.

- Si vous prévoyez de coupler un serveur de sécurité avec cette instance du serveur de connexion View, vérifiez que le Pare-feu Windows avec sécurité avancée est défini sur **[on (activé)]** dans les profils actifs. Il vous est recommandé de régler ce paramètre sur **[on (activé)]** pour tous les profils. Par défaut, des règles IPsec régissent les connexions entre le serveur de sécurité et le serveur de connexion View et requièrent que le Pare-feu Windows avec sécurité avancée soit activé.
- Si votre topologie de réseau inclut un pare-feu principal entre un serveur de sécurité et l'instance de Serveur de connexion View, vous devez configurer le pare-feu pour qu'il prenne en charge IPsec. Reportez-vous à la section « Configuration d'un pare-feu principal pour prendre en charge IPsec », page 62.
- Familiarisez-vous avec les options de ligne de commande du programme d'installation MSI. Reportez-vous à la section « Options de ligne de commande Microsoft Windows Installer », page 64.
- Familiarisez-vous avec les propriétés d'installation silencieuse disponibles avec une installation de réplica de Serveur de connexion View. Reportez-vous à la section « Propriétés de l'installation silencieuse pour une instance répliquée de Serveur de connexion View », page 52.

### Procédure

1 Téléchargez le fichier du programme d'installation de Serveur de connexion View sur la page de produits VMware à l'adresse http://www.vmware.com/fr/products/ sur l'ordinateur Windows Server.

   Le nom de fichier du programme d'installation est `VMware-viewconnectionserver-x86_64-`*`y.y.y-xxxxxx`*`.exe`, où *xxxxxx* est le numéro de build et *y.y.y* le numéro de version.

2 Ouvrez une invite de commande sur l'ordinateur Windows Server.

3 Saisissez la commande d'installation sur une ligne.

   Par exemple : `VMware-viewconnectionserver-`*`y.y.y-xxxxxx`*`.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2 ADAM_PRIMARY_NAME=cs1.companydomain.com VDM_INITIAL_ADMIN_SID=S-1-5-32-544"`

   Si vous installez une instance de Serveur de connexion View répliquée correspondant à la version View 5.1 ou supérieure et que l'instance de Serveur de connexion View existante que vous répliquez correspond à la version View 5.0.*x* ou antérieure, vous devez spécifier un mot de passe de récupération de données et vous pouvez ajouter un rappel de mot de passe. Par exemple : `VMware-viewconnectionserver-`*`y.y.y-xxxxxx`*`.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2 ADAM_PRIMARY_NAME=cs1.companydomain.com VDM_INITIAL_ADMIN_SID=S-1-5-32-544 VDM_SERVER_RECOVERY_PWD=mini VDM_SERVER_RECOVERY_PWD_REMINDER=""First car"""`

   **Important** Lorsque vous exécutez une installation silencieuse, l'ensemble de la ligne de commande, y compris le mot de passe de récupération de données, est journalisé dans le fichier `vminst.log` du programme d'installation. À la fin de l'installation, supprimez ce fichier journal ou changez le mot de passe de récupération de données en utilisant View Administrator.

4 Recherchez les nouveaux correctifs sur l'ordinateur Windows Server et exécutez Windows Update, le cas échéant.

   Même si vous avez corrigé complètement l'ordinateur Windows Server avant l'installation de Serveur de connexion View, l'installation peut avoir activé des fonctions du système d'exploitation pour la première fois. Dans ce cas, des correctifs supplémentaires peuvent être nécessaires.

Les services View sont installés sur l'ordinateur Windows Server. Pour plus d'informations, reportez-vous à la section « Installer une instance répliquée de Serveur de connexion View », page 47.

### Suivant

Configurez un certificat de serveur SSL pour l'instance de Serveur de connexion View. Reportez-vous à la section Chapitre 7, « Configuration de certificats SSL pour des View Servers », page 75.

Vous n'avez pas à effectuer une configuration View initiale sur une instance répliquée de Serveur de connexion View. L'instance répliquée hérite de sa configuration depuis l'instance de Serveur de connexion View existante.

Toutefois, il peut être nécessaire de configurer des paramètres de connexion client pour cette instance de Serveur de connexion View, et vous pouvez optimiser les paramètres Windows Server pour prendre en charge un déploiement de grande envergure. Reportez-vous aux sections « Configuration de connexions View Client », page 112 et « Dimensionnement de paramètres de Windows Server pour prendre en charge votre déploiement », page 122.

## Propriétés de l'installation silencieuse pour une instance répliquée de Serveur de connexion View

Vous pouvez inclure des propriétés spécifiques lorsque vous installez en silence une instance de Serveur de connexion View répliquée depuis la ligne de commande. Vous devez utiliser un format *PROPERTY=value* pour que Microsoft Windows Installer (MSI) puisse interpréter les propriétés et les valeurs.

**Tableau 5-2.** Propriétés MSI pour l'installation silencieuse d'une instance répliquée de Serveur de connexion View

| Propriété MSI | Description | Valeur par défaut |
|---|---|---|
| INSTALLDIR | Chemin d'accès et dossier dans lequel le logiciel Serveur de connexion View est installé.<br>Par exemple : `INSTALLDIR=""D:\abc\my folder""`<br>Les jeux de deux guillemets doubles entourant le chemin autorisent le programme d'installation MSI à interpréter l'espace comme étant une partie valide du chemin.<br>Cette propriété MSI est facultative. | `%ProgramFiles %\VMware\VMware View\Server` |
| VDM_SERVER_INSTANCE_TYPE | Type d'installation du serveur View :<br>■ **1**. Installation standard<br>■ **2**. Installation de réplica<br>■ **3**. Installation d'un serveur de sécurité<br>■ **4**. Installation de Serveur de transfert View<br>Pour installer une instance répliquée, définissez `VDM_SERVER_INSTANCE_TYPE=2`<br>Cette propriété MSI est requise lors de l'installation d'un réplica. | 1 |
| ADAM_PRIMARY_NAME | Nom d'hôte ou adresse IP de l'instance de Serveur de connexion View existante que vous répliquez.<br>Par exemple : `ADAM_PRIMARY_NAME=cs1.companydomain.com`<br>Cette propriété MSI est requise. | Aucun |
| ADAM_PRIMARY_PORT | Port View LDAP de l'instance de Serveur de connexion View existante que vous répliquez.<br>Par exemple : `ADAM_PRIMARY_PORT=cs1.companydomain.com`<br>Cette propriété MSI est facultative. | Aucun |
| FWCHOICE | Propriété MSI qui détermine de configurer un pare-feu pour l'instance de Serveur de connexion View.<br>Une valeur de 1 configure un pare-feu. Une valeur de 2 ne configure pas un pare-feu.<br>Par exemple : `FWCHOICE=1`<br>Cette propriété MSI est facultative. | 1 |

**Tableau 5-2.** Propriétés MSI pour l'installation silencieuse d'une instance répliquée de Serveur de connexion View (suite)

| Propriété MSI | Description | Valeur par défaut |
|---|---|---|
| VDM_SERVER_ RECOVERY_PWD | Mot de passe de récupération de données. Si aucun mot de passe de récupération de données n'est défini dans View LDAP, cette propriété est obligatoire.<br>**Remarque** Le mot de passe de récupération de données n'est pas défini dans View LDAP si l'instance de Serveur de connexion View standard que vous répliquez est View 5.0 ou antérieur. Si l'instance de Serveur de connexion View que vous répliquez est View 5.1 ou supérieur, vous n'avez pas à fournir cette propriété.<br>Le mot de passe doit contenir entre 1 et 128 caractères. Suivez les meilleures pratiques de votre entreprise concernant la génération de mots de passe sécurisés. | Aucun |
| VDM_SERVER_RECOVERY_ PWD_REMINDER | Rappel du mot de passe de récupération de données. Cette propriété est facultative. | Aucun |

# Configurer un mot de passe de couplage de serveur de sécurité

Avant de pouvoir installer un serveur de sécurité, vous devez configurer un mot de passe de couplage de serveur de sécurité. Lorsque vous installez un serveur de sécurité avec le programme d'installation de Serveur de connexion View, le programme vous invite à fournir ce mot de passe lors du processus d'installation.

Le mot de passe de couplage de serveur de sécurité est un mot de passe à usage unique qui permet à un serveur de sécurité d'être couplé avec une instance de Serveur de connexion View. Le mot de passe devient non valide une fois que vous l'avez fourni au programme d'installation de Serveur de connexion View.

**Remarque** Vous ne pouvez pas coupler une version antérieure d'un serveur de sécurité avec la version actuelle de Serveur de connexion View. Si vous configurez un mot de passe de couplage sur la version actuelle de Serveur de connexion View et que vous essayez d'installer une version antérieure du serveur de sécurité, le mot de passe de couplage ne sera pas valide.

### Procédure

1 Dans View Administrator, sélectionnez **[Configuration de View] > [Serveurs]** .

2 Sous l'onglet Serveurs de connexion, sélectionnez l'instance de Serveur de connexion View à coupler avec le serveur de sécurité.

3 Dans le menu déroulant **[Plus de commandes]** , sélectionnez **[Spécifier un mot de passe de couplage de serveur de sécurité]** .

4 Saisissez le mot de passe dans les zones de texte Pairing password (Mot de passe de couplage) et Confirm (Confirmer) et spécifiez une valeur d'expiration du mot de passe.

Vous devez utiliser le mot de passe dans la période d'expiration spécifiée.

5 Cliquez sur **[OK]** pour configurer le mot de passe.

### Suivant

Installez un serveur de sécurité. Reportez-vous à la section « Installer un serveur de sécurité », page 54.

**Important** Si vous ne fournissez pas le mot de passe de couplage de serveur de sécurité au programme d'installation de Serveur de connexion View dans la période d'expiration du mot de passe, le mot de passe devient non valide et vous devez configurer un nouveau mot de passe.

# Installer un serveur de sécurité

Un serveur de sécurité est une instance de Serveur de connexion View qui ajoute une couche supplémentaire de sécurité entre Internet et votre réseau interne. Vous pouvez installer un ou plusieurs serveurs de sécurité à connecter à une instance de Serveur de connexion View.

Le logiciel du serveur de sécurité ne peut pas coexister sur la même machine virtuelle ou physique avec d'autres composants logiciels de View Manager, y compris un serveur réplica, Serveur de connexion View, View Composer, View Agent, View Client ou Serveur de transfert View.

### Prérequis

- Déterminez le type de topologie à utiliser. Par exemple, déterminez quelle solution d'équilibrage de charge utiliser. Décidez si les instances du Serveur de connexion View appairées avec des serveurs de sécurité seront dédiées aux utilisateurs du réseau externe. Pour plus d'informations, consultez le document *VMware Horizon View Architecture Planning*.

  **IMPORTANT** Si vous utilisez un équilibreur de charge, vous devez disposer d'adresses IP statiques pour l'équilibreur de charge et pour chaque serveur de sécurité. Par exemple, si vous utilisez un équilibreur de charge avec deux serveurs de sécurité, vous avez besoin de 3 adresses IP statiques.

- Vérifiez que votre installation satisfait les exigences décrites dans la section « Exigences de View Connection Server », page 7.
- Préparez votre environnement pour l'installation. Reportez-vous à la section « Conditions préalables d'installation pour Serveur de connexion View », page 42.
- Vérifiez que l'instance de Serveur de connexion View à être appairée avec le serveur de sécurité est installée et configurée et exécute une version du Serveur de connexion View qui est compatible avec la version du serveur de sécurité. Reportez-vous à la section « Matrice de compatibilité de composants Horizon View » dans le document *Mises à niveau VMware Horizon View*.
- Vérifiez que l'instance du Serveur de connexion View devant être appairée avec le serveur de sécurité est accessible à l'ordinateur sur lequel vous prévoyez d'installer le serveur de sécurité.
- Configurez un mot de passe de couplage de serveur de sécurité. Reportez-vous à la section « Configurer un mot de passe de couplage de serveur de sécurité », page 53.
- Familiarisez-vous avec le format des URL externes. Reportez-vous à la section « Configuration d'URL externes pour PCoIP Secure Gateway et les connexions par tunnel », page 115.
- Vérifiez que le Pare-feu Windows avec sécurité avancée est défini sur **[activé]** dans les profils actifs. Il vous est recommandé de régler ce paramètre sur **[activé]** pour tous les profils. Par défaut, des règles IPsec régissent les connexions entre le serveur de sécurité et le serveur de connexion View et requièrent que le Pare-feu Windows avec sécurité avancée soit activé.
- Familiarisez-vous avec les ports réseau qui doivent être ouverts sur le Pare-feu Windows pour un serveur de sécurité. Reportez-vous à la section « Règles de pare-feu pour le serveur de connexion View », page 61.
- Si votre topologie de réseau inclut un pare-feu principal entre le serveur de sécurité et Serveur de connexion View, vous devez configurer le pare-feu pour qu'il prenne en charge IPsec. Reportez-vous à la section « Configuration d'un pare-feu principal pour prendre en charge IPsec », page 62.
- Si vous mettez à niveau le serveur de sécurité ou le réinstallez, vérifiez que les règles IPsec existantes du serveur de sécurité ont été supprimées. Reportez-vous à la section « Se préparer à mettre à niveau ou à réinstaller un serveur de sécurité », page 60.

### Procédure

1 Téléchargez le fichier du programme d'installation de Serveur de connexion View sur la page de produits VMware à l'adresse http://www.vmware.com/fr/products/ sur l'ordinateur Windows Server.

Le nom de fichier du programme d'installation est `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`, où *xxxxxx* est le numéro de build et *y.y.y* le numéro de version.

2 Pour démarrer le programme d'installation de Serveur de connexion View, double-cliquez sur le fichier du programme d'installation.

3 Acceptez les termes de licence VMware.

4 Acceptez ou modifiez le dossier de destination.

5 Sélectionnez l'option d'installation **[View Security Server]** .

6 Saisissez le nom de domaine complet ou l'adresse IP de l'instance de Serveur de connexion View à coupler avec le serveur de sécurité dans la zone de texte **[Serveur]** .

Le serveur de sécurité transmet le trafic réseau à cette instance de Serveur de connexion View.

7 Saisissez le mot de passe de couplage de serveur de sécurité dans la zone de texte Mot de passe.

Si le mot de passe a expiré, vous pouvez utiliser View Administrator pour configurer un nouveau mot de passe et saisir le nouveau mot de passe dans le programme d'installation.

8 Dans la zone de texte **[URL externe]** , saisissez l'URL externe du serveur de sécurité pour les clients View Client qui utilisent les protocoles d'affichage RDP ou PCoIP.

L'URL doit contenir le protocole, le nom de serveur de sécurité résolvable par le client et le numéro de port. Les clients tunnel qui s'exécutent en dehors de votre réseau utilisent cette URL pour se connecter au serveur de sécurité.

Par exemple : `https://view.exemple.com:443`

9 Dans la zone de texte **[URL externe PCoIP]** , saisissez l'URL externe du serveur de sécurité pour les clients View Client qui utilisent le protocole d'affichage PCoIP.

Spécifiez l'URL externe PCoIP comme adresse IP avec le numéro de port 4172. N'incluez pas un nom de protocole.

Par exemple : `10.20.30.40:4172`

L'URL doit contenir l'adresse IP et le numéro de port qu'un système client peut utiliser pour atteindre le serveur de sécurité. Vous ne pouvez saisir du texte dans la zone de texte que si PCoIP Secure Gateway est installé sur le serveur de sécurité.

10 Dans la zone de texte **[URL externe Blast]** , tapez l'URL externe du serveur de sécurité pour les utilisateurs qui utilisent l'accès HTML pour se connecter à des postes de travail View.

L'URL doit contenir le protocole HTTPS, le nom d'hôte résolvable par le client et le numéro de port.

Par exemple : `https://myserver.example.com:8443`

Par défaut, l'URL inclut le nom de domaine complet de l'URL externe du tunnel sécurisé et le numéro de port par défaut, 8443. L'URL doit contenir le nom de domaine complet et le numéro de port qu'un système client peut utiliser pour atteindre ce serveur de sécurité.

11 Choisissez comment configurer le service Pare-feu Windows.

| Option | Action |
|---|---|
| **Configurer le Pare-feu Windows automatiquement** | Laissez le programme d'installation configurer le Pare-feu Windows pour autoriser les connexions réseau requises. |
| **Ne pas configurer le Pare-feu Windows** | Configurez les règles de pare-feu Windows manuellement.<br>Sélectionnez cette option uniquement si votre entreprise utilise ses propres règles prédéfinies pour la configuration du pare-feu Windows. |

12 Effectuez l'assistant d'installation pour terminer l'installation du serveur de sécurité.

Les services du serveur de sécurité sont installés sur l'ordinateur Windows Server :

- Serveur de sécurité VMware View
- VMware View Framework Component
- VMware View Security Gateway Component
- VMware View PCoIP Secure Gateway
- VMware Blast Secure Gateway

Pour plus d'informations sur ces services, consultez le document *Administration de VMware Horizon View*.

Le serveur de sécurité apparaît dans le volet Serveurs de sécurité dans View Administrator.

**Remarque** Si l'installation est annulée ou abandonnée, il peut être nécessaire de supprimer les règles IPsec du serveur de sécurité avant d'effectuer l'installation de nouveau. Exécutez cette étape, même si vous avez déjà supprimé les règles IPsec avant de réinstaller le serveur de sécurité ou de le mettre à niveau. Pour plus d'instructions sur la suppression des règles IPsec, reportez-vous à la section « Se préparer à mettre à niveau ou à réinstaller un serveur de sécurité », page 60.

### Suivant

Configurez un certificat de serveur SSL pour le serveur de sécurité. Reportez-vous à la section Chapitre 7, « Configuration de certificats SSL pour des View Servers », page 75.

Il peut être nécessaire de configurer des paramètres de connexion client pour le serveur de sécurité, et vous pouvez optimiser les paramètres Windows Server pour prendre en charge un déploiement de grande envergure. Reportez-vous aux sections « Configuration de connexions View Client », page 112 et « Dimensionnement de paramètres de Windows Server pour prendre en charge votre déploiement », page 122.

Si vos utilisateurs se connectent au serveur de sécurité via HTML Access, vous devez activer une règle dans le Pare-feu Windows pour ouvrir le port HTML Access. Reportez-vous à la section « Ouvrir le port utilisé par HTML Access sur des serveurs de sécurité », page 114.

Si vous réinstallez le serveur de sécurité sur un système d'exploitation Windows Server 2008 et que vous possédez un ensemble de collecteur de données pour analyser les données de performances, arrêtez l'ensemble de collecteur de données et démarrez-le de nouveau.

## Installer un serveur de sécurité en silence

Vous pouvez utiliser la fonction d'installation silencieuse de MSI (Microsoft Windows Installer) pour installer un serveur de sécurité sur plusieurs ordinateurs Windows. Dans une installation silencieuse, vous utilisez la ligne de commande et n'avez pas à répondre à des invites d'assistant.

Avec l'installation silencieuse, vous pouvez déployer efficacement des composants View dans une grande entreprise.

### Prérequis

- Déterminez le type de topologie à utiliser. Par exemple, déterminez quelle solution d'équilibrage de charge utiliser. Décidez si les instances du Serveur de connexion View appairées avec des serveurs de sécurité seront dédiées aux utilisateurs du réseau externe. Pour plus d'informations, consultez le document *VMware Horizon View Architecture Planning*.

  **IMPORTANT** Si vous utilisez un équilibreur de charge, vous devez disposer d'adresses IP statiques pour l'équilibreur de charge et pour chaque serveur de sécurité. Par exemple, si vous utilisez un équilibreur de charge avec deux serveurs de sécurité, vous avez besoin de 3 adresses IP statiques.

- Vérifiez que votre installation satisfait les exigences décrites dans la section « Exigences de View Connection Server », page 7.
- Préparez votre environnement pour l'installation. Reportez-vous à la section « Conditions préalables d'installation pour Serveur de connexion View », page 42.
- Vérifiez que l'instance de Serveur de connexion View à être appairée avec le serveur de sécurité est installée et configurée et exécute une version du Serveur de connexion View qui est compatible avec la version du serveur de sécurité. Reportez-vous à la section « Matrice de compatibilité de composants Horizon View » dans le document *Mises à niveau VMware Horizon View*.
- Vérifiez que l'instance du Serveur de connexion View devant être appairée avec le serveur de sécurité est accessible à l'ordinateur sur lequel vous prévoyez d'installer le serveur de sécurité.
- Configurez un mot de passe de couplage de serveur de sécurité. Reportez-vous à la section « Configurer un mot de passe de couplage de serveur de sécurité », page 53.
- Familiarisez-vous avec le format des URL externes. Reportez-vous à la section « Configuration d'URL externes pour PCoIP Secure Gateway et les connexions par tunnel », page 115.
- Vérifiez que le Pare-feu Windows avec sécurité avancée est défini sur **[activé]** dans les profils actifs. Il vous est recommandé de régler ce paramètre sur **[activé]** pour tous les profils. Par défaut, des règles IPsec régissent les connexions entre le serveur de sécurité et le serveur de connexion View et requièrent que le Pare-feu Windows avec sécurité avancée soit activé.
- Familiarisez-vous avec les ports réseau qui doivent être ouverts sur le Pare-feu Windows pour un serveur de sécurité. Reportez-vous à la section « Règles de pare-feu pour le serveur de connexion View », page 61.
- Si votre topologie de réseau inclut un pare-feu principal entre le serveur de sécurité et Serveur de connexion View, vous devez configurer le pare-feu pour qu'il prenne en charge IPsec. Reportez-vous à la section « Configuration d'un pare-feu principal pour prendre en charge IPsec », page 62.
- Si vous mettez à niveau le serveur de sécurité ou le réinstallez, vérifiez que les règles IPsec existantes du serveur de sécurité ont été supprimées. Reportez-vous à la section « Se préparer à mettre à niveau ou à réinstaller un serveur de sécurité », page 60.
- Familiarisez-vous avec les options de ligne de commande du programme d'installation MSI. Reportez-vous à la section « Options de ligne de commande Microsoft Windows Installer », page 64.
- Familiarisez-vous avec les propriétés d'installation silencieuse disponibles avec un serveur de sécurité. Reportez-vous à la section « Propriétés de l'installation silencieuse pour un serveur de sécurité », page 59.

### Procédure

1 Téléchargez le fichier du programme d'installation de Serveur de connexion View sur la page de produits VMware à l'adresse http://www.vmware.com/fr/products/ sur l'ordinateur Windows Server.

  Le nom de fichier du programme d'installation est `VMware-viewconnectionserver-x86_64-`*`y.y.y`*`-`*`xxxxxx`*`.exe`, où *xxxxxx* est le numéro de build et *y.y.y* le numéro de version.

2 Ouvrez une invite de commande sur l'ordinateur Windows Server.

3 Saisissez la commande d'installation sur une ligne.

Par exemple : `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=3 VDM_SERVER_NAME=cs1.internaldomain.com VDM_SERVER_SS_EXTURL=https://view.companydomain.com:443 VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40 VDM_SERVER_SS_PCOIP_TCPPORT=4172 VDM_SERVER_SS_PCOIP_UDPPORT=4172 VDM_SERVER_SS_BSG_EXTURL=https://view.companydomain.com:8443 VDM_SERVER_SS_PWD=secret"`

Les services View sont installés sur l'ordinateur Windows Server. Pour plus d'informations, reportez-vous à la section « Installer un serveur de sécurité », page 54.

**Remarque** Si l'installation est annulée ou abandonnée, il peut être nécessaire de supprimer les règles IPsec du serveur de sécurité avant d'effectuer l'installation de nouveau. Exécutez cette étape, même si vous avez déjà supprimé les règles IPsec avant de réinstaller le serveur de sécurité ou de le mettre à niveau. Pour plus d'instructions sur la suppression des règles IPsec, reportez-vous à la section « Se préparer à mettre à niveau ou à réinstaller un serveur de sécurité », page 60.

### Suivant

Configurez un certificat de serveur SSL pour le serveur de sécurité. Reportez-vous à la section Chapitre 7, « Configuration de certificats SSL pour des View Servers », page 75.

Il peut être nécessaire de configurer des paramètres de connexion client pour le serveur de sécurité, et vous pouvez optimiser les paramètres Windows Server pour prendre en charge un déploiement de grande envergure. Reportez-vous aux sections « Configuration de connexions View Client », page 112 et « Dimensionnement de paramètres de Windows Server pour prendre en charge votre déploiement », page 122.

Si vos utilisateurs se connectent au serveur de sécurité via HTML Access, vous devez activer une règle dans le Pare-feu Windows pour ouvrir le port HTML Access. Reportez-vous à la section « Ouvrir le port utilisé par HTML Access sur des serveurs de sécurité », page 114.

## Propriétés de l'installation silencieuse pour un serveur de sécurité

Vous pouvez inclure des propriétés spécifiques lorsque vous installez en silence un serveur de sécurité depuis la ligne de commande. Vous devez utiliser un format *PROPERTY=value* pour que Microsoft Windows Installer (MSI) puisse interpréter les propriétés et les valeurs.

**Tableau 5-3.** Propriétés MSI pour installer un serveur de sécurité en silence

| Propriété MSI | Description | Valeur par défaut |
|---|---|---|
| INSTALLDIR | Chemin d'accès et dossier dans lequel le logiciel Serveur de connexion View est installé.<br>Par exemple : `INSTALLDIR=""D:\abc\my folder""`<br>Les jeux de deux guillemets doubles entourant le chemin autorisent le programme d'installation MSI à interpréter l'espace comme étant une partie valide du chemin.<br>Cette propriété MSI est facultative. | `%ProgramFiles %\VMware\VMware View\Server` |
| VDM_SERVER_INSTANCE_TYPE | Type d'installation du serveur View :<br>■ **1**. Installation standard<br>■ **2**. Installation de réplica<br>■ **3**. Installation d'un serveur de sécurité<br>■ **4**. Installation de Serveur de transfert View<br>Pour installer un serveur de sécurité, définissez `VDM_SERVER_INSTANCE_TYPE=3`<br>Cette propriété MSI est requise lors de l'installation d'un serveur de sécurité. | 1 |
| VDM_SERVER_NAME | Nom d'hôte ou adresse IP de l'instance de Serveur de connexion View existante à coupler avec le serveur de sécurité.<br>Par exemple : `VDM_SERVER_NAME=cs1.internaldomain.com`<br>Cette propriété MSI est requise. | Aucun |
| VDM_SERVER_SS_EXTURL | URL externe du serveur de sécurité. L'URL doit contenir le protocole, le nom de serveur de sécurité résolvable en externe et le numéro de port.<br>Par exemple : `VDM_SERVER_SS_EXTURL=https://view.companydomain.com:443`<br>Cette propriété MSI est requise. | Aucun |
| VDM_SERVER_SS_PWD | Mot de passe de couplage de serveur de sécurité.<br>Par exemple : `VDM_SERVER_SS_PWD=secret`<br>Cette propriété MSI est requise. | Aucun |
| FWCHOICE | Propriété MSI qui détermine de configurer un pare-feu pour l'instance de Serveur de connexion View.<br>Une valeur de 1 configure un pare-feu. Une valeur de 2 ne configure pas un pare-feu.<br>Par exemple : `FWCHOICE=1`<br>Cette propriété MSI est facultative. | 1 |
| VDM_SERVER_SS_PCOIP_IP ADDR | Adresse IP externe de PCoIP Secure Gateway. Cette propriété n'est prise en charge que lorsque le serveur de sécurité est installé sur Windows Server 2008 R2 ou supérieur.<br>Par exemple : `VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40`<br>Cette propriété est requise si vous prévoyez d'utiliser le composant PCoIP Secure Gateway. | Aucun |

**Tableau 5-3.** Propriétés MSI pour installer un serveur de sécurité en silence (suite)

| Propriété MSI | Description | Valeur par défaut |
|---|---|---|
| VDM_SERVER_SS_PCOIP_TCPPORT | Numéro de port TCP externe de PCoIP Secure Gateway. Cette propriété n'est prise en charge que lorsque le serveur de sécurité est installé sur Windows Server 2008 R2 ou supérieur.<br>Par exemple : `VDM_SERVER_SS_PCOIP_TCPPORT=4172`<br>Cette propriété est requise si vous prévoyez d'utiliser le composant PCoIP Secure Gateway. | Aucun |
| VDM_SERVER_SS_PCOIP_UDPPORT | Numéro de port UDP externe de PCoIP Secure Gateway. Cette propriété n'est prise en charge que lorsque le serveur de sécurité est installé sur Windows Server 2008 R2 ou supérieur.<br>Par exemple : `VDM_SERVER_SS_PCOIP_UDPPORT=4172`<br>Cette propriété est requise si vous prévoyez d'utiliser le composant PCoIP Secure Gateway. | Aucun |
| VDM_SERVER_SS_BSG_EXTURL | URL externe de Blast Secure Gateway. L'URL doit contenir le protocole HTTPS, un nom de serveur de sécurité résolvable en externe et le numéro de port.<br>Par exemple : `VDM_SERVER_SS_BSG_EXTURL=https://view.companydomain.com:8443`<br>Le numéro de port par défaut est 8443. Blast Secure Gateway doit être installé sur le serveur de sécurité pour permettre aux utilisateurs d'établir des connexions Web avec des postes de travail View. | Aucun |
| VDM_SERVER_SS_FORCE_IPSEC | Force l'utilisation d'IPsec entre le serveur de sécurité et son instance de Serveur de connexion View couplée.<br>Par défaut, l'installation et le couplage sans assistance du serveur de sécurité sur une instance de Serveur de connexion View avec IPsec désactivé entraînent l'échec du couplage.<br>La valeur par défaut de 1 force le couplage IPsec. Définissez cette valeur sur 0 pour permettre le couplage sans IPsec. | 1 |

## Se préparer à mettre à niveau ou à réinstaller un serveur de sécurité

Avant de pouvoir mettre à niveau ou réinstaller une instance du serveur de sécurité, vous devez supprimer les règles IPsec actuelles qui régissent la communication entre le serveur de sécurité et son instance de Serveur de connexion View couplée. Si vous n'effectuez pas cette étape, la mise à niveau ou la réinstallation échoue.

**IMPORTANT** Cette tâche concerne les serveurs de sécurité View 5.1 et supérieur. Elle ne s'applique pas aux serveurs de sécurité View 5.0.x et antérieur.

Par défaut, la communication entre un serveur de sécurité et son instance de Serveur de connexion View couplée est régie par des règles IPsec. Lorsque vous mettez à niveau ou réinstallez le serveur de sécurité et le couplez de nouveau avec l'instance de Serveur de connexion View, un nouveau jeu de règles IPsec doit être établi. Si les règles IPsec existantes ne sont pas supprimées avant la mise à niveau ou la réinstallation, le couplage échoue.

Vous devez effectuer cette étape lorsque vous mettez à niveau ou réinstallez un serveur de sécurité et que vous utilisez IPsec pour protéger la communication entre le serveur de sécurité et Serveur de connexion View.

Vous pouvez configurer un couplage de serveur de sécurité initial sans utiliser de règles IPsec. Avant d'installer le serveur de sécurité, vous pouvez ouvrir View Administrator et désélectionner le paramètre général **[Utiliser IPSec pour les connexions du serveur de sécurité]** , qui est activé par défaut. Si les règles IPsec ne sont pas effectives, vous n'avez pas à les supprimer avant la mise à niveau ou la réinstallation.

**Remarque** Vous n'avez pas à supprimer un serveur de sécurité de View Administrator avant de mettre à niveau ou de réinstaller le serveur de sécurité. Supprimez un serveur de sécurité de View Administrator uniquement si vous prévoyez de le supprimer définitivement de l'environnement Horizon View.

Avec View 5.0.x et versions antérieures, vous pouviez supprimer un serveur de sécurité depuis l'interface utilisateur de View Administrator ou à l'aide de la commande `vdmadmin -S`. Dans View 5.1 et versions supérieures, vous devez utiliser `vdmadmin -S`. Consultez la section « Suppression de l'entrée pour une instance de Serveur de connexion View ou un serveur de sécurité à l'aide de l'option -S » dans le document *Administration de VMware Horizon View*.

**Avertissement** Si vous supprimez les règles IPsec pour un serveur de sécurité actif, la communication avec le serveur de sécurité est perdue jusqu'à ce que vous mettiez à niveau ou réinstalliez le serveur de sécurité.

### Procédure

1 Dans View Administrator, cliquez sur **[Configuration de View] > [Serveurs]** .

2 Sous l'onglet **[Serveurs de sécurité]** , sélectionnez un serveur de sécurité et cliquez sur **[Plus de commandes] > [Préparer la mise à niveau ou la réinstallation]** .

Si vous avez désactivé les règles IPsec avant l'installation du serveur de sécurité, ce paramètre est inactif. Dans ce cas, vous n'avez pas à supprimer les règles IPsec avant la réinstallation ou la mise à niveau.

3 Cliquez sur **[OK]** .

Les règles IPsec sont supprimées et le paramètre **[Préparer la mise à niveau ou la réinstallation]** devient inactif, ce qui indique que vous pouvez réinstaller ou mettre à niveau le serveur de sécurité.

### Suivant

Mettez à niveau ou réinstallez le serveur de sécurité.

## Règles de pare-feu pour le serveur de connexion View

Certains ports doivent être ouverts sur le pare-feu pour les instances de Serveur de connexion View et les serveurs de sécurité.

Lorsque vous installez Serveur de connexion View, le programme d'installation peut configurer de façon facultative les règles de pare-feu Windows requises à votre place. Ces règles ouvrent les ports utilisés par défaut. Si vous modifiez les ports par défaut après l'installation, vous devez configurer manuellement le pare-feu Windows pour permettre à des périphériques View Client de se connecter à View via les ports mis à jour.

**Tableau 5-4.** Ports ouverts lors de l'installation de Serveur de connexion View

| Protocole | Ports | Type d'instance de Serveur de connexion View |
|---|---|---|
| JMS | TCP 4001 entrant | Standard et réplica |
| JMSIR | TCP 4100 entrant | Standard et réplica |
| AJP13 | TCP 8009 entrant | Standard et réplica |
| HTTP | TCP 80 entrant | Standard, réplica et serveur de sécurité |

**Tableau 5-4.** Ports ouverts lors de l'installation de Serveur de connexion View (suite)

| Protocole | Ports | Type d'instance de Serveur de connexion View |
|---|---|---|
| HTTPS | TCP 443 entrant | Standard, réplica et serveur de sécurité |
| PCoIP | TCP 4172 entrant ;<br>UDP 4172 dans les deux directions | Standard, réplica et serveur de sécurité |

## Configuration d'un pare-feu principal pour prendre en charge IPsec

Si la topologie du réseau contient un pare-feu principal entre les serveurs de sécurité et les instances de Serveur de connexion View, vous devez configurer certains protocoles et ports sur le pare-feu pour prendre en charge IPsec. Si vous ne disposez pas d'une configuration correcte, les données envoyées entre un serveur de sécurité et une instance de Serveur de connexion View ne pourront pas traverser le pare-feu.

Par défaut, les règles IPsec régissent les connexions entre les serveurs de sécurité et les instances de Serveur de connexion View. Pour prendre en charge IPsec, le programme d'installation Serveur de connexion View peut définir les règles du pare-feu Windows sur les hôtes Windows Server où les View servers sont installés. Pour un pare-feu principal, vous devez définir les règles vous-même.

**Remarque** Il est vivement recommandé d'utiliser IPsec. Vous pouvez également désactiver le paramètre global View Administrator **[Use IPsec for Security Server Connections (Utiliser IPsec pour les connexions du Serveur de sécurité)]** .

Les règles suivantes doivent permettre le trafic bidirectionnel. Il peut être nécessaire de définir des règles distinctes pour le trafic entrant et le trafic sortant sur le pare-feu.

Différentes règles s'appliquent aux pare-feu qui utilisent NAT (Network Address Translation) et à ceux qui ne n'utilisent pas.

**Tableau 5-5.** Conditions de pare-feu non-NAT pour la prise en charge des règles IPsec

| Source | Protocole | Port | Destination | Remarques |
|---|---|---|---|---|
| Serveur de sécurité | ISAKMP | UDP 500 | Serveur de connexion View | Les serveurs de sécurité utilisent le port UDP 500 pour négocier la sécurité IPsec. |
| Serveur de sécurité | ESP | S/O | Serveur de connexion View | Le protocole ESP encapsule le trafic crypté IPsec.<br>Il est inutile de définir un port pour ESP dans le cadre de la règle. Si nécessaire, vous pouvez définir des adresses IP source et de destination pour réduire la portée de la règle. |

Les règles suivantes s'appliquent aux pare-feu qui utilisent NAT.

**Tableau 5-6.** Conditions de pare-feu NAT pour la prise en charge des règles IPsec

| Source | Protocole | Port | Destination | Remarques |
|---|---|---|---|---|
| Serveur de sécurité | ISAKMP | UDP 500 | Serveur de connexion View | Les serveurs de sécurité utilisent le port UDP 500 pour initier la négociation de sécurité Psec. |
| Serveur de sécurité | NAT-T ISAKMP | UDP 4500 | Serveur de connexion View | Les serveurs de sécurité utilisent le port UDP 4 500 pour traverser les NAT et négocier la sécurité IPsec. |

# Réinstaller Serveur de connexion View avec une configuration de sauvegarde

Dans certaines situations, vous pouvez avoir à réinstaller la version actuelle d'une instance de Serveur de connexion View et à restaurer la configuration View existante en important un fichier LDIF de sauvegarde contenant les données de configuration View LDAP.

Par exemple, dans le cadre d'un plan de continuité d'activité et de reprise d'activité (BC/DR), vous voulez peut-être avoir une procédure prête à mettre en place au cas où un datacenter cesse de fonctionner. La première étape d'un tel plan est de s'assurer que la configuration View LDAP est sauvegardée dans un autre emplacement. La deuxième étape consiste à installer Serveur de connexion View dans le nouvel emplacement et à importer la configuration de sauvegarde, comme décrit dans cette procédure.

Vous pouvez également utiliser cette procédure lorsque vous configurez un deuxième datacenter avec la configuration View existante. Ou vous pouvez l'utiliser si votre déploiement de View contient une seule instance de Serveur de connexion View et qu'un problème se produit avec ce serveur.

Vous n'avez pas à suivre cette procédure si vous avez plusieurs instances de Serveur de connexion View dans un groupe répliqué et qu'une seule instance tombe en panne. Vous pouvez simplement réinstaller Serveur de connexion View en tant qu'instance répliquée. Lors de l'installation, vous fournissez des informations de connexion à une autre instance de Serveur de connexion View et View restaure la configuration View LDAP à partir de l'autre instance.

### Prérequis

- Vérifiez que la configuration View LDAP a été sauvegardée vers un fichier LDIF crypté.
- Familiarisez-vous avec la restauration d'une configuration View LDAP à partir d'un fichier de sauvegarde LDIF à l'aide de la commande `vdmimport`.

  Consultez la section « Sauvegarde et restauration de données de configuration de View » dans le document *Administration de VMware Horizon View*.
- Familiarisez-vous avec les étapes d'installation d'une nouvelle instance de Serveur de connexion View. Reportez-vous à la section « Installer Serveur de connexion View avec une nouvelle configuration », page 42.

### Procédure

1 Installez Serveur de connexion View avec une nouvelle configuration.

2 Décryptez le fichier LDIF crypté.

  Par exemple :

```
vdmimport –d –p mypassword
–f MyEncryptedexport.LDF > MyDecryptedexport.LDF
```

3 Importez le fichier LDIF décrypté pour restaurer la configuration View LDAP.

  Par exemple :

```
vdmimport –f MyDecryptedexport.LDF
```

**Remarque** À ce stade, la configuration View n'est pas encore accessible. Les clients View ne peuvent pas accéder à Serveur de connexion View ou se connecter à leurs postes de travail.

4 Désinstallez Serveur de connexion View de l'ordinateur en utilisant l'utilitaire **[Ajout/Suppression de programmes]** de Windows.

   Ne désinstallez pas la configuration View LDAP, appelée instance AD LDS Instance VMwareVDMDS. Vous pouvez utiliser l'utilitaire **[Ajout/Suppression de programmes]** pour vérifier que l'instance AD LDS Instance VMwareVDMDS n'a pas été supprimée de l'ordinateur Windows Server.

5 Réinstallez Serveur de connexion View.

   À l'invite du programme d'installation, acceptez le répertoire View LDAP existant.

### Suivant

Configurez Serveur de connexion View et votre environnement View comme vous le feriez après avoir installé une instance de Serveur de connexion View avec une nouvelle configuration.

# Options de ligne de commande Microsoft Windows Installer

Pour installer des composants View en silence, vous devez utiliser des options et des propriétés de ligne de commande de MSI (Microsoft Windows Installer). Les programmes d'installation des composants View sont des programmes MSI et utilisent des fonctions MSI standard. Vous pouvez également utiliser des options de ligne de commande MSI pour désinstaller des composants View en silence.

Pour plus d'informations sur MSI, consultez le site Web Microsoft. Pour les options de ligne de commande MSI, rendez-vous sur le site Web de la bibliothèque MSDN (Microsoft Developer Network) et recherchez ces options. Pour voir comment utiliser la ligne de commande MSI, vous pouvez ouvrir une invite de commande sur l'ordinateur de composant View et saisir `msiexec /?`.

Pour exécuter un programme d'installation de composant View en silence, commencez par désactiver le programme de démarrage qui extrait le programme d'installation dans un répertoire temporaire et démarre une installation interactive.

Tableau 5-7 montre des options de ligne de commande qui contrôlent le programme de démarrage du programme d'installation.

**Tableau 5-7.** Options de ligne de commande du programme de démarrage d'un composant View

| Option | Description |
|---|---|
| `/s` | Désactive l'écran de démarrage et la boîte de dialogue d'extraction, qui empêche l'affichage de boîtes de dialogue interactives.<br>Par exemple : `VMware-viewconnectionserver-`*`y.y.y-xxxxxx`*`.exe /s`<br>L'option `/s` est requise pour exécuter une installation silencieuse. Dans les exemples, *xxxxxx* est le numéro de build et *y.y.y* le numéro de version. |
| `/v"`*`MSI_command_line_options`*`"` | Demande au programme d'installation de transmettre la chaîne comprise entre guillemets doubles que vous saisissez sur la ligne de commande sous forme de jeu d'options que MSI doit interpréter. Vous devez insérer des guillemets doubles avant et après vos entrées de ligne de commande. Placez un guillemet double après `/v` et à la fin de la ligne de commande.<br>Par exemple : `VMware-viewagent-`*`y.y.y-xxxxxx`*`.exe /s /v"`*`command_line_options`*`"`<br>Pour demander au programme d'installation MSI d'interpréter une chaîne contenant des espaces, insérez deux jeux de guillemets doubles avant et après la chaîne. Par exemple, vous voulez peut-être installer le composant View dans un nom de chemin d'installation contenant des espaces.<br>Par exemple : `VMware-viewconnectionserver-`*`y.y.y-xxxxxx`*`.exe /s /v"`*`command_line_options`* `INSTALLDIR=""d:\abc\my folder"""`<br>Dans cet exemple, le programme d'installation MSI transmet le chemin du répertoire d'installation et n'essaie pas d'interpréter la chaîne comme deux options de ligne de commande. Notez le guillemet double final entourant toute la ligne de commande.<br>L'option `/v"`*`command_line_options`*`"` est requise pour exécuter une installation silencieuse. |

Vous contrôlez le reste de l'installation silencieuse en transmettant des options de ligne de commande et des valeurs de propriété MSI au programme d'installation MSI, `msiexec.exe`. Le programme d'installation MSI comporte le code d'installation du composant View. Le programme d'installation utilise les valeurs et les options que vous saisissez dans la ligne de commande pour interpréter des choix d'installation et des options de configuration spécifiques au composant View.

Tableau 5-8 montre les options de ligne de commande et les valeurs de propriété MSI transmises au programme d'installation MSI.

**Tableau 5-8.** Options de ligne de commande MSI et propriétés MSI

| Option ou propriété MSI | Description |
|---|---|
| `/qn` | Demande au programme d'installation MSI de ne pas afficher les pages de l'assistant d'installation.<br>Par exemple, vous voulez peut-être installer View Agent en silence et n'utiliser que des options et des fonctions d'installation par défaut :<br>`VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn"`<br>Dans les exemples, *xxxxxx* est le numéro de build et *y.y.y* le numéro de version.<br>Vous pouvez également utiliser l'option `/qb` pour afficher les pages de l'assistant dans une installation non interactive et automatisée. Lors de l'installation, les pages de l'assistant sont affichées, mais vous ne pouvez pas y répondre.<br>L'option `/qn` ou `/qb` est requise pour exécuter une installation silencieuse. |
| `INSTALLDIR` | Spécifie un autre chemin d'installation pour le composant View.<br>Utilisez le format *`INSTALLDIR=path`* pour spécifier un chemin d'installation. Vous pouvez ignorer cette propriété MSI si vous voulez installer le composant View dans le chemin par défaut.<br>Cette propriété MSI est facultative. |
| `ADDLOCAL` | Détermine les fonctions spécifiques du composant à installer. Dans une installation interactive, le programme d'installation View affiche des options d'installation personnalisée à sélectionner. La propriété MSI, `ADDLOCAL`, vous permet de spécifier ces options d'installation sur la ligne de commande.<br>Pour installer toutes les options d'installation personnalisée disponibles, saisissez `ADDLOCAL=ALL`.<br>Par exemple : `VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=ALL"`<br>Si vous n'utilisez pas la propriété MSI, `ADDLOCAL`, les options d'installation par défaut sont installées.<br>Pour spécifier des options d'installation individuelles, saisissez une liste séparée par des virgules de noms d'option d'installation. N'utilisez pas d'espaces entre les noms. Utilisez le format *`ADDLOCAL=value,value,value...`*.<br>Par exemple, vous voulez peut-être installer View Agent dans un système d'exploitation client avec les fonctions View Composer Agent et PCoIP :<br>`VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,SVIAgent,PCoIP"`<br>**Remarque** La fonction `Core` est requise dans View Agent.<br>Cette propriété MSI est facultative. |

**Tableau 5-8.** Options de ligne de commande MSI et propriétés MSI (suite)

| Option ou propriété MSI | Description |
|---|---|
| REBOOT | Vous pouvez utiliser l'option `REBOOT=ReallySuppress` pour permettre à des tâches de configuration système de s'exécuter avant le redémarrage du système.<br>Cette propriété MSI est facultative. |
| `/l*v` *log_file* | Inscrit des informations de journalisation dans le fichier journal spécifié avec une sortie détaillée.<br>Par exemple : `/l*v ""%TEMP%\vmmsi.log""`<br>Cet exemple génère un fichier journal détaillé semblable au journal généré lors d'une installation interactive.<br>Vous pouvez utiliser cette option pour enregistrer des fonctions personnalisées qui peuvent s'appliquer de façon unique à votre installation. Vous pouvez utiliser les informations enregistrées pour spécifier des fonctions d'installation dans les installations silencieuses futures.<br>L'option `/l*v` est facultative. |

# Désinstallation en silence de produits View à l'aide d'options de ligne de commande MSI

Vous pouvez désinstaller des composants View à l'aide d'options de ligne de commande MSI (Microsoft Windows Installer).

## Syntaxe

```
msiexec.exe
/qb
/x
product_code
```

## Options

L'option `/qb` affiche la barre de progression de la désinstallation. Pour ne plus afficher la barre de progression de la désinstallation, remplacez l'option `/qb` par l'option `/qn`.

L'option `/x` désinstalle le composant View.

La chaîne *product_code* identifie les fichiers de produit du composant View pour le programme de désinstallation MSI. Vous pouvez trouver la chaîne *product_code* en recherchant `ProductCode` dans le fichier `%TEMP%\vmmsi.log` créé lors de l'installation.

Pour plus d'informations sur les options de ligne de commande MSI, reportez-vous à la section « Options de ligne de commande Microsoft Windows Installer », page 64.

## Exemples

Désinstallez une instance de View Connection Server.

```
msiexec.exe /qb /x {D6184123-57B7-26E2-809B-090435A8C16A}
```

# Installation de View Transfer Server 6

View Transfer Server transfère des données entre des postes de travail locaux et le datacenter au cours des opérations de restitution, d'emprunt et de réplication. Pour installer View Transfer Server, vous installez le logiciel sur une machine virtuelle Windows Server, ajoutez View Transfer Server à votre déploiement de View Manager et configurez le référentiel de Transfer Server.

Vous devez installer et configurer View Transfer Server si vous déployez View Client with Local Mode sur des ordinateurs client.

Vous devez posséder une licence pour installer View Transfer Server et utiliser des postes de travail locaux.

1 Installer Serveur de transfert View page 68

Serveur de transfert View télécharge des fichiers d'image système, synchronise des données entre des postes de travail locaux et les postes de travail distants correspondants dans le datacenter, et transfère des données lorsque des utilisateurs restituent et empruntent des postes de travail locaux. Vous installez Serveur de transfert View dans une machine virtuelle qui exécute Windows Server.

2 Ajouter Serveur de transfert View à View Manager page 69

Serveur de transfert View fonctionne avec Serveur de connexion View pour transférer des fichiers et des données entre des postes de travail locaux et le datacenter. Avant que Serveur de transfert View puisse effectuer ces tâches, vous devez l'ajouter à votre déploiement de View Manager.

3 Configurer le référentiel de Serveur de transfert page 70

Le référentiel de Serveur de transfert stocke des images de base View Composer pour des postes de travail de clone lié qui s'exécutent en mode local. Pour donner à Serveur de transfert View l'accès au référentiel de Serveur de transfert, vous devez le configurer dans View Manager. Si vous n'utilisez pas de clones liés View Composer en mode local, vous n'avez pas à configurer un référentiel de Serveur de transfert.

4 Règles de pare-feu pour Serveur de transfert View page 72

Certains ports TCP entrants doivent être ouverts sur le pare-feu pour les instances de Serveur de transfert View.

5 Installation de View Transfer Server en silence page 72

Vous pouvez installer View Transfer Server en silence en saisissant le nom de fichier du programme d'installation et des options d'installation sur la ligne de commande. Avec l'installation silencieuse, vous pouvez déployer efficacement des composants View dans une grande entreprise.

# Installer Serveur de transfert View

Serveur de transfert View télécharge des fichiers d'image système, synchronise des données entre des postes de travail locaux et les postes de travail distants correspondants dans le datacenter, et transfère des données lorsque des utilisateurs restituent et empruntent des postes de travail locaux. Vous installez Serveur de transfert View dans une machine virtuelle qui exécute Windows Server.

Au moment de l'exécution, Serveur de transfert View est déployé sur un serveur Web Apache. Lorsque vous installez Serveur de transfert View, le programme d'installation configure le serveur Web Apache en tant que service sur la machine virtuelle. Le service Apache utilise les ports 80 et 443.

### Prérequis

- Vérifiez que vous disposez des privilèges d'administrateur local pour le serveur Windows Server sur lequel vous souhaitez installer le Serveur de transfert View.
- Vérifiez que votre installation satisfait les exigences de Serveur de transfert View décrites dans la section « Exigences de View Transfer Server », page 12.
- Vérifiez que vous disposez d'une licence pour installer le Serveur de transfert View et pour utiliser les postes de travail locaux.
- Vérifiez que vous n'avez pas manuellement ajouté ou supprimé des périphériques PCI sur la machine virtuelle sur laquelle vous prévoyez d'installer Serveur de transfert View. Si vous ajoutez ou supprimez des périphériques PCI, View peut être incapable de découvrir des périphériques ajoutés à chaud, ce qui peut entraîner l'échec des opérations de transfert des données.
- Familiarisez-vous avec les ports réseau qui doivent être ouverts sur le Pare-feu Windows pour les instances de Serveur de connexion View. Reportez-vous à la section « Règles de pare-feu pour Serveur de transfert View », page 72.

### Procédure

1 Téléchargez le fichier du programme d'installation de Serveur de connexion View sur la page de produits VMware à l'adresse http://www.vmware.com/fr/products/ sur l'ordinateur Windows Server.

  Le nom de fichier du programme d'installation est `VMware-viewconnectionserver-x86_64-`*`y.y.y`*`-`*`xxxxxx`*`.exe`, où *xxxxxx* est le numéro de build et *y.y.y* le numéro de version.

2 Pour démarrer le programme d'installation, double-cliquez sur le fichier du programme d'installation.

3 Acceptez les termes de licence VMware.

4 Acceptez ou modifiez le dossier de destination.

5 Sélectionnez **[Serveur de transfert View]** .

6 Configurez le serveur Web Apache sur lequel Serveur de transfert View est déployé.

  Vous pouvez accepter les valeurs par défaut pour le domaine de réseau, le nom du serveur Apache et l'adresse e-mail de l'administrateur qui sont fournis par le programme d'installation.

7 Choisissez comment configurer le service Pare-feu Windows.

| Option | Action |
|---|---|
| **Configurer le Pare-feu Windows automatiquement** | Laissez le programme d'installation configurer le Pare-feu Windows pour autoriser les connexions réseau requises. |
| **Ne pas configurer le Pare-feu Windows** | Configurez les règles de pare-feu Windows manuellement. |

8 Effectuez le programme d'installation pour installer Serveur de transfert View.

Les services Serveur de transfert VMware View, View Transfer Server Control Service et VMware View Framework Component sont installés et démarrés sur la machine virtuelle.

### Suivant

Dans View Administrator, ajoutez Serveur de transfert View à votre déploiement de View Manager.

## Ajouter Serveur de transfert View à View Manager

Serveur de transfert View fonctionne avec Serveur de connexion View pour transférer des fichiers et des données entre des postes de travail locaux et le datacenter. Avant que Serveur de transfert View puisse effectuer ces tâches, vous devez l'ajouter à votre déploiement de View Manager.

Vous pouvez ajouter plusieurs instances de Serveur de transfert View à View Manager. Les instances de Serveur de transfert View accèdent à un référentiel de Serveur de transfert commun. Ils partagent la charge de travail de transfert pour les postes de travail locaux gérés par une instance de Serveur de connexion View ou par un groupe d'instances de Serveur de connexion View répliquées.

---

**Remarque** Quand Serveur de transfert View est ajouté à View Manager, sa règle d'automatisation DRS (Distributed Resource Scheduler) est définie sur Manual (Manuel), ce qui désactive efficacement DRS.

---

### Prérequis

- Vérifiez que Serveur de transfert View est installé sur une machine virtuelle Windows Server.
- Vérifiez que vCenter Server est ajouté à View Manager. La page **[Configuration de View] > [Serveurs]** dans View Administrator affiche les instances de vCenter Server qui sont ajoutées à View Manager.
- Si Serveur de transfert View est à la version 5.1 ou supérieure, et si vous prévoyez d'utiliser des postes de travail de clone lié en mode local, vérifiez que toutes les instances de Serveur de connexion View répliquées dans la configuration de View sont à la version 5.1 ou supérieure. Si une version antérieure de Serveur de connexion View envoie une demande pour publier une image de base au référentiel de Serveur de transfert, Serveur de transfert View ne peut pas effectuer l'opération de publication.

### Procédure

1. Dans View Administrator, cliquez sur **[Configuration de View] > [Serveurs]** .
2. Cliquez sur l'onglet Transfer Servers (Serveurs de transfert) et cliquez sur **[Ajouter]** .
3. Dans l'assistant Add Serveur de transfert (Ajouter un serveur Serveur de transfert), sélectionnez l'instance de vCenter Server qui gère la machine virtuelle Serveur de transfert View et cliquez sur **[Suivant]** .
4. Sélectionnez la machine virtuelle où Serveur de transfert View est installé et cliquez sur **[Terminer]** .

   Serveur de connexion View reconfigure la machine virtuelle avec quatre contrôleurs SCSI. Plusieurs contrôleurs SCSI augmentent le nombre de transferts de disque que Serveur de transfert View peut effectuer simultanément.

Dans View Administrator, l'instance de Serveur de transfert View apparaît dans le volet Serveur de transferts (Serveurs Serveur de transfert). Si aucun référentiel de Serveur de transfert n'est configuré, l'état de Serveur de transfert View passe de **[En attente]** à **[Aucun référentiel de Serveur de transfert configuré]** . Si un référentiel de Serveur de transfert est configuré, l'état passe de **[En attente]** à **[Référentiel de Serveur de transfert en cours d'initialisation]** à **[Prêt]** .

Ce processus peut prendre plusieurs minutes. Vous pouvez cliquer sur le bouton d'actualisation dans View Administrator pour vérifier l'état actuel.

Lorsque l'instance de Serveur de transfert View est ajoutée à View Manager, le service Apache est démarré sur la machine virtuelle Serveur de transfert View.

**AVERTISSEMENT** Si votre machine virtuelle Serveur de transfert View est une version antérieure à la version matérielle 7, vous devez configurer l'adresse IP statique sur la machine virtuelle Serveur de transfert View après avoir ajouté Serveur de transfert View à View Manager.

Lorsque plusieurs contrôleurs SCSI sont ajoutés à la machine virtuelle Serveur de transfert View, Windows supprime l'adresse IP statique et reconfigure la machine virtuelle pour utiliser DHCP. Une fois la machine virtuelle redémarrée, vous devez saisir de nouveau l'adresse IP statique dans la machine virtuelle.

# Configurer le référentiel de Serveur de transfert

Le référentiel de Serveur de transfert stocke des images de base View Composer pour des postes de travail de clone lié qui s'exécutent en mode local. Pour donner à Serveur de transfert View l'accès au référentiel de Serveur de transfert, vous devez le configurer dans View Manager. Si vous n'utilisez pas de clones liés View Composer en mode local, vous n'avez pas à configurer un référentiel de Serveur de transfert.

Si Serveur de transfert View est configuré dans View Manager avant que vous ne configuriez le référentiel de Serveur de transfert, Serveur de transfert View valide l'emplacement du référentiel de Serveur de transfert lors de la configuration.

Si vous prévoyez d'ajouter plusieurs instances de Serveur de transfert View à ce déploiement de View Manager, configurez le référentiel de Serveur de transfert sur un partage de réseau. Les autres instances de Serveur de transfert View ne peuvent pas accéder à un référentiel de Serveur de transfert configuré sur un lecteur local sur une instance de Serveur de transfert View.

Assurez-vous que le référentiel de Serveur de transfert est suffisamment volumineux pour stocker vos images de base générées par View Composer. La taille d'une image de base peut atteindre plusieurs gigaoctets.

Si vous configurez un référentiel de Serveur de transfert distant sur un partage de réseau, vous devez fournir un ID d'utilisateur avec des informations d'identification pour accéder au partage de réseau. Pour améliorer la sécurité de l'accès au référentiel de Serveur de transfert, il est recommandé de limiter l'accès au réseau pour le référentiel aux administrateurs de View.

### Prérequis

- Vérifiez que Serveur de transfert View est installé sur une machine virtuelle Windows Server.
- Vérifiez que Serveur de transfert View est ajouté à View Manager. Reportez-vous à la section « Ajouter Serveur de transfert View à View Manager », page 69.

  **REMARQUE** L'ajout de Serveur de transfert View à View Manager avant de configurer le référentiel de Serveur de transfert est conseillé, il ne s'agit pas d'une obligation.

### Procédure

1 Configurez un chemin et un dossier pour le référentiel de Serveur de transfert.

Le référentiel de Serveur de transfert peut se trouver sur un lecteur local ou un partage de réseau.

| Option | Action |
|---|---|
| **Local Transfer Server repository (Référentiel de Serveur de transfert local)** | Sur la machine virtuelle sur laquelle Serveur de transfert View est installé, créez un chemin et un dossier pour le référentiel de Serveur de transfert.<br>Par exemple : `C:\TransferRepository\` |
| **Remote Transfer Server repository (Référentiel de Serveur de transfert distant)** | Configurez un chemin d'accès UNC pour le partage de réseau.<br>Par exemple : `\\server.domain.com\TransferRepository\`<br>Toutes les instances de Serveur de transfert View que vous ajoutez à ce déploiement de View Manager doivent avoir un accès réseau au lecteur partagé. |

2 Dans View Administrator, cliquez sur **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** .

3 Mettez toutes les instances de Serveur de transfert View en mode de maintenance.

a Dans le panneau Transfer Servers (Serveurs de transfert), sélectionnez une instance de Serveur de transfert View.

b Cliquez sur **[Enter Maintenance Mode (Passer en mode de maintenance)]** et cliquez sur **[OK]** .

L'état de Serveur de transfert View passe sur **[Maintenance mode (Mode de maintenance)]** .

c Répétez l'Étape 3a et Étape 3b pour chaque instance.

Lorsque toutes les instances de Serveur de transfert View sont en mode de maintenance, les opérations de transfert actuelles sont arrêtées.

4 Dans le panneau General (Général) sur la page du référentiel de Serveur de transfert, cliquez sur **[Edit (Modifier)]** .

5 Saisissez l'emplacement du référentiel de Serveur de transfert et d'autres informations.

| Option | Description |
|---|---|
| **Partage de réseau** | ■ **[Path (Chemin d'accès)]** . Saisissez le chemin d'accès UNC que vous avez configuré.<br>■ **[User Name (Nom d'utilisateur)]** . Saisissez l'ID d'utilisateur d'un administrateur avec des informations d'identification pour accéder au partage de réseau.<br>■ **[Password (Mot de passe)]** . Saisissez le mot de passe d'administrateur.<br>■ **[Domain (Domaine)]** . Saisissez le nom de domaine du partage de réseau au format NetBIOS. N'utilisez pas le suffixe `.com`. |
| **Local filesystem (Système de fichiers local)** | Saisissez le chemin d'accès que vous avez configuré sur la machine virtuelle Serveur de transfert View locale. |

6 Cliquez sur **[OK]** .

Si le chemin de réseau ou le lecteur local du référentiel est incorrect, la boîte de dialogue Edit Transfer Server Repository (Modifier le référentiel de Serveur de transfert) affiche un message d'erreur et ne vous permet pas de configurer l'emplacement. Vous devez saisir un emplacement valide.

7 Sur la page **[View Configuration (Configuration de View)] > [Servers (Serveurs)]** , sélectionnez l'instance de Serveur de transfert View et cliquez sur **[Exit Maintenance Mode (Quitter le mode de maintenance)]** .

L'état de Serveur de transfert View passe sur **[Ready (Prêt)]** .

# Règles de pare-feu pour Serveur de transfert View

Certains ports TCP entrants doivent être ouverts sur le pare-feu pour les instances de Serveur de transfert View.

Le programme d'installation peut configurer facultativement les règles de pare-feu Windows requises pour vous. Ces règles ouvrent les ports utilisés par défaut. Si vous modifiez les ports par défaut après l'installation, vous devez configurer manuellement le pare-feu Windows pour permettre à des périphériques View Client de se connecter à Serveur de transfert View via les ports mis à jour.

Tableau 6-1 répertorie les ports TCP entrants qui doivent être ouverts sur le pare-feu pour les instances de Serveur de transfert View.

**Tableau 6-1.** Ports TCP pour des instances de Serveur de transfert View

| Protocole | Ports |
|---|---|
| HTTP | 80 |
| trafic | 443 |

# Installation de View Transfer Server en silence

Vous pouvez installer View Transfer Server en silence en saisissant le nom de fichier du programme d'installation et des options d'installation sur la ligne de commande. Avec l'installation silencieuse, vous pouvez déployer efficacement des composants View dans une grande entreprise.

## Définir des stratégies de groupe pour autoriser l'installation silencieuse de Serveur de transfert View

Avant de pouvoir installer Serveur de transfert View en silence, vous devez configurer des stratégies de groupe Microsoft Windows pour autoriser l'installation avec des privilèges élevés.

Vous devez définir des stratégies de groupe Windows Installer pour des ordinateurs et des utilisateurs sur l'ordinateur local.

### Prérequis

Vérifiez que vous disposez de privilèges d'administrateur local sur l'ordinateur Windows Server sur lequel vous allez installer Serveur de transfert View.

### Procédure

1 Ouvrez une session sur l'ordinateur Windows Server et cliquez sur **[Start (Démarrer)]** > **[Run (Exécuter)]** .

2 Saisissez **`gpedit.msc`** et cliquez sur **[OK]** .

3 Dans l'Éditeur d'objets de stratégie de groupe, cliquez sur **[Local Computer Policy (Stratégie Ordinateur local)]** > **[Computer Configuration (Configuration d'ordinateur)]** .

4 Développez **[Administrative Templates (Modèles administratifs)]** et **[Windows Components (Composants Window)]** , ouvrez le dossier **[Windows Installer]** et double-cliquez sur **[Always install with elevated privileges (Toujours installer avec des droits élevés)]** .

5 Dans la fenêtre **[Always Install with Elevated Privileges Properties (Propriétés de Toujours installer avec des droits élevés)]** , cliquez sur **[Enabled (Activé)]** et sur **[OK]** .

6 Dans le volet de gauche, cliquez sur **[User Configuration (Configuration utilisateur)]** .

7 Développez **[Administrative Templates (Modèles administratifs)]** et **[Windows Components (Composants Window)]** , ouvrez le dossier **[Windows Installer]** et double-cliquez sur **[Always install with elevated privileges (Toujours installer avec des droits élevés)]** .

8 Dans la fenêtre **[Always Install with Elevated Privileges Properties (Propriétés de Toujours installer avec des droits élevés)]** , cliquez sur **[Enabled (Activé)]** et sur **[OK]** .

### Suivant

Installez Serveur de transfert View en silence.

## Installer Serveur de transfert View en silence

Vous pouvez utiliser la fonction d'installation silencieuse de MSI (Microsoft Windows Installer) pour installer Serveur de transfert View sur plusieurs ordinateurs Windows. Dans une installation silencieuse, vous utilisez la ligne de commande et n'avez pas à répondre à des invites d'assistant.

### Prérequis

- Vérifiez que vous disposez des privilèges d'administrateur local pour le serveur Windows Server sur lequel vous souhaitez installer le Serveur de transfert View.
- Vérifiez que votre installation satisfait les exigences de Serveur de transfert View décrites dans la section « Exigences de View Transfer Server », page 12.
- Vérifiez que vous disposez d'une licence pour installer le Serveur de transfert View et pour utiliser les postes de travail locaux.
- Vérifiez que la machine virtuelle sur laquelle vous installez Serveur de transfert View a la version 2.0 ou supérieure du moteur runtime MSI. Pour plus d'informations, consultez le site Web Microsoft.
- Familiarisez-vous avec les options de ligne de commande du programme d'installation MSI. Reportez-vous à la section « Options de ligne de commande Microsoft Windows Installer », page 64.
- Familiarisez-vous avec les propriétés d'installation silencieuse disponibles avec Serveur de transfert View. Reportez-vous à la section « Propriétés de l'installation silencieuse pour View Transfer Server », page 74.
- Vérifiez que les stratégies de groupe Windows Installer requises pour l'installation silencieuse sont configurées sur l'ordinateur Windows Server. Reportez-vous à la section « Définir des stratégies de groupe pour autoriser l'installation silencieuse de Serveur de transfert View », page 72.

### Procédure

1 Téléchargez le fichier du programme d'installation de Serveur de connexion View sur la page de produits VMware à l'adresse http://www.vmware.com/fr/products/ sur l'ordinateur Windows Server.

   Le nom de fichier du programme d'installation est `VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe`, où *xxxxxx* est le numéro de build et *y.y.y* le numéro de version.

2 Ouvrez une invite de commande sur l'ordinateur Windows Server.

3 Saisissez la commande d'installation sur une ligne.

   Par exemple : `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=4"`

Les services Serveur de transfert VMware View, View Transfer Server Control Service et VMware View Framework Component sont installés et démarrés sur la machine virtuelle.

### Suivant

Dans View Administrator, ajoutez Serveur de transfert View à votre déploiement de View Manager.

## Propriétés de l'installation silencieuse pour View Transfer Server

Vous pouvez inclure des propriétés spécifiques lorsque vous installez en silence un serveur View Transfer Server depuis la ligne de commande. Vous devez utiliser un format *PROPERTY=value* pour que Microsoft Windows Installer (MSI) puisse interpréter les propriétés et les valeurs.

**Tableau 6-2.** Propriétés MSI pour l'installation silencieuse de View Transfer Server

| Propriété MSI | Description | Valeur par défaut |
|---|---|---|
| INSTALLDIR | Chemin d'accès et dossier dans lequel le logiciel View Connection Server est installé.<br>Par exemple : `INSTALLDIR=""D:\abc\my folder""`<br>Les jeux de deux guillemets doubles entourant le chemin autorisent le programme d'installation MSI à interpréter l'espace comme étant une partie valide du chemin.<br>Cette propriété MSI est facultative. | `%ProgramFiles %\VMware\VMware View\Server` |
| VDM_SERVER_INSTANCE_TYPE | Type d'installation du serveur View :<br>■ **1**. Installation standard<br>■ **2**. Installation de réplica<br>■ **3**. Installation d'un serveur de sécurité<br>■ **4**. Installation de View Transfer Server<br>Pour installer un serveur View Transfer Server, définissez `VDM_SERVER_INSTANCE_TYPE=4`<br>Cette propriété MSI est facultative pour une installation standard. Elle est requise pour tous les autres types d'installation. | 1 |
| SERVERDOMAIN | Domaine de réseau de la machine virtuelle sur laquelle vous installez View Transfer Server. Cette valeur correspond au domaine de réseau du serveur Web Apache configuré au cours d'une installation interactive.<br>Par exemple : `SERVERDOMAIN=companydomain.com`<br>Si vous spécifiez un domaine de serveur Web Apache personnalisé avec la propriété MSI, `SERVERDOMAIN`, vous devez également spécifier des propriétés `SERVERNAME` et `SERVERADMIN` personnalisées.<br>Cette propriété MSI est facultative. | Aucune |
| SERVERNAME | Nom d'hôte de la machine virtuelle sur laquelle vous installez View Transfer Server. Cette valeur correspond au nom d'hôte du serveur Web Apache configuré au cours d'une installation interactive.<br>Par exemple : `SERVERNAME=ts1.companydomain.com`<br>Si vous spécifiez un nom d'hôte de serveur Web Apache personnalisé avec la propriété MSI, `SERVERNAME`, vous devez également spécifier des propriétés `SERVERDOMAIN` et `SERVERADMIN` personnalisées.<br>Cette propriété MSI est facultative. | Aucune |
| SERVERADMIN | Adresse e-mail de l'administrateur du serveur Web Apache configurée avec View Transfer Server.<br>Par exemple : `SERVERADMIN=admin@companydomain.com`<br>Si vous spécifiez un administrateur de serveur Web Apache personnalisé avec la propriété MSI, `SERVERADMIN`, vous devez également spécifier des propriétés `SERVERDOMAIN` et `SERVERNAME` personnalisées.<br>Cette propriété MSI est facultative. | Aucune |
| FWCHOICE | Propriété MSI qui détermine de configurer un pare-feu pour l'instance de View Connection Server.<br>Une valeur de 1 configure un pare-feu. Une valeur de 2 ne configure pas un pare-feu.<br>Par exemple : `FWCHOICE=1`<br>Cette propriété MSI est facultative. | 1 |

# Configuration de certificats SSL pour des View Servers

7

VMware recommande vivement de configurer des certificats SSL pour l'authentification des instances de Serveur de connexion View, des serveurs de sécurité et des instances de View Composer.

Un certificat de serveur SSL par défaut est généré lorsque vous installez des instances de Serveur de connexion View, des serveurs de sécurité ou des instances de View Composer. Vous pouvez utiliser le certificat par défaut à des fins de test.

**IMPORTANT** Remplacez le certificat par défaut dès que possible. Le certificat par défaut n'est pas signé par une autorité de certification. L'utilisation de certificats non signés par une autorité de certification peut permettre à des parties non approuvées d'intercepter le trafic en se faisant passer pour votre serveur.

Ce chapitre aborde les rubriques suivantes :

# Comprendre les certificats SSL pour des serveurs View Server

Vous devez suivre certaines recommandations pour la configuration de certificats SSL pour les serveurs View Server et les composants associés.

## Serveur de connexion View et serveur de sécurité

SSL est requis pour les connexions de View Client vers View. Les instances client de Serveur de connexion View, les serveurs de sécurité et les serveurs intermédiaires qui terminent des connexions SSL requièrent des certificats de serveur SSL.

Par défaut, lorsque vous installez Serveur de connexion View ou un serveur de sécurité, l'installation génère un certificat auto-signé pour View Server. Toutefois, l'installation utilise un certificat existant dans les cas suivants :

- Si un certificat valide avec le nom convivial `vdm` existe déjà dans le magasin de certificats Windows.
- Si vous effectuez la mise à niveau vers View 5.1 ou supérieur depuis une version antérieure, et qu'un fichier de magasin de clés valide est configuré sur l'ordinateur Windows Server. L'installation extrait les clés et les certificats et les importe dans le magasin de certificats Windows.

## vCenter Server et View Composer

Avant d'ajouter vCenter Server et View Composer à View Manager dans un environnement de production, vérifiez que vCenter Server et View Composer utilisent des certificats signés par une autorité de certification.

Pour plus d'informations sur le remplacement du certificat par défaut pour vCenter Server, consultez le document « Remplacement des certificats vCenter Server » sur le site VMware Technical Papers à l'adresse http://www.vmware.com/resources/techresources/.

Si vous installez vCenter Server et View Composer sur le même hôte Windows Server, ils peuvent utiliser le même certificat SSL, mais vous devez configurer le certificat séparément pour chaque composant.

## PCoIP Secure Gateway

Pour respecter les réglementations de sécurité du secteur ou de la juridiction, vous pouvez remplacer le certificat SSL par défaut généré par le service PCoIP Secure Gateway (PSG) par un certificat signé par une autorité de certification. La configuration du service PSG pour utiliser un certificat signé par une autorité de certification est fortement recommandée, en particulier pour les déploiements qui nécessitent que vous utilisiez des scanners de sécurité pour passer les tests de conformité. Reportez-vous à la section « Configurer PCoIP Secure Gateway pour utiliser un nouveau certificat SSL », page 89.

## Blast Secure Gateway

Par défaut, Blast Secure Gateway (BSG) utilise le certificat SSL configuré pour l'instance de Serveur de connexion View ou le serveur de sécurité sur lequel est exécuté BSG. Si vous remplacez le certificat auto-signé par défaut pour View Server par un certificat signé par une autorité de certification, BSG utilise également le certificat signé par une autorité de certification.

## Serveur de transfert View

Vous n'avez pas à configurer des certificats SSL pour Serveur de transfert View si vous installez View 5.1 ou supérieur.

Un certificat auto-signé par défaut est installé avec Serveur de transfert View que Serveur de connexion View utilise pour gérer les connexions secondaires à des View Client. Reportez-vous à la section « Serveur de transfert View et certificats SSL », page 93.

### Authentificateur SAML 2.0

VMware Horizon Suite utilise des authentificateurs SAML 2.0 pour fournir une authentification et une autorisation basées sur le Web sur des domaines de sécurité. Si vous voulez que View délègue l'authentification à Horizon Suite, vous pouvez configurer View pour accepter les sessions authentifiées de SAML 2.0 depuis Horizon Suite. Lorsque Horizon Application Manager est configuré pour prendre en charge View, les utilisateurs de Horizon peuvent se connecter à des postes de travail View en sélectionnant des icônes de poste de travail sur Horizon User Portal.

Dans View Administrator, vous pouvez configurer des authentificateurs SAML 2.0 pour qu'ils utilisent des instances de Serveur de connexion View.

Avant d'ajouter un authentificateur SAML 2.0 dans View Administrator, vérifiez que l'authentificateur SAML 2.0 utilise un certificat signé par une autorité de certification.

### Recommandations supplémentaires

Pour plus d'informations générales sur la demande et l'utilisation des certificats SSL signés par une autorité de certification, reportez-vous à la section « Avantages des certificats SSL signés par une autorité de certification (CA) », page 94.

Lorsque des View Client se connectent à une instance de Serveur de connexion View ou un serveur de sécurité, ils se voient présenter le certificat de serveur SSL de View Server et des certificats intermédiaires dans la chaîne d'approbation. Pour approuver le certificat de serveur, les systèmes client doivent avoir installé le certificat racine de l'autorité de certification de signature.

Lorsque Serveur de connexion View communique avec vCenter Server et View Composer, Serveur de connexion View se voit présenter des certificats de serveur SSL et des certificats intermédiaires de ces serveurs. Pour approuver les serveurs vCenter Server et View Composer, l'ordinateur Serveur de connexion View doit avoir installé le certificat racine de l'autorité de certification de signature.

De la même façon, si un authentificateur SAML 2.0 est configuré pour Serveur de connexion View, l'ordinateur Serveur de connexion View doit avoir installé le certificat racine de l'autorité de certification de signature pour le certificat du serveur SAML 2.0.

## Présentation des tâches de configuration des certificats SSL

Pour configurer des certificats de serveur SSL pour des serveurs View Server, vous devez effectuer plusieurs tâches de haut niveau.

Les procédures pour réaliser ces tâches sont décrites dans les rubriques qui suivent cette présentation.

1 Déterminez si vous avez besoin d'obtenir un nouveau certificat SSL signé auprès d'une autorité de certification.

Si votre entreprise possède déjà un certificat de serveur SSL valide, vous pouvez l'utiliser pour remplacer le certificat de serveur SSL par défaut fourni avec Serveur de connexion View, le serveur de sécurité ou View Composer. Pour utiliser un certificat existant, vous avez également besoin de la clé privée qui l'accompagne.

| Point de départ | Action |
|---|---|
| Votre entreprise vous a fourni un certificat de serveur SSL valide. | Passez directement à l'étape 2. |
| Vous n'avez pas de certificat de serveur SSL. | Obtenez un certificat de serveur SSL signé auprès d'une autorité de certification. |

2 Importez le certificat SSL dans le magasin de certificats de l'ordinateur local Windows sur l'hôte de View Server.

3 Pour les instances de Serveur de connexion View et les serveurs de sécurité, modifiez le nom convivial du certificat en le renommant **vdm**.

   Attribuez le nom convivial **vdm** à un seul certificat sur chaque hôte de View Server.

4 Sur les ordinateurs Serveur de connexion View, si le certificat racine n'est pas approuvé par l'hôte Windows Server, importez-le dans le magasin de certificats de l'ordinateur local Windows.

   Effectuez cette étape uniquement pour les instances de Serveur de connexion View. Vous n'avez pas à importer le certificat racine dans les hôtes de View Composer, de vCenter Server ou du serveur de sécurité.

5 Si votre certificat de serveur a été signé par une autorité de certification intermédiaire, importez les certificats intermédiaires dans le magasin de certificats de l'ordinateur local Windows.

   Pour simplifier la configuration client, importez la chaîne de certificats complète dans le magasin de certificats de l'ordinateur local Windows. S'il manque des certificats intermédiaires sur View Server, ils doivent être configurés pour les View Client et les ordinateurs qui lancent View Administrator.

6 Pour les instances de View Composer, effectuez l'une de ces étapes :

   - Si vous importez le certificat dans le magasin de certificats de l'ordinateur local Windows avant d'installer View Composer, vous pouvez sélectionner votre certificat lors de l'installation de View Composer.
   - Si vous prévoyez de remplacer un certificat existant ou le certificat auto-signé par défaut par un nouveau certificat après avoir installé View Composer, exécutez l'utilitaire `SviConfig ReplaceCertificate` pour lier le nouveau certificat au port utilisé par View Composer.

7 Si votre autorité de certification n'est pas reconnue, configurez les View Client pour qu'ils approuvent les certificats racine et intermédiaires.

   Vérifiez également que les ordinateurs sur lesquels vous lancez View Administrator approuvent les certificats racine et intermédiaires.

8 Déterminez si vous voulez reconfigurer la vérification de la révocation des certificats.

   Serveur de connexion View effectue la vérification de la révocation des certificats sur les serveurs View Server, View Composer et vCenter Server. La plupart des certificats signés par une autorité de certification incluent des informations de révocation des certificats. Si votre autorité de certification n'inclut pas ces informations, vous pouvez configurer le serveur pour qu'il ne vérifie pas les certificats pour révocation.

   Si un authentificateur SAML 2.0 est configuré pour être utilisé avec une instance de Serveur de connexion View, Serveur de connexion View effectue également la vérification de la révocation des certificats sur le certificat du serveur SAML 2.0.

## Obtention d'un certificat SSL signé auprès d'une autorité de certification

Si votre entreprise ne vous fournit pas de certificat de serveur SSL, vous devez demander un nouveau certificat signé par une autorité de certification.

Vous pouvez utiliser plusieurs méthodes pour obtenir un nouveau certificat signé. Par exemple, vous pouvez utiliser l'utilitaire `certreq` de Microsoft pour générer une demande de signature de certificat (CSR) et envoyer une demande de certificat à une autorité de certification.

Consultez le document *Obtention de certificats SSL pour les serveurs VMware Horizon View* pour voir un exemple indiquant comment utiliser `certreq` pour réaliser cette tâche.

À des fins de test, vous pouvez obtenir un certificat temporaire gratuit basé sur une racine non approuvée de plusieurs autorités de certification.

Lorsque vous générez une demande de certificat sur un ordinateur, vérifiez qu'une clé privée est également générée. Lorsque vous obtenez le certificat de serveur SSL et l'importez dans le magasin de certificats de l'ordinateur local Windows, il doit y avoir une clé privée qui l'accompagne et qui correspond au certificat.

**Important** Ne créez pas de certificats pour des serveurs View Server à l'aide d'un modèle de certificat compatible uniquement avec une autorité de certification d'entreprise Windows Server 2008 ou supérieur.

**Important** Ne générez pas de certificats pour des serveurs View Server à l'aide d'une valeur `KeyLength` inférieure à 1 024. View Client pour Windows et View Client pour Windows with Local Mode ne valideront pas le certificat sur un View Server qui a été généré avec une valeur `KeyLength` inférieure à 1 024 et les View Client ne pourront pas se connecter à View. Les validations de certificat exécutées par Serveur de connexion View échoueront également ; les serveurs View Server affectés apparaîtront alors en rouge dans le tableau de bord de View Administrator.

Pour des informations générales sur l'obtention des certificats, consultez l'aide en ligne de Microsoft disponible avec le composant logiciel Certificat dans MMC. Si le composant logiciel Certificat n'est pas encore installé sur votre ordinateur, reportez-vous à la section « Ajouter le composant logiciel enfichable Certificat à MMC », page 81.

## Obtenir un certificat signé d'une autorité de certification de domaine ou d'entreprise Windows

Pour obtenir un certificat signé d'une autorité de certification de domaine ou d'entreprise Windows, vous pouvez utiliser l'assistant d'inscription de certificats Windows dans le magasin des certificats Windows.

Cette méthode de demande de certificat est adaptée si les communications entre les ordinateurs se limitent à votre domaine interne. Par exemple, l'obtention d'un certificat signé d'une autorité de certification Windows peut être appropriée pour les communications entre les serveurs.

Si les clients View Client se connectent aux View servers depuis un réseau externe, demandez des certificats de serveur SSL signés par une autorité de certification tierce de confiance.

### Prérequis

- Déterminez le nom de domaine complet (FQDN) que les ordinateurs client utilisent pour se connecter à l'hôte.
- Vérifiez que le composant logiciel enfichable Certificat a été ajouté à MMC. Reportez-vous à la section « Ajouter le composant logiciel enfichable Certificat à MMC », page 81.
- Vérifiez que vous disposez des données d'identification appropriées pour demander un certificat qui peut être envoyé à un ordinateur ou un service.

### Procédure

1. Dans la fenêtre MMC sur l'hôte de Windows Server, développez le noeud des **[certificats (ordinateur local)]** et sélectionnez le dossier **[Personal (Personnel)]** .
2. Dans le menu **[Action]** , accédez à **[All Tasks (Toutes les tâches)] > [Request New Certificate (Demander un nouveau certificat)]** pour afficher l'assistant d'inscription de certificats.
3. Sélectionnez une stratégie d'inscription de certificats.
4. Sélectionnez les types de certificats à demander et cliquez sur **[Enroll (Inscrire)]** .
5. Cliquez sur **[Finish (Terminer)]** .

Le nouveau certificat signé est ajouté au dossier **[Personal (Personnel)] > [Certificates (Certificats)]** dans le magasin des certificats Windows.

### Suivant

- Vérifiez que certificat de serveur et la chaîne de certificats ont été importés dans le magasin de certificats Windows.
- Pour une instance de Serveur de connexion View ou le serveur de sécurité, modifiez le nom convivial du certificat en le renommant **vdm**. Reportez-vous à la section « Modifier le nom convivial d'un certificat », page 82.
- Pour un Serveur View Composer, liez le nouveau certificat au port utilisé par View Composer. Reportez-vous à la section « Lier un nouveau certificat SSL au port utilisé par View Composer », page 84.

## Configurer Serveur de connexion View, le serveur de sécurité ou View Composer pour utiliser un nouveau certificat SSL

Pour configurer une instance de Serveur de connexion View, un serveur de sécurité ou une instance de View Composer afin qu'ils utilisent un certificat SSL, vous devez importer le certificat de serveur et la chaîne de certificats complète dans le magasin de certificats de l'ordinateur local Windows sur l'hôte de Serveur de connexion View, du serveur de sécurité ou de View Composer.

Par défaut, Blast Secure Gateway (BSG) utilise le certificat SSL configuré pour l'instance de Serveur de connexion View ou le serveur de sécurité sur lequel est exécuté BSG. Si vous remplacez le certificat auto-signé par défaut pour View Server par un certificat signé par une autorité de certification, BSG utilise également le certificat signé par une autorité de certification.

---

**IMPORTANT** Pour configurer Serveur de connexion View ou le serveur de sécurité pour qu'ils utilisent un certificat, vous devez modifier le nom convivial du certificat par **vdm**. De plus, le certificat doit avoir une clé privée qui l'accompagne.

Si vous prévoyez de remplacer un certificat existant ou le certificat auto-signé par défaut par un nouveau certificat après avoir installé View Composer, vous devez exécuter l'utilitaire `SviConfig ReplaceCertificate` pour lier le nouveau certificat au port utilisé par View Composer.

---

### Procédure

1 Ajouter le composant logiciel enfichable Certificat à MMC page 81

Pour pouvoir ajouter des certificats au magasin des certificats Windows, vous devez ajouter le composant logiciel enfichable Certificat à MMC (Microsoft Management Console) sur l'hôte Windows Server sur lequel View server est installé.

2 Importer un certificat de serveur signé dans un magasin de certificats Windows page 81

Vous devez importer le certificat de serveur SSL dans le magasin de certificats de l'ordinateur local Windows sur l'hôte Windows Server sur lequel l'instance de Serveur de connexion View, le serveur de sécurité ou le service View Composer est installé.

3 Modifier le nom convivial d'un certificat page 82

Pour configurer une instance de Serveur de connexion View ou le serveur de sécurité pour qu'il reconnaisse et utilise un certificat SSL, vous devez modifier le nom convivial du certificat en le renommant `vdm`.

4 Importer un certificat racine et des certificats intermédiaires dans un magasin de certificats Windows page 83

Si l'hôte Windows Server sur lequel Serveur de connexion View est installé n'approuve pas le certificat racine pour le certificat de serveur SSL signé, vous devez importer le certificat racine dans le magasin de certificats de l'ordinateur local Windows. En outre, si l'hôte de Serveur de connexion View n'approuve pas les certificats racine des certificats de serveur SSL configurés pour les hôtes du serveur de sécurité, de View Composer et de vCenter Server, vous devez également importer ces certificats racine.

5 Lier un nouveau certificat SSL au port utilisé par View Composer page 84

Si vous configurez un nouveau certificat SSL après l'installation de View Composer, vous devez exécuter l'utilitaire `SviConfig ReplaceCertificate` pour remplacer le certificat qui est lié au port utilisé par View Composer. Cet utilitaire délie le certificat existant et lie le nouveau certificat au port.

## Ajouter le composant logiciel enfichable Certificat à MMC

Pour pouvoir ajouter des certificats au magasin des certificats Windows, vous devez ajouter le composant logiciel enfichable Certificat à MMC (Microsoft Management Console) sur l'hôte Windows Server sur lequel View server est installé.

### Prérequis

Vérifiez que MMC et le composant logiciel enfichable Certificat sont disponibles sur l'ordinateur Windows Server sur lequel View server est installé.

### Procédure

1 Sur l'ordinateur Windows Server, cliquez sur **[Start (Démarrer)]** et tapez **`mmc.exe`**.

2 Dans la fenêtre MMC, accédez à **[File (Fichier)] > [Add/Remove Snap-in (Ajouter/Supprimer un composant logiciel enfichable)]** .

3 Dans la fenêtre Add or Remove Snap-ins (Ajouter ou supprimer des composants logiciels enfichables, sélectionnez **[Certificates (Certificats)]** et cliquez sur **[Add (Ajouter)]** .

4 Dans la fenêtre Certificates snap-in (Composant logiciel enfichable Certificats), sélectionnez **[Computer account (Compte d'ordinateur)]** , cliquez sur **[Next (Suivant)]** , sélectionnez **[Computer account (Ordinateur local)]** , puis cliquez sur **[Finish (Terminer)]** .

5 Dans la fenêtre Add or Remove snap-in (Ajouter ou supprimer des composants logiciels enfichables), cliquez sur **[OK]** .

### Suivant

Importez le certificat de serveur SSL dans le magasin des certificats Windows.

## Importer un certificat de serveur signé dans un magasin de certificats Windows

Vous devez importer le certificat de serveur SSL dans le magasin de certificats de l'ordinateur local Windows sur l'hôte Windows Server sur lequel l'instance de Serveur de connexion View, le serveur de sécurité ou le service View Composer est installé.

En fonction du format de votre fichier de certificat, la chaîne de certificats complète contenue dans le fichier de magasin de clés peut être importée dans le magasin de certificats de l'ordinateur local Windows. Par exemple, le certificat de serveur, le certificat intermédiaire et le certificat racine peuvent être importés.

Pour les autres types de fichiers de certificat, seul le certificat de serveur est importé dans le magasin de certificats de l'ordinateur local Windows. Dans ce cas, vous devez effectuer des étapes séparées pour importer le certificat racine et des certificats intermédiaires dans la chaîne de certificats.

Pour plus d'informations sur les certificats, consultez l'aide en ligne de Microsoft disponible avec le composant logiciel Certificat dans MMC.

---

**Remarque** Si vous déchargez des connexions SSL vers un serveur intermédiaire, vous devez importer le même certificat de serveur SSL sur le serveur intermédiaire et View Server déchargé. Pour plus d'informations, consultez la section « Décharger des connexions SSL sur des serveurs intermédiaires » dans le document *Administration de VMware Horizon View*.

---

### Prérequis

Vérifiez que le composant logiciel Certificat a été ajouté à MMC. Reportez-vous à la section « Ajouter le composant logiciel enfichable Certificat à MMC », page 81.

### Procédure

1 Dans la fenêtre MMC sur l'hôte Windows Server, développez le nœud **[Certificats (ordinateur local)]** et le dossier **[Personnel]** .

2 Dans le volet Actions, allez dans **[Autres actions]** > **[Toutes les tâches]** > **[Importer]** .

3 Dans l'assistant Importation de certificat, cliquez sur **[Suivant]** et accédez à l'emplacement de stockage du certificat.

4 Sélectionnez le fichier du certificat et cliquez sur **[Ouvrir]** .

Pour afficher votre type de fichier de certificat, vous pouvez sélectionner son format de fichier dans le menu déroulant **[Nom de fichier]** .

5 Tapez le mot de passe de la clé privée incluse dans le fichier de certificat.

6 Sélectionnez **[Marquer cette clé comme exportable]** .

7 Sélectionnez **[Inclure toutes les propriétés extensibles]** .

8 Cliquez sur **[Suivant]** et sur **[Terminer]** .

Le nouveau certificat apparaît dans le dossier **[Certificats (ordinateur local)]** > **[Personnel]** > **[Certificats]** .

9 Vérifiez que le nouveau certificat contient une clé privée.

a Dans le dossier **[Certificats (ordinateur local)]** > **[Personnel]** > **[Certificats]** , double-cliquez sur le nouveau certificat.

b Sous l'onglet Général de la boîte de dialogue Informations sur le certificat, vérifiez que la déclaration suivante existe : `Vous avez une clé privée qui correspond à ce certificat`.

### Suivant

Modifiez le nom convivial du certificat en le renommant **`vdm`**.

## Modifier le nom convivial d'un certificat

Pour configurer une instance de Serveur de connexion View ou le serveur de sécurité pour qu'il reconnaisse et utilise un certificat SSL, vous devez modifier le nom convivial du certificat en le renommant `vdm`.

Il est inutile de modifier le nom convivial des certificats SSL qu'utilise View Composer.

### Prérequis

Vérifiez que le certificat de serveur est importé dans le dossier **[Certificates (Local Computer) (Certificats (Ordinateur local))]** > **[Personal (Personnel)]** > **[Certificates (Certificats)]** dans le magasin de certificats Windows. Reportez-vous à la section « Importer un certificat de serveur signé dans un magasin de certificats Windows », page 81.

### Procédure

1 Dans la fenêtre MMC sur l'hôte Windows Server, développez le noeud des **[certificats (ordinateur local)]** et sélectionnez le dossier **[Personnal (Personnel)]** > **[Certificates (Certificats)]** .

2 Cliquez avec le bouton droit de la souris sur le certificat envoyé à l'hôte View server et cliquez sur **[Properties (Propriétés)]** .

3 Dans l'onglet General (Général), supprimez le texte **[Friendly name (Nom convivial)]** et tapez **`vdm`**.

4 Cliquez sur **[Apply (Appliquer)]** et sur **[OK]** .

### Suivant

Importez le certificat racine et les certificats intermédiaires dans le magasin de certificats de l'ordinateur local Windows.

Une fois tous les certificats de la chaîne importés, vous devez redémarrer le service Serveur de connexion View ou le service Serveur de sécurité pour appliquer les modifications.

## Importer un certificat racine et des certificats intermédiaires dans un magasin de certificats Windows

Si l'hôte Windows Server sur lequel Serveur de connexion View est installé n'approuve pas le certificat racine pour le certificat de serveur SSL signé, vous devez importer le certificat racine dans le magasin de certificats de l'ordinateur local Windows. En outre, si l'hôte de Serveur de connexion View n'approuve pas les certificats racine des certificats de serveur SSL configurés pour les hôtes du serveur de sécurité, de View Composer et de vCenter Server, vous devez également importer ces certificats racine.

Si les certificats de Serveur de connexion View, du serveur de sécurité, de View Composer et de vCenter Server sont signés par une autorité de certification racine qui est connue et approuvée par l'hôte de Serveur de connexion View, et qu'il n'y a pas de certificat intermédiaire dans vos chaînes de certificats, vous pouvez ignorer cette tâche. Les autorités de certification couramment utilisées sont susceptibles d'être approuvées par l'hôte.

**Remarque** Vous n'avez pas à importer le certificat racine dans les hôtes de View Composer, de vCenter Server ou du serveur de sécurité.

Si un certificat de serveur est signé par une autorité de certification intermédiaire, vous devez également importer chaque certificat intermédiaire dans la chaîne de certificats. Pour simplifier la configuration client, importez la chaîne intermédiaire complète dans les hôtes du serveur de sécurité, de View Composer et de vCenter Server ainsi que les hôtes de Serveur de connexion View. S'il manque des certificats intermédiaires sur un hôte de Serveur de connexion View ou du serveur de sécurité, ils doivent être configurés pour les View Client et les ordinateurs qui lancent View Administrator. S'il manque des certificats intermédiaires sur un hôte de View Composer ou vCenter Server, ils doivent être configurés pour chaque instance de Serveur de connexion View.

Si vous avez déjà vérifié que la chaîne de certificats complète est importée dans le magasin de certificats de l'ordinateur local Windows, vous pouvez ignorer cette tâche.

**Remarque** Si un authentificateur SAML 2.0 est configuré pour être utilisé par une instance de Serveur de connexion View, les mêmes recommandations s'appliquent à l'authentificateur SAML 2.0. Si l'hôte de Serveur de connexion View n'approuve pas le certificat racine configuré pour un authentificateur SAML 2.0, ou si le certificat de serveur SAML 2.0 est signé par une autorité de certification intermédiaire, vous devez vérifier que la chaîne de certificats est importée dans le magasin de certificats de l'ordinateur local Windows.

### Procédure

1 Dans la console MMC sur l'hôte Windows Server, développez le nœud **[Certificats (ordinateur local)]** et allez dans le dossier **[Autorités de certification racine de confiance] > [Certificats]** .

- Si votre certificat racine se trouve dans ce dossier, et qu'il n'y a pas de certificat intermédiaire dans votre chaîne de certificats, passez à l'étape 7.
- Si votre certificat racine ne se trouve pas dans ce dossier, passez à l'étape 2.

2 Cliquez avec le bouton droit sur le dossier **[Autorités de certification racine de confiance] > [Certificats]** et cliquez sur **[Toutes les tâches] > [Importer]** .

3 Dans l'assistant Importation de certificat, cliquez sur **[Suivant]** et allez à l'emplacement de stockage du certificat de l'autorité de certification racine.

4 Sélectionnez le fichier du certificat de l'autorité de certification racine et cliquez sur **[Ouvrir]** .

5 Cliquez sur **[Suivant]** , **[Suivant]** et **[Terminer]** .

6 Si votre certificat de serveur a été signé par une autorité de certification intermédiaire, importez tous les certificats intermédiaires se trouvant dans la chaîne de certificats dans le magasin de certificats de l'ordinateur local Windows.

   a Allez dans le dossier **[Certificats (ordinateur local)] > [Autorités de certification intermédiaires] > [Certificats]** .

   b Répétez les étapes 3 à 6 pour chaque certificat intermédiaire devant être importé.

7 Redémarrez le service Serveur de connexion View, le service du serveur de sécurité, le service View Composer ou le service vCenter Server pour que vos modifications prennent effet.

## Lier un nouveau certificat SSL au port utilisé par View Composer

Si vous configurez un nouveau certificat SSL après l'installation de View Composer, vous devez exécuter l'utilitaire `SviConfig ReplaceCertificate` pour remplacer le certificat qui est lié au port utilisé par View Composer. Cet utilitaire délie le certificat existant et lie le nouveau certificat au port.

Si vous installez le nouveau certificat sur l'ordinateur Windows Server avant d'installer View Composer, il est inutile d'exécuter l'utilitaire `SviConfig ReplaceCertificate`. Lorsque vous exécutez le programme d'installation View Composer, vous pouvez sélectionner un certificat signé par une autorité de certification à la place du certificat autosigné par défaut. Lors de l'installation, le certificat sélectionné est lié au port utilisé par View Composer.

Si vous voulez remplacer un certificat existant ou le certificat autosigné par défaut par un nouveau certificat, vous devez utiliser l'utilitaire `SviConfig ReplaceCertificate`.

### Prérequis

Vérifiez que le nouveau certificat a été importé dans le magasin des certificats de l'ordinateur local Windows sur l'ordinateur Windows Server où View Composer est installé.

### Procédure

1 Redémarrez le service View Composer.

2 Ouvrez une invite de commande sur l'hôte Windows Server où se trouve View Composer.

3 Tapez la commande `SviConfig ReplaceCertificate`.

   Par exemple :

```
sviconfig –operation=ReplaceCertificate
          –delete=false
```

   , où `–delete` est un paramètre obligatoire qui agit sur le certificat à remplacer. Vous devez définir `–delete=true` pour supprimer l'ancien certificat du magasin de certificats de l'ordinateur local Windows ou bien `–delete=false` pour conserver l'ancien certificat dans le magasin des certificats Windows.

   L'utilitaire affiche la liste numérotée des certificats SSL disponibles dans le magasin des certificats de l'ordinateur local Windows.

4 Pour sélectionner un certificat, tapez le numéro du certificat et appuyez sur Entrée.

5 Redémarrez le service View Composer pour appliquer les modifications.

### Exemple : SviConfig ReplaceCertificate

L'exemple suivant remplace le certificat lié au port View Composer :

```
sviconfig –operation=ReplaceCertificate
          –delete=false
```

## Configurer des View Client pour approuver des certificats racine et intermédiaires

Si un certificat de View Server est signé par une autorité de certification qui n'est pas approuvée par des ordinateurs View Client et des ordinateurs client qui accèdent à View Administrator, vous pouvez configurer tous les systèmes client Windows dans un domaine pour approuver les certificats racine et intermédiaires. Pour cela, vous devez ajouter la clé publique du certificat racine à la stratégie de groupe Trusted Root Certification Authorities (Autorités de certification racine de confiance) dans Active Directory et ajouter le certificat racine au magasin Enterprise NTAuth.

Par exemple, vous pouvez avoir à effectuer ces étapes si votre entreprise utilise un service de certificat interne.

Vous n'avez pas à suivre ces étapes si le contrôleur de domaine Windows agit en tant qu'autorité de certification racine ou si vos certificats sont signés par une autorité de certification reconnue. Pour les autorités de certification reconnues, les fournisseurs de système d'exploitation préinstallent le certificat racine sur les systèmes clients.

Si vos certificats de View Server sont signés par une autorité de certification intermédiaire peu connue, vous devez ajouter le certificat intermédiaire à la stratégie de groupe Intermediate Certification Authorities (Autorités de certification intermédiaires) dans Active Directory.

Pour les View Client exécutés sur d'autres systèmes d'exploitation et périphériques, lisez les instructions suivantes sur la distribution des certificats racine et intermédiaires que les utilisateurs peuvent installer :

- Pour View Client pour Mac OS X, reportez-vous à la section « Configurer View Client pour Mac OS X pour autoriser les certificats racine et intermédiaires », page 86.
- Pour View Client pour iPad, reportez-vous à la section « Configurer View Client pour iPad pour autoriser les certificats racine et intermédiaires », page 87.
- Pour View Client pour Android, consultez la documentation sur le site Web de Google, comme *Android 3.0 User's Guide (Guide utilisateur Android 3.0)*.
- Pour View Client pour Linux, consultez la documentation Ubuntu.

### Prérequis

Vérifiez que le certificat de View Server a été généré avec une valeur `KeyLength` de 1 024 ou plus. View Client pour Windows et View Client pour Windows with Local Mode ne valideront pas le certificat sur un View Server qui a été généré avec une valeur `KeyLength` inférieure à 1 024 et les View Client ne pourront pas se connecter à View.

### Procédure

1 Sur votre serveur Active Directory, utilisez la commande `certutil` pour publier le certificat dans le magasin Enterprise NTAuth.

  Par exemple : **`certutil –dspublish –f`** ***`path_to_root_CA_cert`*** **`NTAuthCA`**

2 Sur le serveur Active Directory, naviguez vers le plug-in de gestion de stratégie de groupe.

| Version d'AD | Chemin de navigation |
|---|---|
| **Windows 2003** | a Sélectionnez **[Démarrer] > [Tous les programmes] > [Outils d'administration] > [Utilisateurs et ordinateurs Active Directory]** .<br>b Cliquez avec le bouton droit sur votre domaine et cliquez sur **[Propriétés]** .<br>c Sur l'onglet **[Stratégie de groupe]** , cliquez sur **[Ouvrir]** pour ouvrir le plug-in de Gestion de stratégie de groupe.<br>d Cliquez avec le bouton droit sur **[Stratégie de domaine par défaut]** et cliquez sur **[Modifier]** . |
| **Windows 2008** | a Sélectionnez **[Démarrer] > [Outils d'administration] > [Gestion de stratégie de groupe]** .<br>b Développez votre domaine, cliquez avec le bouton droit sur **[Stratégie de domaine par défaut]** et cliquez sur **[Modifier]** . |

3 Développez la section **[Configuration ordinateur]** et allez à **[Paramètres Windows] > [Paramètres de sécurité] > [Stratégies de clé publique]** .

4 Importez le certificat.

| Option | Description |
|---|---|
| **Certificat racine** | a Cliquez avec le bouton droit sur **[Autorités de certification racine de confiance]** et sélectionnez **[Importer]** .<br>b Suivez les invites de l'assistant pour importer le certificat racine (par exemple, `rootCA.cer`) et cliquez sur **[OK]** . |
| **Certificat intermédiaire** | a Cliquez avec le bouton droit sur **[Autorités de certification intermédiaires]** et sélectionnez **[Importer]** .<br>b Suivez les invites de l'assistant pour importer le certificat intermédiaire (par exemple, `intermediateCA.cer`) et cliquez sur **[OK]** . |

5 Fermez la fenêtre Group Policy (Stratégie de groupe).

Tous les systèmes dans le domaine disposent maintenant d'informations de certificat dans leurs magasins de certificats racine approuvés et leurs magasins de certificats intermédiaires ce qui leur permet d'approuver les certificats racine et intermédiaires.

## Configurer View Client pour Mac OS X pour autoriser les certificats racine et intermédiaires

Si un certificat View server est signé par une autorité de certification (CA) non autorisée par les ordinateurs qui exécutent View Client pour Mac OS X, vous pouvez configurer les ordinateurs pour qu'ils autorisent les certificats racine et intermédiaires. Vous devez distribuer le certificat racine et tous les certificats intermédiaires de la chaîne d'approbation vers les ordinateurs clients.

### Procédure

1 Distribuez le certificat racine et les certificats intermédiaires vers l'ordinateur qui exécute View Client pour Mac OS X.

2 Ouvrez le certificat racine sur l'ordinateur Mac OS X.

Le certificat affiche le message suivant : `Voulez-vous que votre ordinateur autorise les certificats signés par` *`CA name`* `à partir de maintenant ?`

3 Cliquez sur **[Always Trust (Toujours faire confiance)]**

4 Tapez le mot de passe de l'utilisateur.

5 Répétez les étapes 2 à 4 pour tous les certificats intermédiaires de la chaîne d'approbation.

### Configurer View Client pour iPad pour autoriser les certificats racine et intermédiaires

Si un certificat View server est signé par une autorité de certification (CA) non autorisée par les iPads qui exécutent View Client pour iPad, vous pouvez configurer les iPads pour qu'ils autorisent les certificats racine et intermédiaires. Vous devez distribuer le certificat racine et tous les certificats intermédiaires de la chaîne d'approbation vers les iPads.

#### Procédure

1 Envoyez le certificat racine et les certificats intermédiaires dans des pièces jointes aux iPads.

2 Ouvrez la pièce jointe du courrier électronique du certificat racine et sélectionnez **[Install (Installer)]** .

Le certificat affiche le message suivant :

```
Profil invérifiable. L'authenticité de Certificate name ne peut pas être vérifiée.
L'installation de ce profil va modifier les paramètres de l'iPad.

Certificat racine : L'installation du certificat Certificate name va l'ajouter à la liste des
certificats de confiance sur l'iPad.
```

3 Sélectionnez de nouveau **[Install (Installer)]** .

4 Répétez les étapes 2 et 3 pour tous les certificats intermédiaires de la chaîne d'approbation.

## Configuration de la vérification de la révocation des certificats sur des certificats de serveur

Chaque instance de Serveur de connexion View effectue la vérification de la révocation des certificats sur son propre certificat et sur ceux des serveurs de sécurité couplés avec elle. Chaque instance vérifie également les certificats des serveurs vCenter View Composer dès qu'elle établit une connexion avec eux. Par défaut, tous les certificats dans la chaîne sont vérifiés, sauf le certificat racine. Toutefois, vous pouvez modifier cette valeur par défaut.

Si un authentificateur SAML 2.0 est configuré pour être utilisé par une instance de Serveur de connexion View, Serveur de connexion View effectue également la vérification de la révocation des certificats sur le certificat du serveur SAML 2.0.

View prend en charge plusieurs méthodes de vérification de la révocation des certificats, telles que des listes de révocation de certificat (CRL) et le protocole OCSP (Online Certificate Status Protocol). Une CRL est une liste de certificats révoqués publiée par l'autorité de certification qui a émis les certificats. OCSP est un protocole de validation de certificat utilisé pour obtenir l'état de révocation d'un certificat X.509.

Avec des listes de révocation de certificat, la liste de certificats révoqués est téléchargée à partir d'un point de distribution de certificat qui est souvent spécifié dans le certificat. View Server va périodiquement à l'URL du point de distribution de la liste de révocation de certificat spécifiée dans le certificat, télécharge la liste et la vérifie pour déterminer si le certificat de serveur a été révoqué. Avec OCSP, View Server envoie une demande à un répondeur OCSP afin de déterminer l'état de révocation du certificat.

Lorsque vous obtenez un certificat de serveur auprès d'une autorité de certification tierce, le certificat inclut une ou plusieurs méthodes grâce auxquelles son état de révocation peut être déterminé, y compris, par exemple, une URL du point de distribution de la liste de révocation de certificat ou l'URL d'un répondeur OCSP. Si vous avez votre propre autorité de certification et que vous générez un certificat mais n'incluez pas d'informations de révocation dans le certificat, la vérification de la révocation des certificats échoue. Un exemple d'informations de révocation pour un tel certificat peut inclure, par exemple, une URL vers un point de distribution de la liste de révocation de certificat basé sur le Web sur un serveur sur lequel vous hébergez une liste de révocation de certificat.

Si vous avez votre propre autorité de certification mais que vous n'incluez ou ne pouvez pas inclure d'informations de révocation dans votre certificat, vous pouvez choisir de ne pas vérifier les certificats pour révocation ou de vérifier uniquement certains certificats dans une chaîne. Sur View Server, avec l'éditeur de Registre Windows, vous pouvez créer la valeur de chaîne (REG_SZ) **[CertificateRevocationCheckType]**, sous `HKLM\Software\VMware, Inc.\VMware VDM\Security`, et définir cette valeur sur l'une des valeurs de données suivantes.

| Valeur | Description |
|---|---|
| 1 | Ne pas effectuer la vérification de la révocation des certificats. |
| 2 | Vérifier uniquement le certificat de serveur. Ne pas vérifier les autres certificats dans la chaîne. |
| 3 | Vérifier tous les certificats dans la chaîne. |
| 4 | (Valeur par défaut) Vérifier tous les certificats sauf le certificat racine. |

Si cette valeur de Registre n'est pas définie, ou si la valeur définie n'est pas valide (c'est-à-dire si la valeur n'est pas 1, 2, 3 ou 4), tous les certificats sont vérifiés sauf le certificat racine. Définissez cette valeur de Registre sur chaque View Server sur lequel vous prévoyez de modifier la vérification de la révocation. Vous n'avez pas à redémarrer le système après avoir défini cette valeur.

**Remarque** Si votre entreprise utilise des paramètres proxy pour l'accès Internet, vous devez peut-être configurer vos ordinateurs Serveur de connexion View pour qu'ils utilisent les paramètres proxy afin de vérifier que la vérification de la révocation des certificats peut être exécutée pour des serveurs de sécurité ou des instances de Serveur de connexion View qui sont utilisés pour des connexions View Client sécurisées. Si une instance de Serveur de connexion View ne peut pas accéder à Internet, la vérification de la révocation des certificats peut échouer et l'instance de Serveur de connexion View ou les serveurs de sécurité couplés peuvent apparaître en rouge sur le tableau de bord de View Administrator. Pour résoudre ce problème, consultez la section « Résolution de la vérification de la révocation des certificats du serveur de sécurité » dans le document *Administration de VMware Horizon View*.

# Configuration de la vérification de certificat dans View Client pour Windows

Vous pouvez utiliser un paramètre de stratégie de groupe lié à la sécurité dans le fichier de modèle d'administration de configuration de View Client (`vdm_client.adm`) pour configurer la vérification de certificat de serveur SSL dans View Client pour Windows.

La vérification des certificats se produit pour les connexions SSL entre Serveur de connexion View et View Client. La vérification des certificats inclut toutes les vérifications suivantes :

- Le certificat a-t-il été révoqué ? Est-il possible de déterminer si le certificat a été révoqué ?
- Le certificat a-t-il un autre but que de vérifier l'identité de l'expéditeur et de chiffrer les communications du serveur ? Ceci étant, s'agit-il du bon type de certificat ?
- Le certificat a-t-il expiré, ou est-il valide uniquement dans le futur ? Ceci étant, le certificat est-il valide en fonction de l'horloge de l'ordinateur ?
- Le nom commun sur le certificat correspond-il au nom d'hôte du serveur qui l'envoie ? Une incompatibilité peut se produire si un équilibreur de charge redirige View Client vers un serveur avec un certificat qui ne correspond pas au nom d'hôte que l'utilisateur a entré. Une incompatibilité peut également se produire si l'utilisateur entre une adresse IP plutôt qu'un nom d'hôte dans le client.
- Le certificat est-il signé par une autorité de certification inconnue ou non approuvée ? Les certificats auto-signés sont un type d'autorité de certification non approuvée.

  Pour passer cette vérification, la chaîne d'approbation du certificat doit être associée à une racine dans le magasin de certificats local du périphérique.

Lorsque vous configurez pour la première fois un environnement View, un certificat auto-signé par défaut est utilisé. Par défaut, **[Avertir, mais autoriser]** est le mode de vérification de certificat. Dans ce mode, lorsque l'un des problèmes de certificat de serveur suivants se produit, un avertissement s'affiche, mais l'utilisateur peut choisir de continuer et d'ignorer l'avertissement :

- Un certificat auto-signé est fourni par le serveur View. Dans ce cas, il est acceptable si le nom de certificat ne correspond pas au nom de Serveur de connexion View fourni par l'utilisateur dans View Client.
- Un certificat vérifiable qui a été configuré dans votre déploiement a expiré ou n'est pas encore valide.

Vous pouvez modifier le mode de vérification de certificat par défaut. Vous pouvez définir le mode sur **[Pas de sécurité]** , pour qu'aucune vérification de certificat ne soit effectuée, ou vous pouvez définir le mode sur **[Sécurité totale]** , pour que les utilisateurs ne soient pas autorisés à se connecter au serveur si l'une des vérifications échoue. Vous pouvez également autoriser les utilisateurs à définir le mode eux-mêmes.

Utilisez le paramètre de stratégie de groupe `Certificate verification mode` (Mode de vérification du certificat) dans le fichier de modèle d'administration de configuration de View Client pour modifier le mode de vérification. Lorsque ce paramètre de stratégie de groupe est configuré, le paramètre est verrouillé dans View Client. Les utilisateurs peuvent afficher le mode de vérification sélectionné dans View Client, mais ils ne peuvent pas configurer le paramètre. Lorsque ce paramètre de stratégie de groupe n'est pas configuré ou est désactivé, les utilisateurs de View Client peuvent sélectionner un mode de vérification.

Des fichiers de modèle d'administration pour composants View sont installés dans le répertoire *`install_directory`*`\VMware\VMware View\Server\Extras\GroupPolicyFiles` sur votre hôte de Serveur de connexion View. Pour plus d'informations sur l'utilisation de ces modèles afin de contrôler les paramètres de GPO, consultez le document *Administration de VMware Horizon View*.

# Configurer PCoIP Secure Gateway pour utiliser un nouveau certificat SSL

Pour respecter les réglementations de sécurité du secteur ou de la juridiction, vous pouvez remplacer le certificat SSL par défaut généré par le service PCoIP Secure Gateway (PSG) par un certificat signé par une autorité de certification.

Dans View 5.2 ou versions supérieures, le service PSG crée un certificat SSL auto-signé par défaut lors de son démarrage. Le service PSG présente le certificat auto-signé aux clients exécutant View Client 2.0 (ou View Client 5.2 pour Windows) ou versions supérieures qui se connectent à PSG.

PSG fournit également un certificat SSL hérité par défaut qui est présenté aux clients exécutant View Client 1.7 (ou View Client 5.1 pour Windows) ou versions antérieures qui se connectent à PSG.

Les certificats par défaut fournissent des connexions sécurisées entre View Client et PSG et ne requièrent pas de configuration supplémentaire dans View Administrator. Toutefois, la configuration du service PSG pour utiliser un certificat signé par une autorité de certification est fortement recommandée, en particulier pour les déploiements qui nécessitent que vous utilisiez des scanners de sécurité pour passer les tests de conformité.

Même si cela n'est pas requis, il vous est conseillé de configurer les nouveaux certificats SSL signés par une autorité de certification pour vos View Server avant de remplacer le certificat PSG par défaut par un certificat signé par une autorité de certification. Les procédures qui suivent supposent que vous avez déjà importé un certificat signé par une autorité de certification dans le magasin de certificats Windows pour View Server sur lequel est exécuté PSG.

---

**Remarque** Si vous utilisez un scanner de sécurité pour les tests de conformité, vous pouvez commencer en réglant PSG afin qu'il utilise le même certificat que View Server et scanne le port View avant le port PSG. Vous pouvez résoudre les problèmes d'approbation ou de validation se produisant lors du scan du port View pour garantir qu'ils n'invalident pas vos tests du port et du certificat PSG. Ensuite, vous pouvez configurer un certificat unique pour PSG et réaliser un autre scan.

---

### Procédure

1 Vérifier que le nom du serveur correspond au nom de sujet du certificat PSG page 90

Lorsqu'une instance de Serveur de connexion View ou un serveur de sécurité est installé, le programme d'installation crée un paramètre de registre avec une valeur contenant le nom de domaine complet de l'ordinateur. Vous devez vérifier que cette valeur correspond à la partie du nom de serveur de l'URL que les scanners de sécurité utilisent pour atteindre le port PSG. Le nom de serveur doit également correspondre au nom de sujet ou un autre nom de sujet du certificat SSL que vous prévoyez d'utiliser pour PSG.

2 Configurer un certificat PSG dans le magasin de certificats Windows page 91

Pour remplacer le certificat PSG par défaut par un certificat signé par une autorité de certification, vous devez configurer le certificat et sa clé privée dans le magasin de certificats de l'ordinateur local Windows sur l'ordinateur Serveur de connexion View ou du serveur de sécurité sur lequel est exécuté PSG.

3 Définir le nom convivial du certificat PSG dans le registre Windows page 92

PSG identifie le certificat SSL à utiliser au moyen du nom de serveur et du nom convivial du certificat. Vous devez définir la valeur Nom convivial dans le registre Windows sur l'ordinateur Serveur de connexion View ou du serveur de sécurité sur lequel est exécuté PSG.

4 (Facultatif) Forcer l'utilisation d'un certificat signé par une autorité de certification pour les connexions à PSG page 93

Vous pouvez garantir que toutes les connexions View Client à PSG utilisent le certificat signé par une autorité de certification pour PSG au lieu du certificat hérité par défaut. Cette procédure n'est pas requise pour configurer un certificat signé par une autorité de certification pour PSG. Effectuez ces étapes uniquement s'il est utile de forcer l'utilisation d'un certificat signé par une autorité de certification dans votre déploiement de View.

## Vérifier que le nom du serveur correspond au nom de sujet du certificat PSG

Lorsqu'une instance de Serveur de connexion View ou un serveur de sécurité est installé, le programme d'installation crée un paramètre de registre avec une valeur contenant le nom de domaine complet de l'ordinateur. Vous devez vérifier que cette valeur correspond à la partie du nom de serveur de l'URL que les scanners de sécurité utilisent pour atteindre le port PSG. Le nom de serveur doit également correspondre au nom de sujet ou un autre nom de sujet du certificat SSL que vous prévoyez d'utiliser pour PSG.

Par exemple, si un scanner se connecte à PSG avec l'URL `https://view.customer.com:4172`, le paramètre de registre doit avoir la valeur `view.customer.com`. Notez que le nom de domaine complet de l'ordinateur Serveur de connexion View ou du serveur de sécurité défini lors de l'installation peut être différent du nom du serveur externe.

### Procédure

1 Démarrez l'éditeur de Registre Windows sur l'ordinateur Serveur de connexion View ou du serveur de sécurité sur lequel est exécuté PCoIP Secure Gateway.

2 Allez au paramètre de Registre `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway\SSLCertPsgSni`.

3 Vérifiez que la valeur du paramètre `SSLCertPsgSni` correspond au nom de serveur dans l'URL que les scanners utiliseront pour se connecter à PSG et correspond au nom de sujet ou un autre nom de sujet du certificat SSL que vous prévoyez d'installer pour PSG.

Si la valeur ne correspond pas, remplacez-la par la valeur correcte.

4 Redémarrez le service VMware View PCoIP Secure Gateway pour que vos modifications prennent effet.

### Suivant

Importez le certificat signé par une autorité de certification dans le magasin de certificats de l'ordinateur local Windows et configurez le nom convivial du certificat.

## Configurer un certificat PSG dans le magasin de certificats Windows

Pour remplacer le certificat PSG par défaut par un certificat signé par une autorité de certification, vous devez configurer le certificat et sa clé privée dans le magasin de certificats de l'ordinateur local Windows sur l'ordinateur Serveur de connexion View ou du serveur de sécurité sur lequel est exécuté PSG.

Si vous voulez que PSG utilise un certificat unique, vous devez importer le certificat dans le magasin de certificats de l'ordinateur local Windows avec une clé privée exportable et définir le nom convivial approprié.

Si vous voulez que PSG utilise le même certificat que View Server, vous n'avez pas à suivre cette procédure. Toutefois, dans le registre Windows, vous devez définir le nom de serveur afin qu'il corresponde au nom de sujet du certificat de View Server et définir le nom convivial sur **[vdm]** .

### Prérequis

- Vérifiez que la longueur de clé est d'au moins 1 024 bits.
- Vérifiez que le certificat SSL est valide. L'heure actuelle sur l'ordinateur View Server doit être comprise entre les dates de début et de fin du certificat.
- Vérifiez que le nom de sujet du certificat ou un autre nom de sujet correspond au paramètre `SSLCertPsgSni` dans le registre Windows. Reportez-vous à la section « Vérifier que le nom du serveur correspond au nom de sujet du certificat PSG », page 90.
- Vérifiez que le composant logiciel Certificat a été ajouté à MMC. Reportez-vous à la section « Ajouter le composant logiciel enfichable Certificat à MMC », page 81.
- Familiarisez-vous avec l'importation d'un certificat dans le magasin de certificats Windows. Reportez-vous à la section « Importer un certificat de serveur signé dans un magasin de certificats Windows », page 81.
- Familiarisez-vous avec la modification du nom convivial du certificat. Reportez-vous à la section « Modifier le nom convivial d'un certificat », page 82.

### Procédure

1 Dans la fenêtre MMC sur l'hôte Windows Server, ouvrez le dossier **[Certificats (ordinateur local)] > [Personnel]** .

2 Importez le certificat SSL émis pour PSG en sélectionnant **[Autres actions] > [Toutes les tâches] > [Importer]** .

Sélectionnez les paramètres suivants dans l'assistant Importation de certificat :

a **[Marquer cette clé comme exportable]**

b **[Inclure toutes les propriétés extensibles]**

Exécutez l'assistant pour terminer l'importation du certificat dans le dossier **[Personnel]** .

3 Vérifiez que le nouveau certificat contient une clé privée en effectuant l'une de ces étapes :

- Vérifiez qu'une clé jaune apparaît sur l'icône du certificat.
- Double-cliquez sur le certificat et vérifiez que la déclaration suivante apparaît dans la boîte de dialogue Informations sur le certificat : `Vous avez une clé privée qui correspond à ce certificat.`

4 Cliquez avec le bouton droit sur le nouveau certificat et cliquez sur **[Propriétés]** .

5 Sous l'onglet Général, supprimez le texte **[Nom convivial]** et entrez le nom convivial de votre choix.

Assurez-vous d'entrer exactement le même nom dans le paramètre `SSLCertWinCertFriendlyName` dans le registre Windows, comme décrit dans la procédure suivante.

6 Cliquez sur **[Appliquer]** puis sur **[OK]** .

PSG présente le certificat signé par l'autorité de certification aux périphériques View Client qui se connectent à View Server via PCoIP.

---

**Remarque** Cette procédure n'affecte pas les périphériques View Client hérités. PSG continue de présenter le certificat hérité par défaut aux périphériques View Client hérités qui se connectent à View Server via PCoIP.

---

### Suivant

Configurez le nom convivial du certificat dans le registre Windows.

## Définir le nom convivial du certificat PSG dans le registre Windows

PSG identifie le certificat SSL à utiliser au moyen du nom de serveur et du nom convivial du certificat. Vous devez définir la valeur Nom convivial dans le registre Windows sur l'ordinateur Serveur de connexion View ou du serveur de sécurité sur lequel est exécuté PSG.

Le nom convivial du certificat **[vdm]** est utilisé pour toutes les instances de Serveur de connexion View et par tous les serveurs de sécurité. A contrario, vous pouvez configurer votre propre nom convivial de certificat pour le certificat PSG. Vous devez configurer un paramètre de registre Windows pour permettre à PSG de correspondre au nom correct avec le nom convivial que vous allez définir dans le magasin de certificats Windows.

PSG peut utiliser le même certificat SSL que View Server sur lequel est exécuté PSG. Si vous configurez PSG pour qu'il utilise le même certificat que View Server, le nom convivial doit être **[vdm]** .

La valeur Nom convivial, dans le registre et dans le magasin de certificats Windows, est sensible à la casse.

### Prérequis

- Vérifiez que le registre Windows contient le nom de sujet correct utilisé pour atteindre le port PSG et qu'il correspond au nom de sujet du certificat PSG ou un autre nom de sujet. Reportez-vous à la section « Vérifier que le nom du serveur correspond au nom de sujet du certificat PSG », page 90.
- Vérifiez que le nom convivial du certificat est configuré dans le magasin de certificats de l'ordinateur local Windows. Reportez-vous à la section « Configurer un certificat PSG dans le magasin de certificats Windows », page 91.

### Procédure

1 Démarrez l'éditeur de Registre Windows sur l'ordinateur Serveur de connexion View ou du serveur de sécurité sur lequel est exécuté PCoIP Secure Gateway.

2 Allez à la clé de Registre `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway`.

3 Ajoutez une nouvelle valeur de chaîne (REG_SZ), `SSLCertWinCertFriendlyName`, à cette clé de registre.

4 Modifiez la valeur `SSLCertWinCertFriendlyName` et entrez le nom convivial du certificat que PSG doit utiliser.

Par exemple : **[pcoip]**

Si vous utilisez le même certificat que View Server, la valeur doit être **[vdm]** .

5 Redémarrez le service VMware View PCoIP Secure Gateway pour que vos modifications prennent effet.

### Suivant

Vérifiez que les périphériques View Client continuent à se connecter à PSG.

Si vous utilisez un scanner de sécurité pour les tests de conformité, scannez le port PSG.

## (Facultatif) Forcer l'utilisation d'un certificat signé par une autorité de certification pour les connexions à PSG

Vous pouvez garantir que toutes les connexions View Client à PSG utilisent le certificat signé par une autorité de certification pour PSG au lieu du certificat hérité par défaut. Cette procédure n'est pas requise pour configurer un certificat signé par une autorité de certification pour PSG. Effectuez ces étapes uniquement s'il est utile de forcer l'utilisation d'un certificat signé par une autorité de certification dans votre déploiement de View.

Dans certains cas, PSG peut présenter le certificat hérité par défaut au lieu du certificat signé par une autorité de certification à un scanner de sécurité, ce qui invalide le test de conformité sur le port PSG. Pour résoudre ce problème, vous pouvez configurer PSG afin qu'il ne présente le certificat hérité par défaut à aucun périphérique qui tente de se connecter.

---

**Important** L'exécution de cette procédure empêche tous les clients hérités de se connecter à ce View Server via PCoIP.

---

### Prérequis

Vérifiez que tous les périphériques client qui se connectent à ce View Server, y compris les clients légers, exécutent View Client 5.2 pour Windows ou View Client 2.0 ou versions supérieures. Vous devez mettre à niveau les clients hérités.

### Procédure

1 Démarrez l'éditeur de Registre Windows sur l'ordinateur Serveur de connexion View ou du serveur de sécurité sur lequel est exécuté PCoIP Secure Gateway.

2 Allez à la clé de Registre `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway`.

3 Ajoutez une nouvelle valeur de chaîne (REG_SZ), `SSLCertPresentLegacyCertificate`, à cette clé de registre.

4 Définissez la valeur `SSLCertPresentLegacyCertificate` sur **[0]** .

5 Redémarrez le service VMware View PCoIP Secure Gateway pour que vos modifications prennent effet.

# Serveur de transfert View et certificats SSL

Vous n'avez pas à configurer des certificats SSL pour Serveur de transfert View si vous installez View 5.1 ou supérieur.

Un certificat auto-signé par défaut est installé avec Serveur de transfert View que Serveur de connexion View utilise pour gérer les connexions secondaires à des View Client.

Lorsque vous ajoutez Serveur de transfert View à View, Serveur de connexion View établit une relation d'approbation avec Serveur de transfert View. Les communications entre Serveur de connexion View et Serveur de transfert View utilisent JMS (Java Message Service). Les messages contenant des données sensibles sont cryptés.

Lorsqu'un client View demande une opération de transfert des données, qui requiert une connexion à Serveur de transfert View, Serveur de connexion View envoie l'empreinte numérique du certificat de Serveur de transfert View au client. Lorsque le client se connecte au serveur Apache associé à Serveur de transfert View, View Client vérifie que l'empreinte numérique transmise à Serveur de connexion View correspond à l'empreinte numérique de certificat sur le serveur Apache.

Le remplacement du certificat par défaut pour Serveur de transfert View par un certificat signé par une autorité de certification n'affecterait pas significativement les communications sécurisées entre Serveur de transfert View, Serveur de connexion View et les clients View.

Dans View 5.0.*x* et versions antérieures, vous deviez configurer un certificat SSL pour Serveur de transfert View.

Si vous effectuez la mise à niveau de View 5.0.*x* ou antérieur vers View 5.1 ou supérieur, et que vous voulez toujours utiliser un certificat signé par une autorité de certification sur la version mise à niveau de Serveur de transfert View, vous devez sauvegarder le certificat, mettre à niveau Serveur de transfert View et configurer le certificat signé pour la nouvelle version de Serveur de transfert View.

Si vous avez configuré un certificat auto-signé pour l'ancien Serveur de transfert View, ou si vous ne prévoyez pas d'utiliser un certificat signé par une autorité de certification existant sur le serveur mis à niveau, vous n'avez pas à configurer de nouveau un certificat. Lors de la mise à niveau, un certificat auto-signé valide est installé avec Serveur de transfert View.

Pour plus d'informations, consultez le document *Mises à niveau de VMware Horizon View*.

## Configuration de View Administrator pour approuver un certificat de vCenter Server ou View Composer

Dans le tableau de bord de View Administrator, vous pouvez configurer View pour approuver un certificat de vCenter Server ou View Composer qui n'est pas approuvé.

VMware vous recommande vivement de configurer vCenter Server et View Composer afin qu'ils utilisent des certificats SSL signés par une autorité de certification. Vous pouvez également accepter l'empreinte numérique du certificat par défaut pour vCenter Server ou View Composer.

De la même façon, VMware vous conseille de configurer des authentificateurs SAML 2.0 afin qu'ils utilisent des certificats SSL signés par une autorité de certification. Dans le tableau de bord de View Administrator, vous pouvez également configurer View pour qu'il approuve un certificat de serveur SAML 2.0 non approuvé en acceptant l'empreinte numérique du certificat par défaut.

## Avantages des certificats SSL signés par une autorité de certification (CA)

Une autorité de certification est une entité approuvée qui garantit l'identité du certificat et de son créateur. Lorsque le certificat est signé par une autorité de certification approuvée, les utilisateurs ne reçoivent plus de messages leur demandant de vérifier le certificat, et les périphériques de client léger peuvent se connecter sans demander de configuration supplémentaire.

Vous pouvez demander un certificat de serveur SSL spécifique d'un domaine Web, tel que `www.mycorp.com`, ou un certificat de serveur SSL avec caractères génériques pouvant être utilisé dans un domaine, tel que `*.mycorp.com`. Pour simplifier l'administration, vous pouvez choisir de demander un certificat de remplacement si vous avez besoin d'installer le certificat sur plusieurs serveurs ou dans différents sous-domaines. Généralement, des certificats de domaine sont utilisés dans les installations sécurisées et les autorités de certification offrent normalement une meilleure protection contre les pertes pour les certificats de domaine que pour les certificats avec caractères génériques. Si vous utilisez un certificat avec caractères génériques, vous devez vérifier que la clé privée est transférable entre les serveurs.

Lorsque vous remplacez le certificat par défaut par votre propre certificat, les clients utilisent votre certificat pour authentifier le serveur. Si votre certificat est signé par une autorité de certification, le certificat pour l'autorité de certification elle-même est généralement incorporé dans le navigateur ou situé dans une base de données approuvée à laquelle le client peut accéder. Lorsqu'un client accepte le certificat, il répond en envoyant une clé secrète, qui est cryptée avec la clé publique contenue dans le certificat. La clé secrète est utilisée pour crypter le trafic entre le client et le serveur.

# Première configuration de View 8

Après avoir installé le logiciel View server et configuré des certificats SSL pour les serveurs, vous devez exécuter quelques opérations supplémentaires pour configurer l'environnement View.

Vous pouvez configurer des comptes d'utilisateur pour vCenter Server et View Composer, installer une clé de licence View, ajouter vCenter Server et View Composer à l'environnement View, configurer la passerelle sécurisée PCoIP, sécuriser un tunnel et définir éventuellement les paramètres Windows Server pour prendre en charge l'environnement View.

Ce chapitre aborde les rubriques suivantes :



## Configuration de comptes d'utilisateur pour vCenter Server et View Composer

Pour utiliser vCenter Server avec View Manager, vous devez configurer un compte d'utilisateur avec l'autorisation d'effectuer des opérations dans vCenter Server. Pour utiliser View Composer, vous devez accorder à l'utilisateur de vCenter Server ces privilèges supplémentaires. Pour gérer des postes de travail utilisés en mode local, vous devez accorder à cet utilisateur des privilèges en plus de ceux requis pour View Manager et View Composer.

Vous devez également créer un utilisateur de domainr pour View Composer dans Active Directory. Reportez-vous à la section « Créer un compte d'utilisateur pour View Composer », page 23.

### Où utiliser l'utilisateur de vCenter Server et l'utilisateur de domaine pour View Composer

Lorsque vous avez créé et configuré ces deux comptes d'utilisateur, vous spécifiez les noms d'utilisateur dans View Administrator.

- Vous spécifiez un utilisateur de vCenter Server lorsque vous ajoutez vCenter Server à View Manager.
- Vous spécifiez un utilisateur de domaine pour View Composer lorsque vous configurez View Composer pour vCenter Server.
- Vous spécifiez l'utilisateur de domaine pour View Composer lorsque vous créez des pools de clone lié.

## Configurer un utilisateur de vCenter Server pour View Manager, View Composer et le mode local

Pour configurer un compte d'utilisateur qui donne à View Manager l'autorisation de fonctionner sur vCenter Server, vous devez affecter un rôle avec des privilèges appropriés à cet utilisateur. Pour utiliser le service View Composer dans vCenter Server, vous devez accorder au compte d'utilisateur des privilèges supplémentaires. Pour gérer des postes de travail utilisés en mode local, vous devez accorder au compte d'utilisateur des privilèges qui comportent des privilèges de View Manager, de View Composer et de mode local.

Pour prendre en charge View Composer, vous devez également faire de cet utilisateur un administrateur système local sur l'ordinateur vCenter Server.

### Prérequis

- Dans Active Directory, créez un utilisateur dans le domaine de View Connection Server ou un domaine approuvé. Reportez-vous à la section « Création d'un compte d'utilisateur pour vCenter Server », page 23.
- Familiarisez-vous avec les privilèges requis pour le compte d'utilisateur. Reportez-vous à la section « Privilèges de View Manager requis pour l'utilisateur de vCenter Server », page 98.
- Si vous utilisez View Composer, familiarisez-vous avec les privilèges requis supplémentaires. Reportez-vous à la section « Privilèges de View Composer requis pour l'utilisateur de vCenter Server », page 99.
- Si vous gérez des postes de travail locaux, familiarisez-vous avec les privilèges requis supplémentaires. Reportez-vous à la section « Privilèges de mode local requis pour l'utilisateur de vCenter Server », page 99.

### Procédure

1 Dans vCenter Server, préparez un rôle avec les privilèges requis pour l'utilisateur.

   - Vous pouvez utiliser le rôle Administrateur prédéfini dans vCenter Server. Ce rôle peut effectuer toutes les opérations dans vCenter Server.
   - Si vous utilisez View Composer, vous pouvez créer un rôle limité avec les privilèges minimum dont View Manager et View Composer ont besoin pour effectuer des opérations vCenter Server.

     Dans vSphere Client, cliquez sur **[Home (Accueil)] > [Roles (Rôles)] > [Add Role (Ajouter un rôle)]** , saisissez un nom de rôle comme **`View Composer Administrator`** et sélectionnez des privilèges pour le rôle.

     Ce rôle possède tous les privilèges dont View Manager et View Composer ont besoin pour fonctionner dans vCenter Server.
   - Si vous gérez des postes de travail locaux, vous pouvez créer un rôle limité avec les privilèges minimum dont View Manager, View Composer et la fonction de mode local ont besoin pour effectuer des opérations vCenter Server.

Dans vSphere Client, cliquez sur **[Home (Accueil)] > [Roles (Rôles)] > [Add Role (Ajouter un rôle)]**, saisissez un nom de rôle comme **`Local Mode Administrator`** et sélectionnez des privilèges pour le rôle.

Ce rôle possède tous les privilèges dont View Manager, View Composer et la fonction de mode local ont besoin pour fonctionner dans vCenter Server.

- Si vous utilisez View Manager sans View Composer et que vous ne gérez pas de postes de travail locaux, vous pouvez créer un rôle encore plus limité avec les privilèges minimum dont View Manager a besoin pour effectuer des opérations vCenter Server.

  Dans vSphere Client, cliquez sur **[Home (Accueil)] > [Roles (Rôles)] > [Add Role (Ajouter un rôle)]**, saisissez un nom de rôle comme **`View Manager Administrator`** et sélectionnez des privilèges pour le rôle.

2 Dans vSphere Client, cliquez avec le bouton droit sur le serveur vCenter Server dans le niveau supérieur de l'inventaire, cliquez sur **[Add Permission (Ajouter une autorisation)]** et ajoutez l'utilisateur de vCenter Server.

**REMARQUE** Vous devez définir l'utilisateur de vCenter Server au niveau de vCenter Server.

3 Dans le menu déroulant, sélectionnez le rôle Administrateur, ou le rôle View Composer ou View Manager que vous avez créé, et affectez-le à l'utilisateur de vCenter Server.

4 Si vous utilisez View Composer, sur l'ordinateur vCenter Server, ajoutez le compte d'utilisateur de vCenter Server en tant que membre du groupe d'administrateurs système local.

View Composer requiert que l'utilisateur de vCenter Server soit un administrateur système sur l'ordinateur vCenter Server.

### Suivant

Dans View Administrator, lorsque vous ajouter vCenter Server à View Manager, spécifiez l'utilisateur de vCenter Server. Reportez-vous à la section « Ajouter des instances de vCenter Server à View Manager », page 102.

## Privilèges de View Manager requis pour l'utilisateur de vCenter Server

L'utilisateur de vCenter Server doit disposer de privilèges suffisants pour activer View Manager afin qu'il fonctionne dans vCenter Server. Créez un rôle View Manager pour l'utilisateur de vCenter Server avec les privilèges requis.

**Tableau 8-1.** Privilèges de View Manager

| Groupe de privilèges | Privilèges à activer |
|---|---|
| **[Dossier]** | **[Créer un dossier]**<br>**[Supprimer un dossier]** |
| **[Machine virtuelle]** | Dans **[Configuration]** :<br>■ **[Ajouter ou supprimer un périphérique]**<br>■ **[Avancé]**<br>■ **[Modifier des paramètres de périphérique]**<br>Dans **[Interaction]** :<br>■ **[Désactiver]**<br>■ **[Activer]**<br>■ **[Réinitialiser]**<br>■ **[Interrompre]**<br>Dans **[Inventaire]** :<br>■ **[Créer un nouveau]**<br>■ **[Supprimer]**<br>Dans **[Approvisionnement]** :<br>■ **[Personnaliser]**<br>■ **[Déployer un modèle]**<br>■ **[Lire des spécifications de personnalisation]** |
| **[Ressource]** | **[Attribuer une machine virtuelle au pool de ressources]** |
| **[Global]** | **[Agir comme vCenter Server]** |
| | Le privilège **[Hôte]** suivant est requis pour mettre en œuvre View Storage Accelerator, qui active la mise en cache de l'hôte ESXi. Si vous n'utilisez pas View Storage Accelerator, l'utilisateur de vCenter Server n'a pas besoin de ce privilège. |
| **[Hôte]** | Dans **[Configuration]** :<br>■ **[Paramètres avancés]** |

## Privilèges de View Composer requis pour l'utilisateur de vCenter Server

Pour prendre en charge View Composer, l'utilisateur de vCenter Server doit disposer de privilèges en plus de ceux requis pour prendre en charge View Manager. Créez un rôle View Composer pour l'utilisateur de vCenter Server avec les privilèges de View Manager et ces privilèges supplémentaires.

**Tableau 8-2.** Privilèges de View Composer

| Groupe de privilèges | Privilèges à activer |
|---|---|
| **[Magasin de données]** | **[Allouer de l'espace]**<br>**[Parcourir le magasin de données]**<br>**[Opérations de fichier de niveau faible]** |
| **[Machine virtuelle]** | **[Inventaire]** (tous)<br>**[Configuration]** (tous)<br>**[État]** (tous)<br>Dans **[Approvisionnement]** :<br>■ **[Cloner la machine virtuelle]**<br>■ **[Autoriser l'accès au disque]** |
| **[Ressource]** | **[Attribuer une machine virtuelle au pool de ressources]**<br>Le privilège suivant est requis pour exécuter des opérations de rééquilibrage de View Composer.<br>**[Migrer une machine virtuelle désactivée]** |
| **[Global]** | **[Activer des méthodes]**<br>**[Désactiver des méthodes]**<br>**[Balise système]**<br>Le privilège suivant est requis pour mettre en œuvre View Storage Accelerator, qui active la mise en cache de l'hôte ESXi. Si vous n'utilisez pas View Storage Accelerator, l'utilisateur de vCenter Server n'a pas besoin de ce privilège.<br>**[Agir comme vCenter Server]** |
| **[Réseau]** | (tous) |

## Privilèges de mode local requis pour l'utilisateur de vCenter Server

Pour gérer des postes de travail utilisés en mode local, l'utilisateur de vCenter Server doit posséder des privilèges en plus de ceux requis pour prendre en charge View Manager et View Composer. Créez un rôle d'administrateur en mode local pour l'utilisateur de vCenter Server qui combine les privilèges de View Manager, les privilèges de View Composer et les privilèges de mode local.

**Tableau 8-3.** Privilèges de mode local

| Groupe de privilèges | Privilèges à activer |
|---|---|
| **[Global]** | **[Gérer des attributs personnalisés]**<br>**[Définir un attribut personnalisé]** |
| **[Hôte]** | Dans **[Configuration]** :<br>**[Gestion de système]** |

# Première configuration de Serveur de connexion View

Lorsque vous avez installé Serveur de connexion View, vous devez installer une licence produit, ajouter des serveurs vCenter Server et des services View Composer à View Manager. Vous pouvez également autoriser les hôtes ESXi à récupérer l'espace disque sur des machines virtuelles de clone lié et configurer des hôtes ESXi afin de mettre en cache des données de disque de machine virtuelle.

Si vous installez des serveurs de sécurité, ils sont ajoutés à View Manager et apparaissent automatiquement dans View Administrator.

## View Administrator et View Connection Server

View Administrator fournit une interface de gestion pour View Manager.

En fonction de votre déploiement View, vous utilisez une ou plusieurs interfaces de View Administrator.

- Utilisez une interface de View Administrator pour gérer les composants View associés à une instance de View Connection Server autonome ou à un groupe d'instances de View Connection Server répliquées.

  Vous pouvez utiliser l'adresse IP de n'importe quelle instance répliquée pour ouvrir une session sur View Administrator.

- Vous devez utiliser une interface de View Administrator séparée pour gérer les composants View pour chaque instance de View Connection Server autonome ou chaque groupe d'instances de View Connection Server répliquées.

Vous pouvez également utiliser View Administrator pour gérer des serveurs de sécurité et des instances de View Transfer Server associés à View Connection Server.

- Chaque serveur de sécurité est associé à une instance de View Connection Server.
- Chaque instance de View Transfer Server peut communiquer avec n'importe quelle instance de View Connection Server dans un groupe d'instances répliquées.

## Ouvrir une session sur View Administrator

Pour effectuer des tâches de configuration initiale, vous devez ouvrir une session sur View Administrator.

### Prérequis

Vérifiez que vous utilisez un navigateur Web pris en charge par View Administrator. Reportez-vous à la section « Exigences de View Administrator », page 9.

### Procédure

1 Ouvrez votre navigateur Web et saisissez l'URL suivante, où *server* est le nom d'hôte de l'instance de Serveur de connexion View.

```
https://server/admin
```

**Remarque** Vous pouvez utiliser l'adresse IP si vous devez accéder à une instance de Serveur de connexion View lorsque le nom d'hôte n'est pas résolvable. Toutefois, l'hôte que vous contactez ne correspondra pas au certificat SSL configuré pour l'instance de Serveur de connexion View, ce qui se traduit par un accès bloqué ou un accès avec une sécurité réduite.

Votre accès à View Administrator dépend du type de certificat configuré sur l'ordinateur Serveur de connexion View.

| Option | Description |
|---|---|
| **Vous avez configuré un certificat signé par une autorité de certification pour Serveur de connexion View.** | Lorsque vous vous connectez pour la première fois, votre navigateur Web affiche View Administrator. |
| **Le certificat auto-signé par défaut fourni avec Serveur de connexion View est configuré.** | À votre première connexion, votre navigateur Web peut afficher une page vous avertissant que le certificat de sécurité associé à l'adresse n'est pas émis par une autorité de certification approuvée.<br>Cliquez sur **[Ignorer]** pour continuer à utiliser le certificat SSL actuel. |

2 Ouvrez une session en tant qu'utilisateur actuel avec des informations d'identification pour accéder au compte View Administrators.

Vous spécifiez le compte View Administrators lorsque vous installez une instance autonome de Serveur de connexion View ou la première instance de Serveur de connexion View dans un groupe répliqué. Le compte View Administrators peut être le groupe Administrators local (BUILTIN\Administrators) sur l'ordinateur Serveur de connexion View ou un compte d'utilisateur ou de groupe de domaine.

Après avoir ouvert une session sur View Administrator, vous pouvez utiliser **[View Configuration (Configuration de View)] > [Administrators (Administrateurs)]** pour modifier la liste d'utilisateurs et de groupes avec le rôle Administrateurs View.

## Installer la clé de licence de Serveur de connexion View

Avant de pouvoir utiliser Serveur de connexion View, vous devez saisir la clé de licence produit.

Lors de votre première ouverture de session, View Administrator affiche la page Licence produit et utilisation.

Une fois la clé de licence installée, View Administrator affiche la page du tableau de bord lors de l'ouverture de la session.

Vous n'avez pas à configurer une clé de licence lorsque vous installez une instance de Serveur de connexion View répliquée ou un serveur de sécurité. Les instances répliquées et les serveurs de sécurité utilisent la clé de licence commune stockée dans la configuration View LDAP.

**Remarque** Le serveur de connexion View nécessite une clé de licence valide pour View 5.0. À partir de la version de View 4.0, la clé de licence de View est composée de 25 caractères.

### Procédure

1 Si la vue de View Configuration n'est pas affichée, cliquez sur **[Configuration de View]** dans le volet de navigation gauche.

2 Cliquez sur **[Licence produit et utilisation]** .

3 Dans le tableau Licence produit, cliquez sur **[Modifier la licence]** et saisissez le numéro de série de licence de View Manager.

4 Cliquez sur **[OK]** .

5 Vérifiez la date d'expiration de la licence.

## Ajouter des instances de vCenter Server à View Manager

Vous devez configurer View Manager pour vous connecter aux instances de vCenter Server dans votre déploiement de View. vCenter Server crée et gère les machines virtuelles que View Manager utilise en tant que sources de postes de travail.

Si vous exécutez des instances de vCenter Server sur un groupe Mode lié, vous devez ajouter chaque instance de vCenter Server sur View Manager séparément.

View Manager se connecte à l'instance de vCenter Server via un canal sécurisé (SSL).

### Prérequis

- Installez la clé de licence produit de Serveur de connexion View.
- Préparez un utilisateur de vCenter Server avec une autorisation d'effectuer les opérations dans vCenter Server qui sont nécessaires pour prendre en charge View Manager. Pour utiliser View Composer, vous devez accorder à l'utilisateur des privilèges supplémentaires. Pour gérer des postes de travail utilisés en mode local, vous devez accorder à l'utilisateur des privilèges en plus de ceux requis pour View Manager et View Composer.

  Reportez-vous à la section « Configurer un utilisateur de vCenter Server pour View Manager, View Composer et le mode local », page 96.
- Vérifiez qu'un certificat de serveur SSL est installé sur l'hôte de vCenter Server. Dans un environnement de production, installez un certificat SSL valide signé par une autorité de certification approuvée.

  Dans un environnement de test, vous pouvez utiliser le certificat par défaut qui est installé avec vCenter Server, mais vous devez accepter l'empreinte numérique de certificat lorsque vous ajoutez vCenter Server à View.
- Vérifiez que toutes les instances de Serveur de connexion View dans le groupe répliqué approuvent le certificat de l'autorité de certification racine pour le certificat de serveur qui est installé sur l'hôte de vCenter Server. Vérifiez si le certificat de l'autorité de certification racine se trouve dans le dossier **[Autorités de certification racine de confiance] > [Certificats]** dans les magasins de certificats de l'ordinateur local Windows sur les hôtes de Serveur de connexion View. Si ce n'est pas le cas, importez le certificat de l'autorité de certification racine dans les magasins de certificats de l'ordinateur local Windows.

  Consultez la section « Importer un certificat racine et des certificats intermédiaires dans un magasin de certificats Windows » dans le document *Installation de VMware Horizon View*.
- Vérifiez que l'instance de vCenter Server contient des hôtes ESXi. Si aucun hôte n'est configuré dans l'instance de vCenter Server, vous ne pouvez pas ajouter l'instance à View.
- Familiarisez-vous avec les paramètres qui déterminent les limites d'opérations maximales pour vCenter Server et View Composer. Reportez-vous aux sections « Nombre maximal d'opérations simultanées pour vCenter Server et View Composer », page 108 et « Définition d'un taux d'opérations d'alimentation simultanées pour prendre en charge les tempêtes d'ouverture de session des postes de travail View », page 109.

### Procédure

1 Dans View Administrator, cliquez sur **[Configuration de View] > [Serveurs]** .

2 Sous l'onglet vCenter Servers, cliquez sur **[Ajouter]** .

3 Dans la zone de texte de l'adresse du serveur vCenter Server Settings (Paramètres de vCenter Server), saisissez le nom de domaine complet (FQDN) de l'instance de vCenter Server.

Le FQDN inclut le nom d'hôte et le nom de domaine. Par exemple, dans le FQDN ***myserverhost.companydomain.com***, ***myserverhost*** est le nom d'hôte et ***companydomain.com*** le domaine.

**REMARQUE** Si vous saisissez un serveur à l'aide d'un nom DNS ou d'une URL, View Manager n'effectue pas de recherche DNS pour vérifier si un administrateur a précédemment ajouté ce serveur à View Manager à l'aide de son adresse IP. Un conflit se produit si vous ajoutez un serveur vCenter Server avec son nom DNS et son adresse IP.

4 Saisissez le nom de l'utilisateur de vCenter Server.

Par exemple : **domain\user** ou **user@domain.com**

5 Saisissez le mot de passe de l'utilisateur de vCenter Server.

6 (Facultatif) Saisissez une description de cette instance de vCenter Server.

7 Saisissez le numéro du port TCP.

Le port par défaut est 443.

8 Sous Paramètres avancés, définissez les limites d'opérations simultanées pour les opérations de vCenter Server et View Composer.

9 Cliquez sur **[Suivant]** pour afficher la page Paramètres de View Composer.

### Suivant

Configurez les paramètres de View Composer.

- Si l'instance de vCenter Server est configurée avec un certificat SSL signé et si Serveur de connexion View approuve le certificat racine, l'assistant Ajouter un serveur vCenter Server affiche la page Paramètres de View Composer.
- Si l'instance de vCenter Server est configurée avec un certificat par défaut, vous devez d'abord déterminer si vous acceptez l'empreinte numérique du certificat existant. Reportez-vous à la section « Accepter l'empreinte numérique d'un certificat SSL par défaut », page 110.

Si View Manager utilise plusieurs instances de vCenter Server, répétez cette procédure pour ajouter les autres instances de vCenter Server.

## Configurer les paramètres de View Composer

Pour utiliser View Composer, vous devez configurer des paramètres qui permettent à View Manager de se connecter au service View Composer. View Composer peut être installé sur son propre hôte séparé ou sur le même hôte que vCenter Server.

Il doit exister un mappage un-à-un entre chaque service View Composer et instance de vCenter Server. Un service View Composer peut fonctionner avec une seule instance de vCenter Server. Une instance de vCenter Server peut être associée à un seul service View Composer.

### Prérequis

- Votre administrateur Active Directory doit créer un utilisateur de domaine avec une autorisation d'ajouter et de supprimer des machines virtuelles du domaine Active Directory contenant vos clones liés. Pour gérer les comptes de machine de clone lié dans Active Directory, l'utilisateur de domaine doit avoir les autorisations **Créer des objets ordinateur**, **Supprimer des objets ordinateur** et **Écrire toutes les propriétés** .

  Reportez-vous à la section « Créer un compte d'utilisateur pour View Composer », page 23.

- Vérifiez que vous avez configuré View Manager pour vous connecter à vCenter Server. Pour cela, vous devez compléter la page Informations sur vCenter Server de l'assistant Ajouter un serveur vCenter Server. Reportez-vous à la section « Ajouter des instances de vCenter Server à View Manager », page 102.
- Vérifiez que ce service View Composer n'est pas déjà configuré pour se connecter à une instance de vCenter Server différente.

### Procédure

1 Dans View Administrator, complétez la page Informations sur vCenter Server de l'assistant Ajouter un serveur vCenter Server.

   a Cliquez sur **[Configuration de View] > [Serveurs]** .

   b Sous l'onglet vCenter Server, cliquez sur **[Ajouter]** et fournissez les paramètres de vCenter Server.

2 Sur la page Paramètres de View Composer, si vous n'utilisez pas View Composer, sélectionnez **[Ne pas utiliser View Composer]** .

   Si vous sélectionnez **[Ne pas utiliser View Composer]** , les autres paramètres de View Composer deviennent inactifs. Lorsque vous cliquez sur **[Suivant]** , l'assistant Ajouter un serveur vCenter Server affiche la page Paramètres de stockage. La page Domaines View Composer ne s'affiche pas.

3 Si vous utilisez View Composer, sélectionnez l'emplacement de l'hôte de View Composer.

| Option | Description |
|---|---|
| **View Composer est installé sur le même hôte que vCenter Server.** | a Sélectionnez **[View Composer est co-installé avec vCenter Server]** .<br>b Vérifiez que le numéro de port est le même que le port spécifié lors de l'installation du service View Composer sur vCenter Server. Le numéro de port par défaut est 18443. |
| **View Composer est installé sur son propre hôte séparé.** | a Sélectionnez **[Serveur View Composer Server autonome]** .<br>b Dans la zone de texte de l'adresse du serveur View Composer, saisissez le nom de domaine complet (FQDN) de l'hôte de View Composer.<br>c Saisissez le nom de l'utilisateur de View Composer.<br>Par exemple : **`domain.com\user`** ou **`user@domain.com`**<br>d Saisissez le mot de passe de l'utilisateur de View Composer.<br>e Vérifiez que le numéro de port est le même que le port spécifié lors de l'installation du service View Composer. Le numéro de port par défaut est 18443. |

4 Cliquez sur **[Suivant]** pour afficher la page Domaines View Composer.

### Suivant

Configurez les domaines de View Composer.

- Si l'instance de View Composer est configurée avec un certificat SSL signé et si Serveur de connexion View approuve le certificat racine, l'assistant Ajouter un serveur vCenter Server affiche la page Domaines View Composer.
- Si l'instance de View Composer est configurée avec un certificat par défaut, vous devez d'abord déterminer si vous acceptez l'empreinte numérique du certificat existant. Reportez-vous à la section « Accepter l'empreinte numérique d'un certificat SSL par défaut », page 110.

## Configurer les domaines de View Composer

Vous devez configurer un domaine Active Directory dans lequel View Composer déploie des postes de travail de clone lié. Vous pouvez configurer plusieurs domaines pour View Composer. Après avoir ajouté des paramètres de vCenter Server et View Composer à View, vous pouvez ajouter plus de domaines View Composer en modifiant l'instance de vCenter Server dans View Administrator.

### Prérequis

Dans View Administrator, vérifiez que vous avez rempli les pages vCenter Server Information (Informations sur vCenter Server) et View Composer Settings (Paramètres de View Composer) dans l'assistant Add vCenter Server (Ajouter un serveur vCenter Server).

### Procédure

1 Sur la page View Composer Domains (Domaines View Composer), cliquez sur **[Ajouter]** pour ajouter l'utilisateur de domaine aux informations du compte View Composer.

2 Saisissez le nom de domaine du domaine Active Directory.

Par exemple : **`domain.com`**

3 Saisissez le nom de l'utilisateur de domaine, y compris le nom de domaine.

Par exemple : **`domain.com\admin`**

4 Saisissez le mot de passe du compte.

5 Cliquez sur **[OK]** .

6 Pour ajouter des comptes d'utilisateur de domaine avec des privilèges dans d'autres domaines Active Directory dans lesquels vous déployez des pools de clone lié, répétez les étapes précédentes.

7 Cliquez sur **[Suivant]** pour afficher la page Paramètres de stockage.

### Suivant

Activez la récupération d'espace disque de machine virtuelle et configurez View Storage Accelerator pour View.

## Autoriser vSphere à récupérer de l'espace disque dans des machines virtuelles de clone lié

Dans vSphere 5.1 et supérieur, vous pouvez activer la fonction de récupération d'espace disque pour View. À partir de vSphere 5.1, View crée des machines virtuelles de clone lié dans un format de disque efficace qui permet à des hôtes ESXi de récupérer l'espace disque inutilisé dans les clones liés, ce qui réduit l'espace de stockage total requis pour les clones liés.

Comme les utilisateurs interagissent avec des postes de travail de clone lié, les disques du système d'exploitation des clones croissent et peuvent finir par utiliser presque autant d'espace disque que les postes de travail de clone complet. La récupération d'espace disque réduit la taille des disques du système d'exploitation sans que vous ayez à actualiser ou recomposer les clones liés. L'espace peut être récupéré lorsque les machines virtuelles sont activées et que les utilisateurs interagissent avec leurs postes de travail.

La récupération d'espace disque est particulièrement utile pour les déploiements qui ne peuvent pas bénéficier de stratégies d'économie de stockage, telles que l'actualisation à la fermeture de session. Par exemple, les travailleurs du savoir qui installent des applications utilisateur sur des postes de travail dédiés peuvent perdre leurs applications personnelles si les postes de travail ont été actualisés ou recomposés. Avec la récupération d'espace disque, View peut conserver les clones liés proches de la taille réduite avec laquelle ils démarrent lors de leur premier approvisionnement.

Cette fonction comporte deux composants : format de disque à optimisation d'espace et opérations de récupération d'espace.

Dans un environnement vSphere 5.1 ou supérieur, lorsqu'une machine virtuelle parente est la version matérielle virtuelle 9 ou supérieure, View crée des clones liés avec des disques du système d'exploitation à optimisation d'espace, que les opérations de récupération d'espace soient activées ou non.

Pour activer les opérations de récupération d'espace, vous devez utiliser View Administrator afin d'activer la récupération d'espace pour vCenter Server et récupérer l'espace de disque de machine virtuelle pour des pools de postes de travail individuels. Le paramètre de récupération d'espace de vCenter Server vous permet de désactiver cette fonction sur tous les pools de postes de travail qui sont gérés par l'instance de vCenter Server. La désactivation de la fonction pour vCenter Server remplace le paramètre au niveau du pool de postes de travail.

Les recommandations suivantes s'appliquent à la fonction de récupération d'espace :

- Elle fonctionne uniquement sur les disques du système d'exploitation à optimisation d'espace dans des clones liés.
- Il n'affecte pas les disques persistants de View Composer.
- Elle fonctionne uniquement avec vSphere 5.1 ou supérieur et uniquement sur des postes de travail avec la version matérielle virtuelle 9 ou supérieure.
- Elle ne fonctionne pas sur les postes de travail de clone complet.
- Elle fonctionne sur les machines virtuelles avec des contrôleurs SCSI. Les contrôleurs IDE ne sont pas pris en charge.
- Elle fonctionne uniquement sur les postes de travail Windows XP et Windows 7. Elle ne fonctionne pas sur les postes de travail Windows 8.

View Composer Array Integration n'est pas pris en charge dans les pools contenant des machines virtuelles avec des disques à optimisation d'espace. View Composer Array Integration utilise la technologie de snapshot NFS natif VAAI (vStorage APIs for Array Integration) pour cloner des machines virtuelles.

### Prérequis

- Vérifiez que vos hôtes de vCenter Server et ESXi sont à la version 5.1 avec le correctif de téléchargement ESXi 5.1 ESXi510-201212001 ou supérieur.

  Dans un cluster ESXi, vérifiez que tous les hôtes sont à la version 5.1 avec le correctif de téléchargement ESXi510-201212001 ou supérieur.

### Procédure

1 Dans View Administrator, complétez les pages de l'assistant Ajouter un serveur vCenter Server qui précèdent la page Paramètres de stockage.

   a Sélectionnez **[Configuration de View] > [Serveurs]** .

   b Sous l'onglet Serveurs vCenter Server, cliquez sur **[Ajouter]** .

   c Complétez les pages Informations sur vCenter Server, Paramètres de View Composer et Domaines View Composer.

2 Sur la page Paramètres de stockage, vérifiez que **[Activer la récupération d'espace]** est sélectionné.

   La récupération d'espace est sélectionnée par défaut si vous effectuez une nouvelle installation de View 5.2 ou supérieur. Vous devez sélectionner **[Activer la récupération d'espace]** si vous effectuez une mise à niveau vers View 5.2 ou supérieur depuis View 5.1 ou une version antérieure.

### Suivant

Sur la page Paramètres de stockage, configurez View Storage Accelerator.

Pour terminer la configuration de la récupération d'espace disque dans View, configurez la récupération d'espace pour les pools de postes de travail.

## Configurer View Storage Accelerator pour vCenter Server

Dans vSphere 5.0 et supérieur, vous pouvez configurer des hôtes ESXi pour mettre en cache des données de disque de machine virtuelle. Cette fonction, appelée View Storage Accelerator, utilise la fonction CBRC (Content Based Read Cache) dans les hôtes ESXi. View Storage Accelerator améliore les performances de View lors des tempêtes d'E/S, qui peuvent se produire lorsque de nombreux postes de travail démarrent ou exécutent des analyses antivirus simultanément. La fonction est également utile lorsque des administrateurs ou des utilisateurs chargent des applications ou des données fréquemment. Au lieu de lire tout le système d'exploitation ou l'application depuis le système de stockage encore et encore, un hôte peut lire des blocs de données communes depuis le cache.

En réduisant le nombre d'IOPS au cours des tempêtes de démarrage, View Storage Accelerator diminue la demande sur la baie de stockage. Vous pouvez ainsi utiliser moins de bande passante d'E/S de stockage pour prendre en charge votre déploiement de View.

Vous activez la mise en cache sur vos hôtes ESXi en sélectionnant le paramètre View Storage Accelerator dans l'assistant vCenter Server dans View Administrator, comme décrit dans cette procédure.

Vérifiez que View Storage Accelerator est également configuré pour des pools de postes de travail individuels. View Storage Accelerator est activé pour les pools par défaut, mais cette fonction peut être désactivée ou activée lorsque vous créez ou modifiez un pool. Pour fonctionner sur un pool, View Storage Accelerator doit être activé pour vCenter Server et pour le pool individuel.

Vous pouvez activer View Storage Accelerator sur des pools contenant des clones liés et sur des pools contenant des machines virtuelles complètes.

View Storage Accelerator est également pris en charge avec le mode local. Les utilisateurs peuvent emprunter des postes de travail dans des pools activés pour View Storage Accelerator. View Storage Accelerator est désactivé lorsqu'un poste de travail est emprunté et réactivé lorsque le poste de travail est restitué.

View Composer Array Integration n'est pas pris en charge dans les pools qui sont activés pour View Storage Accelerator. View Composer Array Integration utilise la technologie de snapshot NFS natif VAAI (vStorage APIs for Array Integration) pour cloner des machines virtuelles.

View Storage Accelerator est maintenant conçu pour fonctionner dans des configurations qui utilisent la hiérarchisation de réplica View, dans lesquelles des réplicas sont stockés dans un magasin de données séparé des clones liés. Bien que les avantages de performance de l'utilisation de View Storage Accelerator avec la hiérarchisation de réplica View ne soient pas matériellement importants, certains avantages liés à la capacité peuvent être atteints en stockant les réplicas sur un magasin de données séparé. Par conséquent, cette combinaison est testée et prise en charge.

### Prérequis

- Vérifiez que vos hôtes vCenter Server et ESXi sont les versions 5.0 ou supérieures.

  Dans un cluster ESXi, vérifiez que la version de tous les hôtes est la version 5.0 ou supérieure.

- Vérifiez que l'utilisateur de vCenter Server s'est vu affecté le privilège **Général > Agir comme vCenter Server** dans vCenter Server. Consultez les rubriques dans la documentation *Installation de VMware Horizon View* qui décrivent les privilèges de View Manager et de View Composer requis pour l'utilisateur de vCenter Server.

### Procédure

1 Dans View Administrator, complétez les pages de l'assistant Ajouter un serveur vCenter Server qui précèdent la page Paramètres de stockage.

   a Sélectionnez **[Configuration de View]** > **[Serveurs]** .

   b Sous l'onglet Serveurs vCenter Server, cliquez sur **[Ajouter]** .

   c Complétez les pages Informations sur vCenter Server, Paramètres de View Composer et Domaines View Composer

2 Sur la page Paramètres de stockage, vérifiez que la case **[Activer View Storage Accelerator]** est cochée.

   Cette case est cochée par défaut.

3 Spécifiez une taille par défaut pour le cache de l'hôte.

   La taille de cache par défaut s'applique à tous les hôtes ESXi gérés par cette instance de vCenter Server.

   La valeur par défaut est 1 024 Mo. La taille de cache doit être comprise entre 100 Mo et 2 048 Mo.

4 Pour spécifier une taille de cache différente pour un hôte ESXi en particulier, sélectionnez un hôte ESXi et cliquez sur **[Modifier la taille de cache]** .

   a Dans la boîte de dialogue Cache de l'hôte, cochez la case **[Remplacer la taille de cache de l'hôte par défaut]** .

   b Saisissez une valeur **[Taille de cache de l'hôte]** comprise entre 100 Mo et 2 048 Mo et cliquez sur **[OK]** .

5 Sur la page Paramètres de stockage, cliquez sur **[Suivant]** .

6 Cliquez sur **[Terminer]** pour ajouter vCenter Server, View Composer et Paramètres de stockage à View.

### Suivant

Pour configurer PCoIP Secure Gateway, le tunnel sécurisé et des URL externes pour les connexions client, reportez-vous à la section « Configuration de connexions View Client », page 112.

Pour régler les paramètres de View Storage Accelerator dans View, configurez View Storage Accelerator pour des pools de postes de travail. Consultez la section « Configurer View Storage Accelerator pour des pools de postes de travail » dans le document *Administration de VMware Horizon View*.

## Nombre maximal d'opérations simultanées pour vCenter Server et View Composer

Lorsque vous ajoutez vCenter Server à View ou modifiez les paramètres vCenter Server, vous pouvez configurer plusieurs options qui définissent le nombre maximal d'opérations simultanées exécutées par vCenter Server et View Composer.

Vous définissez ces options dans le panneau des paramètres avancés de la page des informations vCenter Server.

**Tableau 8-4.** Nombre maximal d'opérations simultanées pour vCenter Server et View Composer

| Paramètre | Description |
|---|---|
| **[Max concurrent vCenter provisioning operations (Opérations d'approvisionnement de vCenter simultanées max.)]** | Ce paramètre détermine le nombre maximal de demandes simultanées que View Manager peut créer pour approvisionner et supprimer des machines virtuelles complètes dans cette instance de vCenter Server.<br>La valeur par défaut est 20.<br>Le paramètre s'applique uniquement aux machines virtuelles complètes. |
| **[Opérations d'alimentation simultanées max.]** | Ce paramètre détermine le nombre maximal d'opérations d'alimentation (démarrage, arrêt, interruption, etc.) pouvant se dérouler simultanément sur les machines virtuelles gérées par View Manager dans l'instance de vCenter Server.<br>La valeur par défaut est 50.<br>Pour les instructions de calcul d'une valeur pour ce paramètre, voir « Définition d'un taux d'opérations d'alimentation simultanées pour prendre en charge les tempêtes d'ouverture de session des postes de travail View », page 109.<br>Le paramètre s'applique uniquement aux machines virtuelles complètes et aux clones liés. |
| **[Max concurrent View Composer maintenance operations (Nombre max. d'opérations de maintenance View Composer simultanées)]** | Détermine le nombre maximal d'opérations d'actualisation, de recomposition et de rééquilibrage View Composer pouvant se dérouler simultanément sur les clones liés gérés par l'instance de View Composer.<br>La valeur par défaut est 12.<br>Si des sessions sont actives sur des postes de travail, elles doivent être fermées pour qu'une opération de maintenance puisse commencer. Si vous forcez les utilisateurs à fermer les sessions dès qu'une opération de maintenance commence, le nombre maximal d'opérations simultanées sur les postes de travail dont les sessions doivent être fermées est égal à la moitié de la valeur définie. Par exemple, si vous affectez à ce paramètre la valeur 24 et que vous forciez les utilisateurs à fermer leur session, le nombre maximal d'opérations simultanées sur les postes de travail dont les sessions doivent être fermées est égal à 12.<br>Le paramètre ne s'applique qu'aux clones liés. |
| **[Max concurrent View Composer provisioning operations (Nombre max. d'opérations d'approvisionnement View Composer simultanées)]** | Détermine le nombre maximal d'opérations de création et de suppression pouvant se dérouler simultanément sur les clones liés gérés par l'instance de View Composer.<br>La valeur par défaut est 8.<br>Le paramètre ne s'applique qu'aux clones liés. |

## Définition d'un taux d'opérations d'alimentation simultanées pour prendre en charge les tempêtes d'ouverture de session des postes de travail View

Le paramètre **[Opérations d'alimentation simultanées max]** régit le nombre maximal d'opérations d'alimentation simultanées qui se produisent sur des machines virtuelles de poste de travail View dans une instance de vCenter Server. À partir de View 5.0, cette limite est définie sur 50 par défaut. Vous pouvez modifier cette valeur pour prendre en charge les taux maximaux d'activation lorsque de nombreux utilisateurs se connectent à leurs postes de travail en même temps.

Il est recommandé de réaliser une phase pilote afin de déterminer la valeur correcte de ce paramètre. Pour voir des recommandations sur la planification, consultez la section « Recommandations sur la planification et les éléments de conception d'architecture » dans le document *Planification de l'architecture de VMware Horizon View*.

Le nombre requis d'opérations d'alimentation simultanées se base sur le taux maximal auquel les postes de travail sont activés et sur la durée nécessaire au poste de travail pour s'activer, démarrer et devenir disponible pour la connexion. En général, la limite d'opérations d'alimentation recommandée est la durée totale nécessaire au poste de travail pour démarrer multipliée par le taux d'activation maximal.

Par exemple, un poste de travail moyen prend entre deux et trois minutes pour démarrer. Par conséquent, la limite d'opérations d'alimentation simultanées doit être 3 fois le taux d'activation maximal. Le paramètre par défaut de 50 devrait prendre en charge un taux d'activation maximal de 16 postes de travail par minute.

View attend cinq minutes au maximum qu'un poste de travail démarre. Si la durée de démarrage est plus longue, d'autres erreurs peuvent se produire. Pour être classique, vous pouvez définir une limite d'opérations d'alimentation simultanées de 5 fois le taux d'activation maximal. Avec une approche classique, le paramètre par défaut de 50 prend en charge un taux d'activation maximal de 10 postes de travail par minute.

Les ouvertures de session, et donc les opérations d'activation de poste de travail, se produisent en général d'une façon normalement distribuée sur une certaine fenêtre de temps. Vous pouvez estimer le taux d'activation maximal en supposant qu'il se produise au milieu de la fenêtre de temps, quand environ 40 % des opérations d'activation se produisent dans 1/6ème de la fenêtre de temps. Par exemple, si des utilisateurs ouvrent une session entre 8h00 et 9h00, la fenêtre de temps est d'une heure et 40 % des ouvertures de session se produisent dans les 10 minutes entre 8h25 et 8h35. S'il y a 2 000 utilisateurs, dont 20 % ont leurs postes de travail désactivés, alors 40 % des 400 opérations d'activation de poste de travail se produisent dans ces 10 minutes. Le taux d'activation maximal est de 16 postes de travail par minute.

## Accepter l'empreinte numérique d'un certificat SSL par défaut

Lorsque vous ajoutez des instances de vCenter Server et View Composer à Horizon View, vous devez vérifier que les certificats SSL qui sont utilisés pour les instances de vCenter Server et View Composer sont valides et approuvées par Serveur de connexion View. Si les certificats par défaut qui sont installés avec vCenter Server et View Composer sont toujours en place, vous devez choisir d'accepter ou non les empreintes numériques de ces certificats.

Si une instance de vCenter Server ou View Composer est configurée avec un certificat signé par une autorité de certification, et si le certificat racine est approuvé par Serveur de connexion View, vous n'avez pas à accepter l'empreinte numérique de certificat. Aucune action n'est requise.

Si vous remplacez un certificat par défaut par un certificat signé par une autorité de certification, mais que Serveur de connexion View n'approuve pas le certificat racine, vous devez déterminer si vous acceptez l'empreinte numérique de certificat. Une empreinte numérique est un hachage cryptographique d'un certificat. L'empreinte numérique est utilisée pour déterminer rapidement si un certificat présenté est le même qu'un autre certificat, tel que le certificat qui a été accepté précédemment.

**Remarque** Si vous installez vCenter Server et View Composer sur le même hôte Windows Server, ils peuvent utiliser le même certificat SSL, mais vous devez configurer le certificat séparément pour chaque composant.

Pour des détails sur la configuration des certificats SSL, reportez-vous à la section Chapitre 7, « Configuration de certificats SSL pour des View Servers », page 75.

Vous ajoutez d'abord vCenter Server et View Composer dans View Administrator à l'aide de l'assistant Ajouter un serveur vCenter Server. Si un certificat n'est pas approuvé et si vous n'acceptez pas l'empreinte numérique, vous ne pouvez pas ajouter vCenter Server et View Composer.

Une fois que ces serveurs sont ajoutés, vous pouvez les reconfigurer dans la boîte de dialogue Modifier vCenter Server.

**Remarque** Vous devez également accepter une empreinte numérique de certificat lorsque vous effectuez une mise à niveau depuis une version antérieure à Horizon View 5.1 ou supérieur, et lorsqu'un certificat de vCenter Server ou View Composer n'est pas approuvé, ou si vous remplacez un certificat approuvé par un certificat non approuvé.

Sur le tableau de bord de View Administrator, l'icône de vCenter Server ou View Composer devient rouge et la boîte de dialogue Certificat non valide détecté s'affiche. Vous devez cliquer sur **[Vérifier]** et suivre la procédure indiquée ici.

De la même façon, dans View Administrator, vous pouvez configurer un authentificateur SAML 2.0 qu'utilisera une instance de Serveur de connexion View. Si le certificat de serveur SAML 2.0 n'est pas approuvé par Serveur de connexion View, vous devez déterminer si vous acceptez l'empreinte numérique de certificat. Si vous n'acceptez pas l'empreinte numérique, vous ne pouvez pas configurer l'authentificateur SAML 2.0 dans Horizon View. Une fois que l'authentificateur SAML 2.0 est configuré, vous pouvez le reconfigurer dans la boîte de dialogue Modifier Serveur de connexion View.

### Procédure

1 Lorsque View Administrator affiche la boîte de dialogue Certificat non valide détecté, cliquez sur **[Afficher le certificat]** .

2 Examinez l'empreinte numérique de certificat dans la fenêtre Informations sur le certificat.

3 Examinez l'empreinte numérique de certificat qui a été configurée pour l'instance de vCenter Server ou View Composer.

   a Sur l'hôte de vCenter Server ou View Composer, démarrez le composant logiciel MMC et ouvrez le magasin de certificats Windows.

   b Allez au certificat de vCenter Server ou View Composer.

   c Cliquez sur l'onglet Détails du certificat pour afficher l'empreinte numérique de certificat.

   De la même façon, examinez l'empreinte numérique de certificat pour un authentificateur SAML 2.0. Le cas échéant, réalisez les étapes précédentes sur l'hôte d'authentificateur SAML 2.0.

4 Vérifiez que l'empreinte numérique dans la fenêtre Informations sur le certificat correspond à l'empreinte numérique de l'instance de vCenter Server ou View Composer.

   De la même façon, vérifiez que les empreintes numériques correspondent pour un authentificateur SAML 2.0.

5 Déterminez si vous acceptez l'empreinte numérique de certificat.

| Option | Description |
|---|---|
| **Les empreintes numériques correspondent.** | Cliquez sur **[Accepter]** pour utiliser le certificat par défaut. |
| **Les empreintes numériques ne correspondent pas.** | Cliquez sur **[Refuser]** .<br>Corrigez les certificats incompatibles. Par exemple, vous avez peut-être fourni une adresse IP incorrecte pour vCenter Server ou View Composer. |

# Configuration de connexions View Client

Les clients View communiquent avec un hôte de Serveur de connexion View ou du serveur de sécurité sur des connexions sécurisées.

La connexion View Client initiale, utilisée pour l'authentification utilisateur et la sélection de poste de travail View, est créée sur HTTPS lorsqu'un utilisateur fournit un nom de domaine à View Client. Si les logiciels de pare-feu et d'équilibrage de charge ont été configurés correctement dans votre environnement réseau, cette demande atteint l'hôte de Serveur de connexion View ou du serveur de sécurité. Avec cette connexion, les utilisateurs sont authentifiés et un poste de travail est sélectionné, mais les utilisateurs ne sont pas encore connectés à des postes de travail View.

Lorsque des utilisateurs se connectent à des postes de travail View, View Client établit par défaut une deuxième connexion à l'hôte de Serveur de connexion View ou du serveur de sécurité. Cette connexion est appelée connexion par tunnel car elle fournit un tunnel sécurisé pour le transport des données RDP et d'autres données sur HTTPS.

Lorsque des utilisateurs se connectent à des postes de travail View avec le protocole d'affichage PCoIP, View Client peut réaliser une autre connexion à PCoIP Secure Gateway sur l'hôte de Serveur de connexion View ou du serveur de sécurité. Le composant PCoIP Secure Gateway vérifie que seuls des utilisateurs authentifiés peuvent communiquer avec des postes de travail View sur PCoIP.

Lorsque le tunnel sécurisé ou PCoIP Secure Gateway est désactivé, des sessions de postes de travail View sont établies directement entre le système client et la machine virtuelle de poste de travail View, en outrepassant l'hôte de Serveur de connexion View ou du serveur de sécurité. Ce type de connexion est appelé connexion directe.

Les sessions de postes de travail qui utilisent des connexions directes restent connectées même si Serveur de connexion View n'est plus en cours d'exécution.

En général, pour fournir des connexions sécurisées à des clients externes qui se connectent à un hôte du serveur de sécurité ou de Serveur de connexion View sur un réseau WAN, vous activez à la fois le tunnel sécurisé et PCoIP Secure Gateway. Vous pouvez désactiver le tunnel sécurisé et PCoIP Secure Gateway pour autoriser des clients internes connectés sur un réseau LAN à établir des connexions directes sur des postes de travail View.

Certains points de terminaison de View Client, tels que des clients légers, ne prennent pas en charge la connexion par tunnel et utilisent des connexions directes pour les données RDP, mais ils prennent en charge PCoIP Secure Gateway pour les données PCoIP.

Vous pouvez également fournir des connexions sécurisées aux utilisateurs externes qui utilisent HTML Access pour se connecter à des postes de travail View. Blast Secure Gateway, activé par défaut sur les hôtes de Serveur de connexion View et du serveur de sécurité, garantit que seuls les utilisateurs authentifiés peuvent communiquer avec des postes de travail View. Avec HTML Access, le logiciel View Client n'a pas à être installé sur les périphériques de point de terminaison des utilisateurs.

SSL est requis pour toutes les connexions client aux hôtes de Serveur de connexion View et du serveur de sécurité.

## Configurer les connexions via PCoIP Secure Gateway et par tunnel sécurisé

Vous utilisez View Administrator pour configurer l'utilisation du tunnel sécurisé et de PCoIP Secure Gateway. Ces composants garantissent que seuls les utilisateurs authentifiés peuvent communiquer avec des postes de travail View.

Les clients qui utilisent le protocole d'affichage PCoIP peuvent utiliser le composant PCoIP Secure Gateway. Les clients qui utilisent le protocole d'affichage RDP peuvent utiliser le tunnel sécurisé.

**IMPORTANT** Une configuration de réseau classique pouvant fournir des connexions sécurisées à des clients externes inclut un serveur de sécurité. Pour activer ou désactiver le tunnel sécurisé et PCoIP Secure Gateway sur un serveur de sécurité, vous devez modifier l'instance de Serveur de connexion View couplée avec le serveur de sécurité.

Dans une configuration de réseau dans laquelle des clients externes se connectent directement à un hôte de Serveur de connexion View, vous activez ou désactivez le tunnel sécurisé et PCoIP Secure Gateway en modifiant cette instance de Serveur de connexion View dans View Administrator.

### Prérequis

- Si vous prévoyez d'activer le composant PCoIP Secure Gateway, vérifiez que l'instance de Serveur de connexion View et que le serveur de sécurité couplé sont View 4.6 ou supérieur.
- Si vous couplez un serveur de sécurité avec une instance de Serveur de connexion View sur laquelle vous avez déjà activé le composant PCoIP Secure Gateway, vérifiez que le serveur de sécurité est View 4.6 ou supérieur.

### Procédure

1 Dans View Administrator, sélectionnez **[Configuration de View] > [Serveurs]** .

2 Dans le volet Serveur de connexions View, sélectionnez l'instance de Serveur de connexion View et cliquez sur **[Modifier]** .

3 Configurez l'utilisation du tunnel sécurisé.

| Option | Description |
|---|---|
| **Désactiver le tunnel sécurisé** | Décochez la case **[Utiliser une connexion par tunnel sécurisé vers le poste de travail]** . |
| **Activer le tunnel sécurisé** | Cochez la case **[Utiliser une connexion par tunnel sécurisé vers le poste de travail]** . |

Le tunnel sécurisé est activé par défaut.

4 Configurez l'utilisation de PCoIP Secure Gateway.

| Option | Description |
|---|---|
| **Activer PCoIP Secure Gateway** | Cochez la case **[Utiliser des connexions PCoIP Secure Gateway pour PCoIP vers le poste de travail]** . |
| **Désactiver PCoIP Secure Gateway** | Décochez la case **[Utiliser des connexions PCoIP Secure Gateway pour PCoIP vers le poste de travail]** . |

PCoIP Secure Gateway est désactivé par défaut.

5 Cliquez sur **[OK]** pour enregistrer vos modifications.

## Configurer un accès HTML sécurisé

Dans View Administrator, vous pouvez configurer l'utilisation de Blast Secure Gateway afin de fournir un accès HTML sécurisé à des postes de travail View.

Blast Secure Gateway vérifie que seuls des utilisateurs authentifiés peuvent communiquer avec des postes de travail View à l'aide d'HTML Access. View Client n'a pas à être installé sur les périphériques de point de terminaison des utilisateurs.

Lorsque Blast Secure Gateway n'est pas activé, les navigateurs Web clients utilisent HTML Access pour établir des connexions directes avec des machines virtuelles de poste de travail View, en outrepassant Blast Secure Gateway.

**IMPORTANT** Une configuration de réseau classique pouvant fournir des connexions sécurisées à des utilisateurs externes inclut un serveur de sécurité. Pour activer ou désactiver Blast Secure Gateway sur un serveur de sécurité, vous devez modifier l'instance de Serveur de connexion View couplée avec le serveur de sécurité. Si des utilisateurs externes se connectent directement à un hôte de Serveur de connexion View, vous activez ou désactivez Blast Secure Gateway en modifiant cette instance de Serveur de connexion View.

### Prérequis

- Si des utilisateurs sélectionnent des postes de travail View à l'aide d'Horizon User Portal, vérifiez qu'Horizon Workspace est installé et configuré pour être utilisé avec Serveur de connexion View et que Serveur de connexion View est couplé avec un serveur d'authentification SAML 2.0.
- Vérifiez que le tunnel sécurisé est activé. S'il est désactivé, Blast Secure Gateway ne peut pas être activé.

### Procédure

1 Dans View Administrator, sélectionnez **[Configuration de View] > [Serveurs]** .

2 Dans le volet Serveur de connexions View, sélectionnez l'instance de Serveur de connexion View et cliquez sur **[Modifier]** .

3 Configurez l'utilisation de Blast Secure Gateway.

| Option | Description |
|---|---|
| **Activer Blast Secure Gateway** | Cochez la case **[Utiliser Blast Secure Gateway pour un accès HTML au poste de travail]** |
| **Désactiver Blast Secure Gateway** | Décochez la case **[Utiliser Blast Secure Gateway pour un accès HTML au poste de travail]** |

Blast Secure Gateway est activé par défaut.

4 Cliquez sur **[OK]** pour enregistrer vos modifications.

## Ouvrir le port utilisé par HTML Access sur des serveurs de sécurité

Lorsque vous installez Serveur de connexion View ou un serveur de sécurité, le programme d'installation de View Server crée la règle de Pare-feu Windows pour le port utilisé par HTML Access pour les connexions client, mais il laisse la règle désactivée tant qu'elle n'est pas réellement nécessaire. Lorsque vous installez ultérieurement HTML Access sur une instance de Serveur de connexion View, le programme d'installation HTML Access active automatiquement la règle pour autoriser la communication avec ce port. Toutefois, sur les serveurs de sécurité, vous devez activer manuellement la règle dans le Pare-feu Windows pour autoriser la communication avec le port.

Par défaut, HTML Access utilise le port TCP 8443 pour les connexions client avec Blast Secure Gateway.

**Procédure**

- Pour ouvrir le port utilisé par HTML Access sur un ordinateur Serveur de connexion View, installez HTML Access sur cet ordinateur.

  Le programme d'installation HTML Access active la règle **[Serveur de connexion VMware View (Blast-In)]** dans le Pare-feu Windows.

- Pour ouvrir le port pour HTML Access sur un serveur de sécurité, activez manuellement la règle **[Serveur de connexion VMware View (Blast-In)]** dans le Pare-feu Windows.

## Configuration d'URL externes pour PCoIP Secure Gateway et les connexions par tunnel

Pour utiliser le tunnel sécurisé, un système client doit avoir accès à une adresse IP (ou à un nom de domaine complet (FQDN) qu'il peut résoudre en adresse IP) qui permet au client d'atteindre un hôte de Serveur de connexion View ou du serveur de sécurité.

Pour utiliser PCoIP Secure Gateway, un système client doit avoir accès à une adresse IP qui permet au client d'atteindre un hôte de Serveur de connexion View ou du serveur de sécurité.

Pour utiliser Blast Secure Gateway, le périphérique de point de terminaison d'un utilisateur doit avoir accès à un nom de domaine complet qu'il peut résoudre en adresse IP qui permet au navigateur Web de l'utilisateur d'atteindre un hôte de Serveur de connexion View ou du serveur de sécurité.

### Utilisation de connexions par tunnel à partir de sites externes

Par défaut, un hôte de Serveur de connexion View ou d'un serveur de sécurité ne peut être contacté que par des clients tunnel qui résident sur le même réseau et qui peuvent donc localiser l'hôte demandé.

De nombreuses entreprises veulent que les utilisateurs puissent se connecter à partir d'un site externe en utilisant une adresse IP ou un nom de domaine résolvable par le client spécifique, et un port spécifique. Ces informations peuvent ou pas ressembler à l'adresse et au numéro de port réels de l'hôte de Serveur de connexion View ou du serveur de sécurité. Les informations sont fournies à un système client sous forme d'URL. Par exemple :

- `https://view_exemple.com:443`
- `https://view.exemple.com:443`
- `https://exemple.com:1234`
- `https://10.20.30.40:443`

Pour utiliser des adresses comme celles-ci dans View Manager, vous devez configurer l'hôte de Serveur de connexion View ou du serveur de sécurité pour renvoyer une URL externe au lieu d'un FQDN de l'hôte.

### Configuration d'URL externes

Vous configurez plusieurs URL externes. La première URL permet aux systèmes client de faire des connexions par tunnel. Une deuxième URL permet aux systèmes client qui utilisent PCoIP de réaliser des connexions sécurisées via PCoIP Secure Gateway. Vous devez spécifier l'URL externe PCoIP comme adresse IP, ce qui permet aux systèmes client de se connecter à partir d'un site externe.

Une troisième URL permet aux utilisateurs de faire des connexions sécurisées depuis leurs navigateurs Web via Blast Secure Gateway.

Si votre configuration de réseau inclut des serveurs de sécurité, fournissez des URL externes aux serveurs de sécurité. Les URL externes ne sont pas requises sur les instances de Serveur de connexion View couplées avec les serveurs de sécurité.

Le processus de configuration des URL externes est différent pour des instances de Serveur de connexion View et des serveurs de sécurité.

- Pour une instance de Serveur de connexion View, vous définissez les URL externes en modifiant des paramètres de Serveur de connexion View dans View Administrator.
- Pour un serveur de sécurité, vous définissez les URL externes lorsque vous exécutez le programme d'installation de Serveur de connexion View. Vous pouvez utiliser View Administrator pour modifier une URL externe d'un serveur de sécurité.

## Définir les URL externes d'une instance de Serveur de connexion View

Vous utilisez View Administrator pour configurer les URL externes d'une instance de Serveur de connexion View.

L'URL externe de tunnel sécurisé et l'URL externe PCoIP doivent être les adresses que les systèmes client utilisent pour atteindre cette instance de Serveur de connexion View. Par exemple, ne spécifiez pas l'URL externe de tunnel sécurisé pour cette instance et l'URL externe PCoIP pour un serveur de sécurité couplé.

De la même façon, l'URL externe de tunnel sécurisé et l'URL externe Blast doivent être les adresses que les connexions HTML utilisent pour atteindre cette instance de Serveur de connexion View. Par exemple, ne spécifiez pas l'URL externe de tunnel sécurisé pour cette instance et l'URL externe Blast pour un serveur de sécurité couplé.

### Prérequis

- Vérifiez que les connexions par tunnel sécurisé et PCoIP Secure Gateway sont activés sur l'instance de Serveur de connexion View. Reportez-vous à la section « Configurer les connexions via PCoIP Secure Gateway et par tunnel sécurisé », page 113.
- Pour définir l'URL externe Blast, vérifiez que Blast Secure Gateway est activé sur l'instance de Serveur de connexion View. Reportez-vous à la section « Configurer un accès HTML sécurisé », page 114.

### Procédure

1 Dans View Administrator, cliquez sur **[Configuration de View] > [Serveurs]** .

2 Sous l'onglet Serveurs de connexion, sélectionnez une instance de Serveur de connexion View et cliquez sur **[Modifier]** .

3 Saisissez l'URL externe du tunnel sécurisé dans la zone de texte **[URL externe]** .

L'URL doit contenir le protocole, le nom d'hôte résolvable par le client et le numéro de port.

Par exemple : `https://myserver.example.com:443`

---

**Remarque** Vous pouvez utiliser l'adresse IP si vous devez accéder à une instance de Serveur de connexion View lorsque le nom d'hôte n'est pas résolvable. Toutefois, l'hôte que vous contactez ne correspondra pas au certificat SSL configuré pour l'instance de Serveur de connexion View, ce qui se traduit par un accès bloqué ou un accès avec une sécurité réduite.

---

4 Saisissez l'URL externe de PCoIP Secure Gateway dans la zone de texte **[URL externe PCoIP]** .

Spécifiez l'URL externe PCoIP comme adresse IP avec le numéro de port 4172. N'incluez pas un nom de protocole.

Par exemple : `10.20.30.40:4172`

L'URL doit contenir l'adresse IP et le numéro de port qu'un système client peut utiliser pour atteindre cet hôte de Serveur de connexion View. Vous ne pouvez saisir du texte dans la zone de texte que si PCoIP Secure Gateway est installé sur l'instance de Serveur de connexion View.

5 Saisissez l'URL externe Blast Secure Gateway dans la zone de texte **[URL externe Blast]** .

L'URL doit contenir le protocole HTTPS, le nom d'hôte résolvable par le client et le numéro de port.

Par exemple : `https://myserver.example.com:8443`

Par défaut, l'URL inclut le nom de domaine complet de l'URL externe du tunnel sécurisé et le numéro de port par défaut, 8443. L'URL doit contenir le nom de domaine complet et le numéro de port qu'un système client peut utiliser pour atteindre cet hôte de Serveur de connexion View. Vous ne pouvez saisir du texte dans la zone de texte que si Blast Secure Gateway est installé sur l'instance de Serveur de connexion View.

6 Cliquez sur **[OK]** .

## Modifier les URL externes d'un serveur de sécurité

Vous utilisez View Administrator pour modifier les URL externes d'un serveur de sécurité.

Vous configurez pour la première fois ces URL externes lorsque vous installez un serveur de sécurité dans le programme d'installation de Serveur de connexion View.

L'URL externe de tunnel sécurisé, l'URL externe PCoIP et l'URL externe Blast doivent être les adresses que les systèmes client utilisent pour atteindre ce serveur de sécurité. Par exemple, ne spécifiez pas l'URL externe de tunnel sécurisé pour ce serveur de sécurité et l'URL externe PCoIP pour une instance couplée de Serveur de connexion View.

### Prérequis

- Pour un accès sécurisé à des postes de travail View sur PCoIP, vérifiez que la version du serveur de sécurité est View 4.6 ou supérieur.
- Pour un accès HTML sécurisé à des postes de travail View, vérifiez que la version du serveur de sécurité est View 5.2 ou supérieur.
- Vérifiez que les connexions par tunnel sécurisé et PCoIP Secure Gateway sont activés sur l'instance de Serveur de connexion View qui est couplée avec ce serveur de sécurité. Reportez-vous à la section « Configurer les connexions via PCoIP Secure Gateway et par tunnel sécurisé », page 113.
- Pour définir l'URL externe Blast, vérifiez que Blast Secure Gateway est activé sur l'instance de Serveur de connexion View qui est couplée avec ce serveur de sécurité. Reportez-vous à la section « Configurer un accès HTML sécurisé », page 114.

### Procédure

1 Dans View Administrator, sélectionnez **[Configuration de View] > [Serveurs]** .

2 Sélectionnez l'onglet Serveurs de sécurité, sélectionnez le serveur de sécurité et cliquez sur **[Modifier]** .

Le bouton **[Modifier]** est indisponible si le serveur de sécurité n'est pas mis à niveau vers Serveur de connexion View 4.6 ou supérieur.

3 Saisissez l'URL externe du tunnel sécurisé dans la zone de texte **[URL externe]** .

L'URL doit contenir le protocole, le nom d'hôte de serveur de sécurité résolvable par le client et le numéro de port.

Par exemple : `https://view.exemple.com:443`

---

**Remarque** Vous pouvez utiliser l'adresse IP si vous devez accéder à un serveur de sécurité lorsque le nom d'hôte n'est pas résolvable. Toutefois, l'hôte que vous contactez ne correspondra pas au certificat SSL configuré pour le serveur de sécurité, ce qui se traduit par un accès bloqué ou un accès avec une sécurité réduite.

---

4 Saisissez l'URL externe de PCoIP Secure Gateway dans la zone de texte **[URL externe PCoIP]** .

Spécifiez l'URL externe PCoIP comme adresse IP avec le numéro de port 4172. N'incluez pas un nom de protocole.

Par exemple : `10.20.30.40:4172`

L'URL doit contenir l'adresse IP et le numéro de port qu'un système client peut utiliser pour atteindre ce serveur de sécurité. Vous ne pouvez saisir du texte dans la zone de texte que si PCoIP Secure Gateway est installé sur le serveur de sécurité.

5 Saisissez l'URL externe Blast Secure Gateway dans la zone de texte **[URL externe Blast]** .

L'URL doit contenir le protocole HTTPS, le nom d'hôte résolvable par le client et le numéro de port.

Par exemple : `https://myserver.example.com:8443`

Par défaut, l'URL inclut le nom de domaine complet de l'URL externe du tunnel sécurisé et le numéro de port par défaut, 8443. L'URL doit contenir le nom de domaine complet et le numéro de port qu'un système client peut utiliser pour atteindre ce serveur de sécurité. Vous ne pouvez saisir du texte dans la zone de texte que si Blast Secure Gateway est installé sur le serveur de sécurité.

6 Cliquez sur **[OK]** pour enregistrer vos modifications.

View Administrator envoie les URL externes mises à jour au serveur de sécurité. Vous n'avez pas à redémarrer le service du serveur de sécurité pour que les modifications prennent effet.

# Remplacement des ports par défaut pour les services View

Lors de l'installation, les services View sont configurés pour écouter sur certains ports réseau par défaut. Dans certaines entreprises, ces ports doivent être modifiés pour respecter les stratégies d'entreprise ou pour éviter la contention. Vous pouvez modifier les ports par défaut qui sont utilisés par les services Serveur de connexion View, le serveur de sécurité, PCoIP Secure Gateway, View Composer et Serveur de transfert View.

La modification des ports est une tâche de configuration facultative. Utilisez les ports par défaut si votre déploiement ne requiert pas que vous les modifiiez.

Pour voir une liste des ports TCP et UDP par défaut utilisés par des serveurs View Server, consultez la section « Ports TCP et UDP de View » dans le document *Sécurité de VMware Horizon View*.

## Remplacer les ports HTTP ou les cartes réseau par défaut pour des instances de Serveur de connexion View et des serveurs de sécurité

Vous pouvez remplacer les ports HTTP ou les cartes réseau par défaut pour une instance de Serveur de connexion View ou un serveur de sécurité en modifiant le fichier `locked.properties` sur l'ordinateur de View Server. Votre entreprise peut vous demander d'effectuer ces étapes pour respecter les stratégies d'entreprise ou pour éviter la contention.

Le port SSL par défaut est 443. Le port non-SSL par défaut est 80.

Le port spécifié dans l'URL externe de tunnel sécurisé ne change pas suite aux modifications que vous apportez aux ports dans cette procédure. En fonction de votre configuration de réseau, vous devrez peut-être changer le port de l'URL externe de tunnel sécurisé également.

Si l'ordinateur de View Server contient plusieurs cartes réseau, il écoute sur toutes les cartes réseau par défaut. Vous pouvez sélectionner une carte réseau pour écouter sur le port configuré en spécifiant l'adresse IP qui est liée à cette carte réseau.

Lors de l'installation, View configure le pare-feu Windows pour qu'il ouvre les ports par défaut requis. Si vous modifiez un numéro de port ou la carte réseau sur lequel il écoute, vous devez reconfigurer manuellement votre pare-feu Windows pour ouvrir les ports mis à jour afin que les périphériques View Client puissent se connecter à View Server.

### Prérequis

Vérifiez que le port spécifié dans l'URL externe pour cette instance de Serveur de connexion View ou ce serveur de sécurité sera toujours valide une fois que vous aurez changé les ports dans cette procédure.

### Procédure

1 Créez ou modifiez le fichier `locked.properties` dans le dossier de configuration de la passerelle SSL sur l'ordinateur Serveur de connexion View ou du serveur de sécurité.

Par exemple : *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

Les propriétés dans le fichier `locked.properties` sont sensibles à la casse.

2 Ajoutez la propriété `serverPort` ou `serverPortNonSsl`, ou les deux, au fichier `locked.properties`.

Par exemple :

```
serverPort=4443
serverPortNonSsl=8080
```

3 (Facultatif) Si l'ordinateur de View Server contient plusieurs cartes réseau, sélectionnez une carte réseau pour écouter sur les ports configurés.

Ajoutez les propriétés `serverHost` et `serverHostNonSsl` pour spécifier l'adresse IP qui est liée à la carte réseau désignée.

Par exemple :

```
serverHost=10.20.30.40
serverHostNonSsl=10.20.30.40
```

En général, les écouteurs SSL et non-SSL sont configurés pour utiliser la même carte réseau. Toutefois, si vous utilisez la propriété `serverProtocol=http` pour décharger SSL pour des connexions client, vous pouvez définir la propriété `serverHost` sur une carte réseau séparée afin de fournir des connexions SSL à des systèmes utilisés pour lancer View Administrator.

Si vous configurez des connexions SSL et non-SSL pour qu'elles utilisent la même carte réseau, les ports SSL et non-SSL doivent être différents.

4 Redémarrez le service Serveur de connexion View ou le service du serveur de sécurité pour que vos modifications prennent effet.

### Suivant

Si nécessaire, configurez manuellement votre pare-feu Windows pour ouvrir les ports mis à jour.

## Remplacer les ports ou les cartes réseau par défaut pour PCoIP Secure Gateway sur des instances de Serveur de connexion View et des serveurs de sécurité

Vous pouvez remplacer les ports ou les cartes réseau par défaut utilisés par un service PCoIP Secure Gateway exécuté sur une instance de Serveur de connexion View ou un serveur de sécurité. Votre entreprise peut vous demander d'effectuer ces étapes pour respecter les stratégies d'entreprise ou pour éviter la contention.

Pour les connexions TCP et UDP client, PCoIP Secure Gateway écoute sur le port 4172 par défaut. Pour les connexions UDP vers des postes de travail View, PCoIP Secure Gateway écoute sur le port 55000 par défaut.

Le port spécifié dans l'URL externe PCoIP ne change pas suite aux modifications que vous apportez aux ports dans cette procédure. En fonction de votre configuration de réseau, vous devrez peut-être changer le port de l'URL externe PCoIP également.

Si l'ordinateur sur lequel PCoIP Secure Gateway est exécuté contient plusieurs cartes réseau, il écoute sur toutes les cartes réseau par défaut. Vous pouvez sélectionner une carte réseau pour écouter sur les ports configurés en spécifiant l'adresse IP qui est liée à cette carte réseau.

### Prérequis

Vérifiez que le port spécifié dans l'URL externe PCoIP sur l'instance de Serveur de connexion View ou le serveur de sécurité sera toujours valide une fois que vous aurez changé les ports dans cette procédure.

### Procédure

1 Démarrez l'éditeur de Registre Windows sur l'ordinateur Serveur de connexion View ou du serveur de sécurité sur lequel est exécuté PCoIP Secure Gateway.

2 Allez à la clé de Registre `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway`.

3 Sous cette clé de Registre, ajoutez une ou plusieurs des valeurs de chaîne suivantes (`REG_SZ`) avec vos numéros de port mis à jour.

   Par exemple :

   ```
   ExternalTCPPort "44172"
   ExternalUDPPort "44172"
   InternalUDPPort "55111"
   ```

4 (Facultatif) Si l'ordinateur sur lequel PCoIP Secure Gateway est exécuté contient plusieurs cartes réseau, sélectionnez une carte réseau pour écouter sur les ports configurés.

   Sous la même clé de Registre, ajoutez les valeurs de chaîne suivantes (`REG_SZ`) pour spécifier l'adresse IP qui est liée à la carte réseau désignée.

   Par exemple :

   ```
   ExternalBindIP "10.20.30.40"
   InternalBindIP "172.16.17.18"
   ```

   Si vous configurez des connexions externes et internes pour qu'elles utilisent la même carte réseau, les ports UDP externes et internes doivent être différents.

5 Redémarrez le service VMware View PCoIP Secure Gateway pour que vos modifications prennent effet.

## Remplacer le port par défaut pour View Composer

Le certificat SSL utilisé par le service View Composer est lié à un certain port par défaut. Vous pouvez remplacer le port par défaut à l'aide de l'utilitaire `SviConfig ChangeCertificateBindingPort`.

Lorsque vous spécifiez un nouveau port avec l'utilitaire `SviConfig ChangeCertificateBindingPort`, l'utilitaire annule la liaison entre le certificat View Composer et le port actuel et le lie au nouveau port.

Lors de l'installation, View Composer configure le pare-feu Windows pour qu'il ouvre le port par défaut requis. Si vous modifiez le port, vous devez reconfigurer manuellement votre pare-feu Windows pour ouvrir le port mis à jour et assurer la connectivité avec le service View Composer.

### Prérequis

Vérifiez que le port que vous spécifiez est disponible.

### Procédure

1 Arrêtez le service View Composer.

2 Ouvrez une invite de commande sur l'hôte Windows Server sur lequel est installé View Composer.

3 Tapez la commande `SviConfig ChangeCertificateBindingPort`.

Par exemple :

```
sviconfig –operation=ChangeCertificateBindingPort
          –Port=port number
```

où `–port=port number` est le nouveau port auquel View Composer lie le certificat. Le paramètre `–port=port number` est requis.

4 Redémarrez le service View Composer pour que vos modifications prennent effet.

### Suivant

Si nécessaire, reconfigurez manuellement le pare-feu Windows sur le serveur View Composer pour ouvrir le port mis à jour.

## Remplacer les ports par défaut pour Serveur de transfert View

Par défaut, le serveur Web Apache installé avec Serveur de transfert View écoute sur le port 80 ou, si SSL est utilisé, le port 443. Vous pouvez modifier les ports par défaut en modifiant les fichiers de configuration du serveur Web Apache.

Le port HTTP par défaut est 80. Vous modifiez le port HTTP en modifiant le fichier `httpd.conf` sur l'ordinateur Serveur de transfert View.

Le port HTTPS par défaut est 443. Vous modifiez le port HTTPS en modifiant le fichier `mod_vprov.conf` sur l'ordinateur Serveur de transfert View.

Lors de l'installation, View configure le Pare-feu Windows pour ouvrir les ports utilisés par Serveur de transfert View par défaut. Si vous modifiez les ports, vous devez reconfigurer manuellement votre Pare-feu Windows pour qu'il ouvre les ports mis à jour afin que les périphériques View Client puissent se connecter à l'instance de Serveur de transfert View.

### Procédure

1 Arrêtez le service Serveur de transfert VMware View.

2 Sur l'ordinateur Serveur de transfert View, accédez au répertoire *install_directory*`\VMware\VMware View\Server\httpd\conf`.

Les fichiers `httpd.conf` et `mod_vprov.conf` se trouvent dans ce répertoire.

3 Modifiez le port HTTP.

a Ouvrez le fichier `httpd.conf`.

b Mettez à jour la valeur `Listen`.

Par exemple : **[Listen 4080]**

c Enregistrez le fichier `httpd.conf`.

4 Modifiez le port HTTPS.

a Ouvrez le fichier `mod_vprov.conf`.

b Mettez à jour la valeur `Listen`.

Par exemple : **[Listen 4443]**

c Mettez à jour l'entrée `Virtual Host`.

Par exemple, mettez à jour l'entrée comme suit :

```
# Configure SSL
<VirtualHost_default_:4443>
  SSLEngine on
  SSLCertificateFile ./conf/server.crt
  SSLCertificateKeyFile ./conf/server.key

  <Location /vprov>
    SetHandler vprov
  </Location>
</VirtualHost>
```

d Enregistrez le fichier `mod_vprov.conf`.

5 Redémarrez le service Serveur de transfert VMware View pour que vos modifications prennent effet.

**Suivant**

Si nécessaire, configurez manuellement votre pare-feu Windows pour ouvrir les ports mis à jour.

# Dimensionnement de paramètres de Windows Server pour prendre en charge votre déploiement

Pour prendre en charge un déploiement important de postes de travail View Manager, vous pouvez configurer les ordinateurs Windows Server sur lesquels vous installez Serveur de connexion View. Sur chaque ordinateur, vous pouvez dimensionner le fichier d'échange Windows.

Sur les ordinateurs Windows Server 2008 64 bits, les ports éphémères, la table de hachage TCB et les paramètres de la machine virtuelle Java sont dimensionnés par défaut. Ces réglages garantissent que les ordinateurs ont des ressources adéquates pour s'exécuter correctement avec la charge utilisateur prévue.

Par défaut, le système peut créer un maximum de 16 000 ports éphémères environ qui s'exécutent simultanément sur Windows Server 2008. 16 000 ports éphémères peuvent prendre en charge plus de 2 000 connexions client simultanées, le maximum pris en charge pour une instance de Serveur de connexion View.

Sur des ordinateurs Windows Server 2008, vous n'avez pas à augmenter la taille maximale de la table de hachage TCB. Windows Server 2008 ajuste totalement cette valeur par défaut.

Pour les exigences matérielles et de mémoire pour Serveur de connexion View, reportez-vous à la section « Exigences matérielles de Serveur de connexion View », page 8.

Pour des recommandations matérielles et de mémoire pour utiliser Serveur de connexion View dans un déploiement important de View, consultez la section « Configuration de machine virtuelle et nombre maximum dans Serveur de connexion View » dans le document *Planification de l'architecture de VMware Horizon View*.

## Dimensionnement de la machine virtuelle Java

Le programme d'installation de View Connection Server dimensionne la mémoire du segment de la machine virtuelle Java (JVM) sur des ordinateurs View Connection Server pour prendre en charge un nombre important de sessions de poste de travail View simultanées.

Sur un ordinateur Windows Server 64 bits avec au moins 10 Go de mémoire, le programme d'installation configure une taille de segment JVM de 2 Go pour le composant View Secure Gateway Server. Cette configuration prend en charge environ 2 000 sessions par tunnel simultanées, le nombre maximum que View Connection Server peut prendre en charge. Augmenter la taille de segment JVM sur un ordinateur 64 bits avec 10 Go de mémoire n'a aucun avantage.

**Remarque** Sur un ordinateur View Connection Server 64 bits, 10 Go de mémoire sont recommandés pour le déploiement de 50 postes de travail View ou plus. Configurez moins de 10 Go de mémoire uniquement pour les petits déploiements de test de concept.

Si un ordinateur 64 bits possède moins de 10 Go de mémoire, le programme d'installation configure une taille de segment JVM de 512 Mo pour le composant View Secure Gateway Server. Si l'ordinateur possède le minimum requis de 4 Go de mémoire, cette configuration prend en charge environ 500 sessions par tunnel simultanées. Cette configuration est plus qu'adéquate pour prendre en charge les petits déploiements de test de concept.

Si vous augmentez la mémoire d'un ordinateur 64 bits à 10 Go pour prendre en charge un déploiement plus important, View Connection Server n'augmente pas la taille de segment JVM. Pour ajuster la taille de segment JVM à la valeur recommandée, réinstallez View Connection Server.

**Important** Ne modifiez pas la taille de segment JVM sur des ordinateurs Windows Server 64 bits. Modifier cette valeur peut rendre le comportement de View Connection Server instable. Sur des ordinateurs 64 bits, le programme d'installation de View Connection Server définit la taille de segment JVM pour concorder avec la mémoire physique. Si vous modifiez la mémoire physique sur un ordinateur View Connection Server 64 bits, réinstallez View Connection Server pour réinitialiser la taille de segment JVM.

## Configurer les paramètres du fichier d'échange du système

Vous pouvez optimiser la mémoire virtuelle sur les ordinateurs Windows Server sur lesquels vos instances de View Connection Server sont installées en modifiant les paramètres du fichier d'échange du système.

Lors de l'installation de Windows Server, Windows calcule une taille de fichier d'échange initiale et maximale sur la mémoire physique installée sur l'ordinateur. Ces paramètres par défaut restent fixes lorsque vous redémarrez l'ordinateur.

Si l'ordinateur Windows Server est une machine virtuelle, vous pouvez modifier la taille de la mémoire via vCenter Server. Toutefois, si Windows utilise le paramètre par défaut, la taille du fichier d'échange du système ne s'ajuste pas à la nouvelle taille de mémoire.

### Procédure

1 Sur l'ordinateur Windows Server sur lequel View Connection Server est installé, naviguez vers la boîte de dialogue Virtual Memory (Mémoire virtuelle).

   Par défaut, **[Custom size (Taille personnalisée)]** est sélectionné. Une taille de fichier d'échange initiale et maximale apparaît.

2 Cliquez sur **[System managed size (Taille gérée par le système)]** .

Windows recalcule en continu la taille du fichier d'échange du système par rapport à l'utilisation de la mémoire actuelle et de la mémoire disponible.

# Ajout du plug-in de postes de travail View à vSphere Web Client

9

Le plug-in de postes de travail View vous permet d'utiliser vSphere Web Client pour rechercher des informations sur les déploiements de View exécutés dans votre environnement vSphere. Vous ajoutez le plug-in de postes de travail View à vSphere Web Client en l'enregistrant avec vCenter Lookup Service.

Dans View 5.2, le plug-in de postes de travail View est une fonction de la présentation technique qui vous permet de naviguer rapidement entre les utilisateurs de postes de travail virtuels dans View et les machines virtuelles sous-jacentes sur lesquelles ces postes de travail virtuels sont basés.

Utilisez le plug-in de postes de travail View pour dépanner le poste de travail d'un utilisateur. Si un utilisateur appelle avec un problème tel qu'un poste de travail qui s'exécute lentement, vous pouvez immédiatement accéder à la machine virtuelle de l'utilisateur sur la page Machines virtuelles de vSphere Web Client et résoudre le problème.

Ce chapitre aborde les rubriques suivantes :



## Ajouter le plug-in View Desktops

Pour ajouter le plug-in View Desktops à vSphere Web Client, vous devez configurer vCenter Lookup Service et enregistrer le plug-in. Pour effectuer ces tâches, vous exécutez l'utilitaire `regtool.cmd` installé avec Serveur de connexion View.

### Procédure

1 Prise en charge de View Desktops pour les groupes View et les services vCenter Server page 126

Le plug-in View Desktops prend en charge un seul groupe d'instances répliquées de Serveur de connexion View. Vous ne pouvez pas utiliser le plug-in View Desktops pour rechercher des postes de travail gérés par différents groupes d'instances répliquées de Serveur de connexion View.

2 Conditions préalables pour l'inscription de View Desktops page 126

Avant d'ajouter le plug-in View Desktops à vSphere Web Client, vous devez vérifier que vos environnements vSphere et View sont préparés pour l'inscription. Vous devez également identifier les comptes d'utilisateur avec les privilèges d'administrateur requis pour enregistrer le plug-in.

3 Configurer View pour reconnaître vCenter Lookup Service page 127

Vous devez configurer View pour reconnaître vCenter Lookup Service. Vous réalisez cette tâche de configuration une fois pour toutes les instances de Serveur de connexion View dans un groupe répliqué.

4 Enregistrer le plug-in View Desktops page 128

Vous devez enregistrer le plug-in View Desktops avec vCenter Single-Sign On Service et vCenter Lookup Service.

## Prise en charge de View Desktops pour les groupes View et les services vCenter Server

Le plug-in View Desktops prend en charge un seul groupe d'instances répliquées de Serveur de connexion View. Vous ne pouvez pas utiliser le plug-in View Desktops pour rechercher des postes de travail gérés par différents groupes d'instances répliquées de Serveur de connexion View.

Même si plusieurs groupes View utilisent les mêmes vCenter Single Sign-On Service et vCenter Lookup Service, le plug-in View Desktops ne peut prendre en charge qu'un seul groupe à la fois.

Pour utiliser le plug-in View Desktops pour un groupe View différent, vous devez désinscrire le plug-in View Desktops sur toutes les instances de Serveur de connexion View dans le premier groupe et enregistrer le plug-in sur les instances de Serveur de connexion View dans le deuxième groupe.

À l'inverse, si un groupe View est configuré avec plusieurs instances de vCenter Server, chacune utilisant ses propres vCenter Single Sign-On Service et vCenter Lookup Service, vous pouvez configurer le plug-in View Desktops pour un seul vCenter Lookup Service. Pour utiliser le plug-in View Desktops pour un vCenter Lookup Service différent, vous devez désinscrire le plug-in View Desktops sur toutes les instances de Serveur de connexion View et supprimer vCenter Lookup Service de Serveur de connexion View (le groupe View). Vous pouvez ensuite configurer et enregistrer le groupe View pour utiliser le nouveau vCenter Lookup Service.

Pour plus d'informations sur la désinscription et la suppression du plug-in, reportez-vous à la section « Retirer le plug-in View Desktops », page 130.

## Conditions préalables pour l'inscription de View Desktops

Avant d'ajouter le plug-in View Desktops à vSphere Web Client, vous devez vérifier que vos environnements vSphere et View sont préparés pour l'inscription. Vous devez également identifier les comptes d'utilisateur avec les privilèges d'administrateur requis pour enregistrer le plug-in.

### Procédure

- Vérifiez que les produits suivants sont installés :
  - VMware vSphere 5.1 ou une mise à jour ou une version supérieure
  - VMware Horizon View 5.2 ou une mise à jour ou une version supérieure
- Vérifiez que vSphere Web Client est configuré et accessible.
- Vérifiez que les horloges du système sur vos systèmes vSphere et View sont synchronisées.
- Vérifiez que des certificats SSL valides sont configurés sur vos serveurs vSphere et View.

  Si le certificat SSL émis pour vCenter Lookup Service n'est pas approuvé par l'ordinateur Serveur de connexion View sur lequel vous configurez le plug-in View Desktops, vous devez accepter l'empreinte numérique du certificat vCenter Lookup Service lors de l'étape de configuration.
- Vérifiez que des snapshots ont été pris des machines virtuelles sur lesquelles les services vCenter Server sont installés :
  - vCenter Single Sign-On
  - vSphere Web Client

  Ces services peuvent être configurés sur des systèmes séparés ou sur le même système.

- Vérifiez que vous avez un utilisateur avec des privilèges d'administrateur vCenter Single Sign-On (SSO).

  Vous devez fournir ce compte lorsque vous enregistrez le plug-in View Desktops.

  a Connectez-vous à vSphere Web Client avec un compte d'utilisateur disposant de privilèges d'administrateur vCenter SSO.

    Par exemple, sur un vCenter Server exécuté sur Windows Server, l'utilisateur administrateur vCenter SSO par défaut est *Admin*`@System-Domain`. Sur vCenter Server Virtual Appliance, l'utilisateur par défaut est `root@localos`.

  b Allez à **[Administration] > [Accès] > [Utilisateurs et groupes SSO]** .

    L'onglet Utilisateurs sur la page Utilisateurs et groupes vCenter Single Sign-On affiche les utilisateurs avec des privilèges d'administrateur vCenter SSO. Vous pouvez utiliser n'importe quel utilisateur affiché.

- Vérifiez que vous avez un utilisateur avec le rôle Administrateurs View ou Administrateurs de configuration et règles générales. Vous pouvez également utiliser un utilisateur avec le rôle Administrateurs View sur un dossier individuel.

  Vous devez fournir ce compte lorsque vous configurez vCenter Lookup Service et enregistrez le plug-in View Desktops.

  Vous autorisez un compte View Administrators lorsque vous installez Serveur de connexion View. Reportez-vous à la section « Installer Serveur de connexion View avec une nouvelle configuration », page 42.

  Dans l'interface utilisateur de View Administrator, vous pouvez autoriser des utilisateurs supplémentaires avec le rôle Administrateurs View ou Administrateurs de configuration et règles générales. En outre, vous pouvez autoriser un utilisateur à avoir le rôle Administrateurs View sur un dossier individuel. Consultez la section « Gérer des administrateurs » dans le document *Administration de VMware Horizon View*.

### Suivant

Configurez vCenter Lookup Service.

## Configurer View pour reconnaître vCenter Lookup Service

Vous devez configurer View pour reconnaître vCenter Lookup Service. Vous réalisez cette tâche de configuration une fois pour toutes les instances de Serveur de connexion View dans un groupe répliqué.

### Prérequis

- Vérifiez que vos environnements vCenter Server et View sont préparés pour l'inscription. Reportez-vous à la section « Conditions préalables pour l'inscription de View Desktops », page 126.

### Procédure

1 Sur l'ordinateur Serveur de connexion View, allez à l'utilitaire `regtool.cmd`, situé dans le répertoire suivant :

  *`install_directory`*`\VMware\VMware View\Server\TechPreview\ViewAdminPlugin`

2 (Facultatif) Réglez la variable d'environnement `JAVA_HOME` sur le dossier `jre`.

  Par exemple : **`set JAVA_HOME=c:\Program Files\VMware\VMware View\Server\jre`**

3 Configurez vCenter Lookup Service.

Par exemple :
**regtool.cmd configureLookupService -u *view-admin@domain* -ld https://*lookup-server*:7444/lookupservice/sdk**

*view-admin@domain* est le nom d'utilisateur et le domaine d'un utilisateur avec le rôle Administrateurs View.

*lookup-server@domain* est le nom d'hôte ou l'adresse IP et le domaine de l'ordinateur sur lequel vCenter Lookup Service est installé.

4 Si le certificat SSL émis pour vCenter Lookup Service n'est pas approuvé par l'ordinateur Serveur de connexion View, acceptez l'empreinte numérique de certificat.

Le message d'erreur suivant s'affiche :

```
Error: The security certificate presented by this Lookup Service was not
issued by a trusted certificate authority. The thumbprint of the certificate is
thumbprint.
Return code: -1
```

Acceptez l'empreinte numérique en utilisant l'option `-lt` et en copiant l'empreinte numérique. Vous pouvez copier l'empreinte numérique affichée dans le message d'erreur et la coller dans la ligne de commande.

Par exemple :
**regtool.cmd configureLookupService -u *view-admin@domain* -ld https://*lookup-server*:7444/lookupservice/sdk -lt *thumbprint***

L'empreinte numérique *thumbprint* peut ressembler à ce qui suit : `31:2A:32:50:1A:0B:34:B1:65:46:13:A8:0A:5E:F7:43:6E:A9:2C:3E`

5 À l'invite, tapez le mot de passe de l'utilisateur View Administrators.

Le code de retour `0` indique que la configuration a réussi.

---

**Remarque** Lorsque vous tapez le mot de passe, le message d'avertissement suivant peut apparaître. Vous pouvez ignorer ce message :

```
log4j: WARN No appenders could be found for logger
<com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl>.
log4j: WARN Please initialize the log4j system properly.
```

---

### Suivant

Enregistrez le plug-in View Desktops.

## Enregistrer le plug-in View Desktops

Vous devez enregistrer le plug-in View Desktops avec vCenter Single-Sign On Service et vCenter Lookup Service.

Vous devez enregistrer le plug-in View Desktops sur chaque instance de Serveur de connexion View dans un groupe répliqué. Répétez cette procédure sur chaque ordinateur Serveur de connexion View.

---

**Remarque** Les commandes `regtool.cmd register` dans cette procédure supposent que votre service Serveur de connexion View utilise le port par défaut, 443. Si vous modifiez le port par défaut de Serveur de connexion View, utilisez l'option `-p` *port-number* avec la commande `regtool.cmd register` pour spécifier le numéro de port personnalisé.

---

### Prérequis

Vérifiez que vCenter Lookup Service est configuré pour le plug-in View Desktops. Reportez-vous à la section « Configurer View pour reconnaître vCenter Lookup Service », page 127.

### Procédure

1 Sur l'ordinateur Serveur de connexion View, allez à l'utilitaire `regtool.cmd`, situé dans le répertoire suivant :

*install_directory*`\VMware\VMware View\Server\TechPreview\ViewAdminPlugin`

2 Enregistrez le plug-in View Desktops.

Par exemple : **`regtool.cmd register -u`** ***`view-admin@domain`*** **`-lu`** ***`sso-admin@domain`***

*view-admin@domain* est le nom d'utilisateur et le domaine d'un utilisateur avec le rôle Administrateurs View.

*sso-admin@domain* est le nom d'utilisateur et le domaine d'un utilisateur avec les privilèges d'administrateur vCenter SSO. Sur un vCenter Server exécuté sur Windows Server, l'utilisateur administrateur vCenter SSO par défaut est *Admin*`@System-Domain`. Sur vCenter Server Virtual Appliance, l'utilisateur par défaut est `root@localos`.

3 À l'invite, tapez le mot de passe de l'utilisateur View Administrators.

4 À l'invite, tapez le mot de passe de l'utilisateur administrateur vCenter SSO.

Le code de retour `0` indique que la configuration a réussi.

---

**Remarque** Lorsque vous tapez le mot de passe, le message d'avertissement suivant peut apparaître. Vous pouvez ignorer ce message :

```
log4j: WARN No appenders could be found for logger
<com.vmware.vim.vmomi.core.types.impl.VmodlContextImpl>.
log4j: WARN Please initialize the log4j system properly.
```

---

5 Si nécessaire, redémarrez le service VMware vSphere Web Client.

Dans certains cas, ce service doit être redémarré pour que l'enregistrement prenne effet.

Le service réside sur l'ordinateur vCenter Server ou un autre ordinateur, pas sur l'ordinateur Serveur de connexion View.

6 (Facultatif) Vérifiez que le groupe Serveur de connexion View, le plug-in View Desktops et l'instance de Serveur de connexion View ont été enregistrés à l'aide de la commande `regtool.cmd showDetails`.

Par exemple : **`regtool.cmd showDetails -u`** ***`view-admin@domain`***

### Suivant

Connectez-vous à vSphere Web Client pour vérifier que le plug-in View Desktops a été ajouté. Reportez-vous à la section « Rechercher des utilisateurs View dans vSphere Web Client », page 130.

# Rechercher des utilisateurs View dans vSphere Web Client

Dans **[View Desktops]** dans vSphere Web Client, vous pouvez effectuer une recherche rapide ou simple d'un utilisateur View, afficher les postes de travail associés à cet utilisateur et examiner les machines virtuelles sous-jacentes. Après avoir configuré le plug-in View Desktops, effectuez cette tâche pour vérifier que le plug-in a été ajouté à vSphere Web Client.

Lorsque vous recherchez un utilisateur View dans vSphere Web Client, **[View Desktops]** affiche des postes de travail flottants sur lesquels l'utilisateur a ouvert une session et des postes de travail dédiés affectés à l'utilisateur. Notez qu'un poste de travail flottant est affiché même lorsque la session est dans un état déconnecté. Si un utilisateur est autorisé sur un pool de postes de travail flottants mais qu'il n'a pas de session ouverte, aucun poste de travail flottant dans ce pool n'est affiché.

Cette procédure utilise la recherche rapide. Vous pouvez également utiliser une recherche simple pour rechercher des utilisateurs View. Dans cette présentation technique, vous ne pouvez pas utiliser la recherche avancée pour rechercher des utilisateurs View.

### Prérequis

- Vérifiez que le plug-in View Desktops a été configuré avec vCenter Lookup Service et enregistré avec vSphere Web Client. Reportez-vous aux sections « Configurer View pour reconnaître vCenter Lookup Service », page 127 et « Enregistrer le plug-in View Desktops », page 128.
- Vérifiez que vous pouvez ouvrir une session sur vSphere Web Client en tant qu'utilisateur avec le rôle Administrateurs View ou Administrateurs View (lecture seule) et avec le privilège Administrateur vSphere pour les machines virtuelles de poste de travail View et les dossiers vCenter Server qui stockent les machines virtuelles.

  Si vous recherchez des postes de travail sans disposer du privilège Administrateur vSphere, les noms de machine virtuelle sont affichés sous forme de liens désactivés et vous ne pouvez pas accéder aux informations de machine virtuelle.

### Procédure

1. Ouvrez une session sur vSphere Web Client en tant qu'utilisateur avec le rôle Administrateurs View ou Administrateurs View (lecture seule) et les privilèges Administrateur vSphere appropriés.

   Par exemple : `https://vSphere_Web_Client_IP_address_or_FQDN:9443/vsphere-client/`
2. Dans la zone Rechercher, tapez le nom d'un utilisateur de View.
3. Sélectionnez le nom d'utilisateur dans les résultats de la recherche.
4. Sélectionnez un poste de travail associé à l'utilisateur dans la liste de postes de travail.
5. Allez à la page Machines virtuelles pour voir des détails sur la machine virtuelle de poste de travail sous-jacente.

# Retirer le plug-in View Desktops

Pour retirer le plug-in View Desktops de vSphere Web Client, vous devez désinscrire le plug-in sur chaque instance de Serveur de connexion View dans un groupe répliqué. Ensuite, vous retirez la configuration vCenter Lookup Service.

Dans un groupe répliqué d'instances de Serveur de connexion View, vous ne pouvez pas désinscrire l'instance sur laquelle vous avez enregistré le plug-in View Desktops en premier tant que toutes les autres instances ne sont pas désinscrites.

Si vous prévoyez de réaliser des opérations de maintenance sur les instances de Serveur de connexion View dans un groupe répliqué, vous pouvez utiliser l'option `–f` avec la commande `regtool.cmd removeLookUpService` pour désinscrire toutes les instances de Serveur de connexion View et retirer la configuration vCenter Lookup Service en une seule étape.

Si vous prévoyez d'interrompre une instance de Serveur de connexion View pour une maintenance planifiée, vous devez désinscrire l'instance de vCenter Lookup Service avant de démarrer la procédure de maintenance.

### Procédure

1 Sur l'ordinateur Serveur de connexion View, allez à l'utilitaire `regtool.cmd`, situé dans le répertoire suivant :

*install_directory*`\VMware\VMware View\Server\TechPreview\ViewAdminPlugin`

2 Désinscrivez le plug-in View Desktops.

Par exemple : **`regtool.cmd unregister –u`** ***`view–admin@domain`***

*view–admin@domain* est le nom d'utilisateur et le domaine d'un utilisateur avec le rôle Administrateurs View.

3 À l'invite, tapez le mot de passe de l'utilisateur View Administrators.

Le code de retour `0` indique que la configuration a réussi.

4 Répétez les étapes précédentes pour désinscrire le plug-in sur toutes les instances de Serveur de connexion View dans un groupe répliqué.

Lorsque toutes les autres instances sont désinscrites, désinscrivez le plug-in sur l'instance sur laquelle vous avez effectué l'inscription en premier.

5 Retirez la configuration vCenter Lookup Service de Serveur de connexion View.

Par exemple : **`regtool.cmd removeLookUpService –u`** ***`view–admin@domain`***

Vous pouvez exécuter cette commande sur n'importe quelle instance de Serveur de connexion View dans un groupe répliqué. La commande échoue si le plug-in View Desktops est toujours enregistré sur une instance de Serveur de connexion View.

6 À l'invite, tapez le mot de passe de l'utilisateur View Administrators.

Le code de retour `0` indique que la configuration a réussi.

# Configuration du reporting d'événements 10

Vous pouvez créer une base de données des événements pour enregistrer des informations sur des événements de View Manager. En outre, si vous utilisez un serveur Syslog, vous pouvez configurer Serveur de connexion View pour qu'il envoie des événements à un serveur Syslog ou créer un fichier plat d'événements écrit au format `Syslog`.

Ce chapitre aborde les rubriques suivantes :



## Ajouter une base de données et un utilisateur de base de données pour des événements View

Vous créez une base de données des événements en l'ajoutant à un serveur de base de données existant. Vous pouvez alors utiliser un logiciel de reporting d'entreprise pour analyser les événements dans la base de données.

Le serveur de base de données pour la base de données des événements peut résider sur un hôte de View Connection Server lui-même ou sur un serveur dédié. Vous pouvez également utiliser un serveur de base de données existant approprié, tel qu'un serveur hébergeant une base de données View Composer.

**Remarque** Vous n'avez pas à créer une source de données ODBC pour cette base de données.

### Prérequis

- Vérifiez que vous possédez un serveur de base de données Microsoft SQL Server ou Oracle pris en charge sur un système auquel une instance de View Connection Server a accès. Pour voir une liste des versions de base de données prises en charge, reportez-vous à la section « Exigences de base de données pour View Composer », page 11.
- Vérifiez que vous disposez des privilèges de base de données requis pour créer une base de données et un utilisateur sur le serveur de base de données.
- Si vous ne connaissez pas bien la procédure pour créer des bases de données sur des serveurs de base de données Microsoft SQL Server, reportez-vous aux étapes dans la section « Ajouter une base de données View Composer à SQL Server », page 30.

- Si vous ne connaissez pas bien la procédure pour créer des bases de données sur des serveurs de base de données Oracle, reportez-vous aux étapes dans la section « Ajouter une base de données View Composer à Oracle 11g ou 10g », page 33.

### Procédure

1 Ajoutez une nouvelle base de données au serveur et donnez-lui un nom descriptif tel que ViewEvents.

2 Ajoutez un utilisateur à cette base de données qui a l'autorisation de créer des tableaux, des vues et, dans le cas d'Oracle, des déclenchements et des séquences, ainsi que l'autorisation de lire ces objets et d'incrire sur ces objets.

   Pour une base de données Microsoft SQL Server, n'utilisez pas la méthode du modèle de sécurité d'authentification Windows intégrée. Assurez-vous d'utiliser la méthode d'authentification SQL Server.

La base de données est créée, mais le schéma n'est pas installé tant que vous n'avez pas configuré la base de données dans View Administrator.

### Suivant

Suivez les instructions de la section « Configurer la base de données des événements », page 135.

## Préparer une base de données SQL Server pour le reporting d'événements

Avant de pouvoir utiliser View Administrator pour configurer une base de données des événements sur Microsoft SQL Server, vous devez configurer les propriétés TCP/IP correctes et vérifier que le serveur utilise l'authentification SQL Server.

### Prérequis

- Créez une base de données SQL Server pour le reporting d'événements. Reportez-vous à la section « Ajouter une base de données et un utilisateur de base de données pour des événements View », page 133.
- Vérifiez que vous disposez des privilèges de base de données requis pour configurer la base de données.
- Vérifiez que le serveur de base de données utilise la méthode d'authentification SQL Server. N'utilisez pas l'authentification Windows.

### Procédure

1 Ouvrez le Gestionnaire de configuration SQL Server et développez **[SQL Server*YYYY*Network Configuration (Configuration du réseau SQL Server*YYYY*)]** .

2 Sélectionnez **[Protocols for*server_name*(Protocoles pour*server_name*)]** .

3 Dans la liste de protocoles, cliquez avec le bouton droit sur **[TCP/IP]** et sélectionnez **[Properties (Propriétés)]** .

4 Définissez la propriété **[Enabled (Activé)]** sur **[Yes (Oui)]** .

5 Vérifiez qu'un port est affecté ou, si nécessaire, affectez-en un.

   Pour plus d'informations sur les ports statiques et dynamiques et comment les affecter, consultez l'aide en ligne du Gestionnaire de configuration SQL Server.

6 Vérifiez que ce port n'est pas bloqué par un pare-feu.

### Suivant

Utilisez View Administrator pour connecter la base de données à View Connection Server. Suivez les instructions de la section « Configurer la base de données des événements », page 135.

# Configurer la base de données des événements

La base de données des événements stocke des informations sur des événements View sous forme d'enregistrements dans une base de données plutôt que dans un fichier journal.

Vous configurez une base de données des événements après l'installation d'une instance de Serveur de connexion View. Vous devez configurer uniquement un hôte dans un groupe Serveur de connexion View. Les hôtes restant dans le groupe sont configurés automatiquement.

**Remarque** La sécurité de la connexion de la base de données entre l'instance de Serveur de connexion View et une base de données externe est de la responsabilité de l'administrateur, même si le trafic des événements est limité à des informations sur l'intégrité de l'environnement View. Si vous voulez prendre des précautions supplémentaires, vous pouvez sécuriser ce canal via IPSec ou d'autres moyens ou vous pouvez déployer la base de données localement sur l'ordinateur Serveur de connexion View.

Vous pouvez utiliser des outils de rapport de base de données de Microsoft SQL Server ou d'Oracle pour examiner des événements dans les tableaux de base de données. Pour plus d'informations, consultez le document *Intégration de VMware Horizon View*.

Vous pouvez également générer des événements View au format `Syslog` pour qu'un logiciel d'analyse tiers puisse accéder aux données d'événement. Vous utilisez la commande `vdmadmin` avec l'option `–I` pour enregistrer des messages d'événement View au format `Syslog` dans des fichiers de journal des événements. Consultez la section « Génération de messages de journal des événements View au format Syslog à l'aide de l'option -I » dans le document *Administration de VMware Horizon View*.

### Prérequis

Vous avez besoin des informations suivantes pour configurer une base de données des événements :

- Le nom DNS ou l'adresse IP du serveur de base de données.
- Le type de serveur de base de données : Microsoft SQL Server ou Oracle.
- Le numéro de port utilisé pour accéder au serveur de base de données. Le port par défaut est 1521 pour Oracle et 1433 pour SQL Server. Pour SQL Server, si le serveur de base de données est une instance nommée, ou si vous utilisez SQL Server Express, vous devez déterminer le numéro de port. Pour plus d'informations sur la connexion à une instance nommée de SQL Server, consultez l'article de la Base de connaissances Microsoft à l'adresse http://support.microsoft.com/kb/265808.
- Le nom de la base de données des événements que vous avez créé sur le serveur de base de données. Reportez-vous à la section « Ajouter une base de données et un utilisateur de base de données pour des événements View », page 133.
- Le nom d'utilisateur et le mot de passe de l'utilisateur que vous avez créés pour cette base de données. Reportez-vous à la section « Ajouter une base de données et un utilisateur de base de données pour des événements View », page 133.

  Utilisez l'authentification SQL Server pour cet utilisateur. N'utilisez pas la méthode du modèle de sécurité d'authentification Windows intégrée.
- Un préfixe pour les tableaux dans la base de données des événements, par exemple, VE_. Le préfixe permet de partager la base de données sur plusieurs installations de View.

  **Remarque** Vous devez saisir des caractères valides pour le logiciel de base de données que vous utilisez. La syntaxe du préfixe n'est pas vérifiée lorsque vous remplissez la boîte de dialogue. Si vous saisissez des caractères qui ne sont pas valides pour le logiciel de base de données que vous utilisez, une erreur se produit lorsque Serveur de connexion View tente de se connecter au serveur de base de données. Le fichier journal indique toutes les erreurs, y compris cette erreur et les autres renvoyées à partir du serveur de base de données si le nom de la base de données n'est pas valide.

### Procédure

1 Dans View Administrator, sélectionnez **[Configuration de View] > [Configuration d'événements]** .

2 Dans la fenêtre **[Base de données des événements]** , cliquez sur **[Modifier]** , saisissez les informations dans les champs fournis et cliquez sur **[OK]** .

3 (Facultatif) Dans la fenêtre Paramètres des événements, cliquez sur **[Modifier]** , modifiez le délai d'affichage des événements et le nombre de jours pour classer des événements comme nouveaux et cliquez sur **[OK]** .

   Ces paramètres concernent la durée pendant laquelle les événements sont répertoriés dans l'interface de View Administrator. Après cette durée, les événements ne sont disponibles que dans les tableaux de base de données historiques.

   La fenêtre Database Configuration (Configuration de base de données) affiche la configuration actuelle de la base de données des événements.

4 Sélectionnez **[Contrôle] > [Événements]** pour vérifier que la connexion à la base de données des événements fonctionne correctement.

   Si la connexion échoue, un message d'erreur apparaît. Si vous utilisez SQL Express ou une instance nommée de SQL Server, vous devez déterminer le numéro de port correct, comme indiqué dans les conditions préalables.

Dans le tableau de bord de View Administrator, l'état du composant système affiche le serveur de base de données des événements sous le titre Reporting Database (Base de données de rapports).

## Configurer la journalisation des événements pour des serveurs Syslog

Vous pouvez générer des événements View au format `Syslog` pour qu'un logiciel d'analyse puisse accéder aux données d'événement.

Vous devez configurer uniquement un hôte dans un groupe Serveur de connexion View. Les hôtes restant dans le groupe sont configurés automatiquement.

Si vous activez la journalisation d'événements basée sur des fichiers, les événements sont accumulés dans un fichier journal local. Si vous spécifiez un partage de fichiers, ces fichiers journaux sont déplacés dans ce partage.

- Utilisez un fichier local uniquement pour un dépannage rapide lors de la configuration, peut-être avant que la base de données des événements soit configurée, pour que vous puissiez voir les événements.

  La taille maximale du répertoire local pour les journaux des événements, y compris les fichiers journaux fermés, avant que les fichiers les plus anciens soient supprimés, est de 300 Mo. La destination par défaut de la sortie Syslog est `%PROGRAMDATA%\VMware\VDM\events\`.

- Utilisez un chemin d'accès UNC pour enregistrer les fichiers journaux afin de conserver longtemps les événements, ou si vous ne possédez pas de serveur Syslog ou si votre serveur Syslog actuel ne répond pas à vos besoins.

Vous pouvez également utiliser une commande `vdmadmin` pour configurer la journalisation d'événements basée sur des fichiers au format Syslog. Consultez la rubrique sur la génération de messages de journal des événements View au format Syslog à l'aide de l'option `–I` de la commande `vdmadmin`, dans le document *Administration de VMware Horizon View*.

**IMPORTANT** Des données Syslog sont envoyées sur le réseau sans chiffrement logiciel et elles peuvent contenir des données sensibles, telles que des noms d'utilisateur. VMware recommande d'utiliser une sécurité de couche de liaison, telle qu'IPSEC, pour éviter que ces données soient surveillées sur le réseau.

### Prérequis

Vous avez besoin des informations suivantes pour configurer Serveur de connexion View pour que les événements puissent être enregistrés au format Syslog ou envoyés à un serveur Syslog, ou les deux :

- Si vous prévoyez d'utiliser un serveur Syslog pour écouter les événements View sur un port UDP, vous devez posséder le nom DNS ou l'adresse IP du serveur Syslog et le numéro de port UDP. Le numéro de port UDP par défaut est 514.
- Si vous prévoyez de collecter des journaux dans un format de fichier plat, vous devez posséder le chemin d'accès UNC vers le partage de fichiers et le dossier dans lequel seront stockés les fichiers journaux, et vous devez posséder le nom d'utilisateur, le nom de domaine et le mot de passe d'un compte avec l'autorisation d'écrire sur le partage de fichiers.

### Procédure

1 Dans View Administrator, sélectionnez **[Configuration de View] > [Configuration d'événements]** .

2 (Facultatif) Dans la zone **[Syslog]** , pour configurer Serveur de connexion View afin qu'il envoie des événements à un serveur Syslog, cliquez sur **[Ajouter]** à côté de **[Envoyer à des serveurs syslog]** et indiquez le nom de serveur ou l'adresse IP et le numéro de port UDP.

3 (Facultatif) Pour permettre à des messages de journal des événements View d'être générés et stockés au format Syslog, dans des fichiers journaux, cochez la case **[Enregistrer dans un fichier : Activer]** .

   Les fichiers journaux sont conservés localement, sauf si vous spécifiez un chemin d'accès UNC vers un partage de fichiers.

4 (Facultatif) Pour stocker les messages de journal des événements View sur un partage de fichiers, cliquez sur **[Ajouter]** à côté de **[Copier vers l'emplacement]** et indiquez le chemin d'accès UNC vers le partage de fichiers et le dossier dans lequel seront stockés les fichiers journaux, avec le nom d'utilisateur, le nom de domaine et le mot de passe d'un compte avec l'autorisation d'écrire sur le partage de fichiers.

   Voici un exemple de chemin d'accès UNC :

   ```
   \\syslog-server\folder\file
   ```

# Index

## R



## S



## T



## U



## V

## W