Installation de View

VMware Horizon 6.0

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-001496-00

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 View

Installation de View explique comment installer le serveur VMware Horizon™ avec View™ et les composants client.

Public cible

Ces informations sont destinées à toute personne souhaitant installer View. Les informations sont destinées aux administrateurs 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 d'View doivent satisfaire à des exigences matérielles et logicielles spécifiques.

Ce chapitre aborde les rubriques suivantes :

Exigences de Serveur de connexion View

Serveur de connexion View agit comme un broker pour les connexions clientes en authentifiant et en dirigeant les demandes entrantes d'utilisateur vers les applications et les postes de travail distants appropriés. Le Serveur de connexion View a des exigences matérielles, de système d'exploitation, d'installation et de logiciels pris en charge spécifiques.

Exigences matérielles de Serveur de connexion View

Vous devez installer tous les types d'installation de Serveur de connexion View, y compris les installations standard, de réplica et de serveur de sécurité, sur une machine physique ou virtuelle dédiée répondant à des exigences matérielles spécifiques.

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

Composant matériel	Requis	Recommandé
Processeur	Processeur Pentium IV 2.0 GHz ou supérieur	4 CPU
Carte réseau	Carte réseau 100 Mbit/s	Des cartes réseau de 1 Gbit/s
Mémoire Windows Server 2008 64 bits	RAM de 4 Go ou plus	Au moins 10 Go de RAM pour des déploiements de 50 postes de travail distants ou plus
Mémoire Windows Server 2012 64 bits	RAM de 4 Go ou plus	Au moins 10 Go de RAM pour des déploiements de 50 postes de travail distants ou plus

Ces exigences s'appliquent aussi aux instances de Serveur de connexion View de réplica et de serveur de sécurité que vous installez pour une haute disponibilité ou un accès externe.

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

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

Vous devez installer Serveur de connexion View sur un système d'exploitation Windows Server pris en charge.

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

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

Système d'exploitation	Version	Édition
Windows Server 2008 R2	64 bits	Standard Enterprise
Windows Server 2008 R2 SP1	64 bits	Standard Enterprise
Windows Server 2012 R2	64 bits	Standard

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'View compatibles avec les versions de vCenter Server et d'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

Lorsque vous installez des instances répliquées de Serveur de connexion View, vous devez généralement configurer les instances dans le même emplacement physique et les connecter sur un réseau local haute performance. Sinon, des problèmes de latence peuvent entraîner l'incohérence des configurations de View LDAP sur les instances de Serveur de connexion View. L'accès d'un utilisateur peut être refusé lors de la connexion à une instance de Serveur de connexion View avec une configuration périmée.

IMPORTANT Pour utiliser un groupe d'instances du Serveur de connexion View répliquées dans un réseau étendu, un réseau métropolitain ou autre réseau non local dans des scénarios dans lesquels un déploiement d'View doit s'étendre sur plusieurs centres de données, vous devez utiliser la fonctionnalité Cloud Pod Architecture. Vous pouvez relier quatre espaces View afin de fournir un seul vaste environnement de gestion et d'échange de postes de travail pour deux sites géographiquement distants et gérer jusqu'à 20 000 postes de travail distants. Pour en savoir plus, consultez *Administration de Cloud Pod Architecture* dans View.

Exigences de View Administrator

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

View Administrator est une application Web installée lorsque vous installez le Serveur de connexion View. Vous pouvez accéder à View Administrator et l'utiliser 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 10.1 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 View* concernant l'importation de certificats racine et intermédiaires.

Pour que le texte s'affiche correctement, View Administrator requiert des polices 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 les 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

Avec View Composer, vous pouvez 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 limitations spécifiques. Vous pouvez installer View Composer sur la même machine physique ou virtuelle que vCenter Server ou sur un serveur séparé.

- Exigences matérielles de View Composer autonome page 10

  Si vous installez View Composer sur une machine physique ou virtuelle autre que celle utilisée pour vCenter Server, vous devez utiliser une machine dédiée qui satisfait à 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 View Composer Server.

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 limitations spécifiques. Vous pouvez installer View Composer sur la même machine physique ou virtuelle que vCenter Server ou sur un serveur séparé.

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

Système d'exploitation	Version	Édition
Windows Server 2008 R2	64 bits	Standard Enterprise
Windows Server 2008 R2 SP1	64 bits	Standard Enterprise
Windows Server 2012 R2	64 bits	Standard

Si vous prévoyez d'installer View Composer sur une machine physique ou virtuelle autre que vCenter Server, reportez-vous à « Exigences matérielles de View Composer autonome », page 10.

Exigences matérielles de View Composer autonome

Si vous installez View Composer sur une machine physique ou virtuelle autre que celle utilisée pour vCenter Server, vous devez utiliser une machine dédiée qui satisfait à des exigences matérielles spécifiques.

Une installation View Composer autonome fonctionne avec vCenter Server installé sur une machine Windows Server séparée ou avec le dispositif vCenter Server Linux. VMware recommande la mise en place d'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	Requis	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 Mbit/s	Des cartes réseau de 1 Gbit/s

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

Composant matériel	Requis	Recommandé
Mémoire	RAM de 4 Go ou plus	RAM de 8 Go ou plus pour des déploiements de 50 postes de travail distants 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 View Composer Server.

Si une instance du serveur de base de données existe déjà pour vCenter Server, View Composer peut utiliser cette instance existante s'il s'agit d'une version répertoriée dans Tableau 1-5 Par exemple, View Composer peut utiliser l'instance Microsoft SQL Server fournie avec vCenter Server. Si aucune instance du serveur de base de données n'existe, vous devez en installer une.

View Composer prend en charge un sous-ensemble des serveurs de base de données compatibles avec vCenter Server. 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 distinct à utiliser pour les événements des bases de données View Composer et View.

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.

Le tableau suivant répertorie les serveurs de base de données pris en charge et leurs versions. Pour la liste complète des versions de base de données prises en charge avec vCenter Server, reportez-vous aux matrices d'interopérabilité des produits VMware à l'adresse http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Les versions de vCenter Server répertoriées dans les titres de colonne de tableau sont générales. Pour les versions de mise à jour spécifiques prises en charge de chaque version de vCenter Server, reportez-vous aux matrices d'interopérabilité des produits VMware à l'adresse http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

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

Base de données	vCenter Server 5.5	vCenter Server 5.1	vCenter Server 5.0	vCenter Server 4.1
Microsoft SQL Server 2012 Express (32 et 64 bits)	Oui	Oui	Oui	Non
Microsoft SQL Server 2012 (SP1) Standard et Enterprise (32 et 64 bits)	Oui	Oui	Oui	Non
Microsoft SQL Server 2008 Express (R2 SP2) (64 bits)	Non	Oui	Oui	Non
Microsoft SQL Server 2008 (SP3), Standard, Enterprise et Datacenter (32 et 64 bits)	Non	Oui	Oui	Oui
Microsoft SQL Server 2008 (R2 SP2), 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 5.5	vCenter Server 5.1	vCenter Server 5.0	vCenter Server 4.1
Oracle 10g Release 2, Standard, Standard ONE et Enterprise [10.2.0.4] (32 et 64 bits)	Non	Oui	Oui	Oui
Oracle 11g Release 2, Standard, Standard ONE et Enterprise [11.2.0.3] (32 et 64 bits)	Oui	Oui	Oui	Oui

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'authentification unique, la redirection de périphérique et d'autres fonctionnalités. Vous devez installer View Agent sur l'ensemble des machines virtuelles, des systèmes physiques et des hôtes RDS.

Le tableau suivant répertorie les versions du système d'exploitation Windows qui sont prises en charge sur les machines virtuelles dans un pool de postes de travail.

Tableau 2-1. Systèmes d'exploitation pour postes de travail distants de clone lié ou de clone complet

Système d'exploitation client	Version	Édition	Service Pack
Windows 8.1	32 bits et 64 bits	Enterprise et Professional	Aucun et mettre à jour
Windows 8	32 bits et 64 bits	Enterprise et Professional	Aucune
Windows 7	32 bits et 64 bits	Enterprise et Professional	Aucun et SP1
Windows Vista	32 bits	Business et Enterprise	SP2
Windows XP	32 bits	Professional	SP3
Windows Server 2008 R2	64 bits	Datacenter	SP1

IMPORTANT La version de la machine virtuelle doit prendre en charge le système d'exploitation invité. Par exemple, pour installer Windows 8.1, vous devez utiliser une machine virtuelle vSphere 5.1 ou version ultérieure.

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 les ordinateurs physiques ou sur les hôtes RDS.

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 14.

Le tableau suivant répertorie les versions du système d'exploitation Windows qui sont prises en charge pour la création de pools de postes de travail et d'applications sur un hôte RDS.

Tableau 2-2. Systèmes d'exploitation pour hôtes RDS, fournissant des applications ou des postes de travail distants

Système d'exploitation client	Édition	Service Pack
Windows Server 2008 R2	Standard, Enterprise et Datacenter	SP1
Windows Server 2012	Standard et Datacenter	Aucune
Windows Server 2012 R2	Standard et Datacenter	Aucune

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 2-3 répertorie les systèmes d'exploitation pris en charge pour le logiciel View Persona Management autonome.

Tableau 2-3. 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 et logiciels d'affichage à distance fournissent l'accès aux applications et postes de travail distants. Le protocole d'affichage à distance utilisé dépend du type de périphérique client, de votre choix de vous connecter à un poste de travail ou à une application distante et de la manière dont l'administrateur configure le pool d'applications ou de postes de travail.

- PCoIP page 15

  PCoIP (PC-over-IP) offre une expérience de poste de travail optimisée pour fournir une application distante ou l'intégralité de l'environnement d'un poste de travail distant, y compris des applications, des images, du contenu audio et vidéo, à un grand nombre d'utilisateurs sur le réseau local ou sur le réseau étendu. PCoIP peut compenser une augmentation de la latence ou une réduction de la bande passante pour garantir que les utilisateurs peuvent rester productifs quelles que soient les conditions du réseau.

- Microsoft RDP page 17

  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.

PCoIP

PCoIP (PC-over-IP) offre une expérience de poste de travail optimisée pour fournir une application distante ou l'intégralité de l'environnement d'un poste de travail distant, y compris des applications, des images, du contenu audio et vidéo, à un grand nombre d'utilisateurs sur le réseau local ou sur le réseau étendu. PCoIP peut compenser une augmentation de la latence ou une réduction de la bande passante pour garantir que les utilisateurs peuvent rester productifs quelles que soient les conditions du réseau.

PCoIP est pris en charge comme protocole d'affichage pour les applications et les postes de travail distants qui utilisent des machines virtuelles, des machines physiques qui contiennent des cartes d'hôte Teradici ou des postes de travail à session partagée sur un hôte RDS.

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 établir une connexion chiffrée et sécurisée avec un serveur de sécurité 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 disposant des versions de système d'exploitation View Agent répertoriées dans la section « Systèmes d'exploitation pris en charge pour View Agent », page 13 sont prises en charge.
- Les connexions à partir de tous les types d'appareils clients.
- Les contrôles d'optimisation pour la réduction de l'utilisation de bande passante sur les réseaux LAN et WAN.
- Les couleurs 32 bits sont prises en charge pour les affichages virtuels.
- Les polices ClearType sont prises en charge.
- Redirection audio avec réglage dynamique de la qualité audio pour les réseaux locaux et les réseaux étendus.

- Audio/vidéo en temps réel pour l'utilisation de webcams et de microphones sur certains types de clients.
- Copier-coller de texte et, sur certains clients, d'images entre le système d'exploitation client et une application ou un poste de données distant. Pour d'autres types de clients, seul le copier-coller de texte brut est pris en charge. Vous ne pouvez pas copier et coller des objets système comme des dossiers et des fichiers entre des systèmes.
- Plusieurs écrans sont pris en charge pour certains types de client. Par exemple, sur les clients Windows, vous pouvez utiliser jusqu'à quatre écrans et régler la résolution de chaque écran séparément, avec une résolution maximale de 2 560 x 1 600 par écran. La rotation d'affichage et l'ajustement automatique sont également pris en charge.

  Lorsque la fonctionnalité 3D est activée, jusqu'à 2 moniteurs sont pris en charge avec une résolution maximale de 1 920 x 1 200.
- La redirection USB est prise en charge pour certains types de client.
- La redirection MMR est prise en charge pour certains systèmes d'exploitation clients Windows et certains systèmes d'exploitation de postes de travail distants (sur lesquels View Agent est installé).

Pour plus d'informations sur les systèmes d'exploitation de postes de travail qui prennent en charge des fonctionnalités PCoIP spécifiques, reportez-vous à « Matrice de prise en charge des fonctionnalités pour View Agent » dans le document *Planification de l'architecture de View*.

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 recommandés pour les postes de travail distants incluent notamment :

- 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 ou les postes de travail Windows Server 2012 ou R2 : 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. Pour utiliser vDGA (Virtual Dedicated Graphics Acceleration) pour les applications graphiques intensives telles que les applications CAO, une capacité de 4 Go de RAM est requise.

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 distant dispose d'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 distant dispose d'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 distant dispose d'une CPU virtuelle double, vous pouvez lire une vidéo formatée à 1 080p, bien que la taille d'écran du lecteur multimédia puisse nécessiter une diminution.
rendu 3D	Vous pouvez configurer des postes de travail distants pour utiliser des graphiques à accélération matérielle ou logicielle. La fonctionnalité graphique à accélération logicielle vous permet d'exécuter des applications DirectX 9 et OpenGL 2.1 sans nécessiter de GPU physique. Les fonctionnalités graphiques à accélération matérielle permettent aux machines virtuelles de partager les GPU (graphical processing unit) physiques sur un hôte vSphere ou de dédier une GPU physique à un seul poste de travail de machine virtuelle. Pour les applications 3D, jusqu'à deux moniteurs sont pris en charge et la résolution d'écran maximale est de 1 920 x 1 200. Le système d'exploitation invité sur les postes de travail de machines virtuelles doivent exécuter Windows 7 ou version ultérieure.

Exigences matérielles des systèmes client

Pour plus d'informations sur les exigences de processeur et de mémoire, reportez-vous au document « Utilisation de VMware Horizon Client » pour le type spécifique de poste de travail ou d'appareil mobile client. 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 est un protocole d'affichage pris en charge par les postes de travail distants utilisant les machines virtuelles, les machines physiques ou les postes de travail en session partagée sur un hôte RDS. (Seul le protocole d'affichage PCoIP est pris en charge pour les applications distantes.) 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 distant.
- 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, reportez-vous au document « Utilisation de VMware Horizon Client » pour le type spécifique de système client. Allez sur https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

Remarque Les périphériques clients mobiles 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 niveaux fonctionnels de domaine des services de domaine Active Directory (AD DS) suivants :

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Ce chapitre aborde les rubriques suivantes :

Configuration de domaines et de relations d'approbation

Vous devez associer chaque hôte de Serveur de connexion View à un domaine Active Directory. L'hôte ne doit pas être un contrôleur de domaine. Vous placez des postes de travail distants dans le même domaine que l'hôte de Serveur du connexion View ou dans un domaine qui a une relation d'approbation bidirectionnelle avec le domaine de l'hôte de Serveur du connexion View. Plus spécifiquement, il doit s'agir d'une approbation bidirectionnelle non transitive externe.

Vous pouvez autoriser l'accès à des utilisateurs et à des groupes dans le domaine de l'hôte de connexion View vers des applications et des postes de travail distants. Vous pouvez également sélectionner des utilisateurs et des groupes du domaine de l'hôte de Serveur de connexion View 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 Serveur de connexion View.

Les utilisateurs sont authentifiés par Active Directory pour le domaine de l'hôte de Serveur de connexion View 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, le 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 les domaines que vous ne souhaitez pas proposer aux utilisateurs lorsqu'ils se connectent à leurs applications et postes de travail distants.

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. Reportez-vous au document *Administration de View* pour plus d'informations.

Création d'une UO pour des postes de travail distants

Vous devez créer une unité d'organisation (UO) spécifiquement pour vos postes de travail distants. 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 d'View et le lier à l'UO qui contient vos postes de travail distants. 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 distants. Les administrateurs 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 le logiciel client pour se connecter à une instance du Serveur de connexion View et lancer une session de bureau 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.

Reportez-vous au document *Administration de View* pour plus d'informations.

Création de groupes pour les utilisateurs

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

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 du Serveur de connexion View 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 91 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 requiert que ce compte joigne les machines virtuelles 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 :

   - Lister le contenu
   - Lire toutes les propriétés
   - Écrire toutes les propriétés
   - Autorisations de lecture
   - 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 :

   - Lister le contenu
   - Lire toutes les propriétés
   - Autorisations de lecture
   - 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 pouvoir se connecter à un poste de travail distant, les utilisateurs doivent appartenir au groupe Utilisateurs du Bureau à distance local du poste de travail distant. 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 distant joint 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 distant sont toujours ajoutés au groupe Utilisateurs du Bureau à distance local de chaque poste de travail distant joint 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 distant.

Prérequis

Créez un groupe pour les utilisateurs de postes de travail distants de 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**. b Cliquez avec le bouton droit sur votre domaine et cliquez sur **Propriétés**. c Sous l'onglet **Stratégie de groupe**, cliquez sur **Ouvrir** pour ouvrir le plug-in Gestion de stratégie de groupe. 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**. b Développez votre domaine, cliquez avec le bouton droit sur **Stratégie de domaine par défaut** et cliquez sur **Modifier**.

2 Développez la section **Configuration ordinateur** et ouvrez **Paramètres Windows\Paramètres de sécurité**.

3 Cliquez avec le bouton droit sur **Groupes restreints**, sélectionnez **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 distant à la liste d'appartenance au groupe.

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

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

View inclut plusieurs fichiers de modèle d'administration (ADM et ADMX) de stratégie de groupe spécifiques d'un composant.

Tous les fichiers ADM et ADMX fournissant les paramètres de stratégie de groupe pour View sont disponibles dans un fichier `.zip` groupé nommé `VMware-Horizon-View-GPO-Bundle-x.x.x-yyyyyyy.zip`, où *x.x.x* est la version et *yyyyyyy* est le numéro de build. Vous pouvez télécharger le fichier depuis le site de téléchargement de VMware Horizon (avec View) à l'adresse http://www.vmware.com/go/downloadview-fr.

Pour optimiser et sécuriser des postes de travail distants, ajoutez les paramètres de stratégie dans ces fichiers à un nouveau GPO ou un GPO existant dans Active Directory, puis liez ce GPO à l'UO qui contient vos postes de travail.

Reportez-vous au document *Administration de View* et *Configuration de pools de postes de travail et d'applications dans View* pour obtenir des informations sur l'utilisation de paramètres de stratégie de groupe de 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 24

  Comme les ouvertures de session par carte à puce reposent sur des noms d'utilisateur principaux (UPN), les comptes d'utilisateurs et d'administrateurs 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 racines de confiance page 25

  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 Autorités de certification racines 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 26

  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 26

  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 et d'administrateurs 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 **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 racines 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 Autorités de certification racines 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**. b Cliquez avec le bouton droit sur votre domaine et cliquez sur **Propriétés**. c Sous l'onglet **Stratégie de groupe**, cliquez sur **Ouvrir** pour ouvrir le plug-in Gestion de stratégie de groupe. 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**. b Développez votre domaine, cliquez avec le bouton droit sur **Stratégie de domaine par défaut** et cliquez sur **Modifier**.

2 Développez la section **Configuration ordinateur** et ouvrez le dossier **Paramètres Windows\Paramètres de sécurité\Clé publique**.

3 Cliquez avec le bouton droit sur **Autorités de certification racines de confiance** et sélectionnez **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 26.

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**. b Cliquez avec le bouton droit sur votre domaine et cliquez sur **Propriétés**. c Sous l'onglet **Stratégie de groupe**, cliquez sur **Ouvrir** pour ouvrir le plug-in Gestion de stratégie de groupe. 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**. b Développez votre domaine, cliquez avec le bouton droit sur **Stratégie de domaine par défaut** et cliquez sur **Modifier**.

2 Développez la section **Configuration ordinateur** et ouvrez la stratégie de **Paramètres Windows\Paramètres de sécurité\Clé publique**.

3 Cliquez avec le bouton droit sur **Autorités de certification intermédiaires** et sélectionnez **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 28

  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 30

  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 **Démarrer > 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 Explorateur d'objets, cliquez avec le bouton droit sur l'entrée Bases de données et sélectionnez **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 Bases de données dans le volet 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 29.

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 28.

Procédure

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

2 Sélectionnez l'onglet **Nom DSN système**.

3 Cliquez sur **Ajouter** et sélectionnez **SQL Native Client** dans la liste.

4 Cliquez sur **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 **Suivant**.

8 Assurez-vous que la case **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 **Suivant**.

10 Cochez la case **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 **Utiliser le cryptage renforcé pour les données**.

12 Effectuez et fermez l'assistant 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 34.

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 31

  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 31

  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 32

  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 33

  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 **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 **Démarrer > Tous les programmes > Oracle-OraDb11g_home > Outils de configuration et de migration > Assistant de configuration de base de données**.
Oracle 10g	Sélectionnez **Démarrer > Tous les programmes > Oracle-OraDb10g_home > Outils de configuration et de migration > Assistant de configuration de base de données**.

2 Sur la page Opérations, sélectionnez **Créer une base de données**.

3 Sur la page Modèles de base de données, sélectionnez le modèle **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 Options de gestion, cliquez sur **Suivant** pour accepter les réglages par défaut.

6 Sur la page Informations d'identification de la base de données, sélectionnez **Utiliser les mêmes mots de passe d'administration pour tous les comptes** et saisissez un mot de passe.

7 Sur les pages de configuration restantes, cliquez sur **Suivant** pour accepter les réglages par défaut.

8 Sur la page Options de création, vérifiez que **Créer une base de données** est sélectionné et cliquez sur **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 Création de bases 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 33.

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 32.

Suivez les instructions de la section « Ajouter une source de données ODBC à Oracle 11g ou 10g », page 33

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 31 ou « Utiliser une instruction SQL pour ajouter une base de données View Composer à une instance d'Oracle », page 31.

Procédure

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

2 Dans l'assistant Administrateur de sources de données ODBC de Microsoft, sélectionnez l'onglet **Nom DNS système**.

3 Cliquez sur **Ajouter** et sélectionnez le pilote Oracle approprié dans la liste.

Par exemple : **`OraDb11g_home`**

4 Cliquez sur **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 **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 **Tester la connexion** et sur **OK**.

Suivant

Installez le nouveau service View Composer. Reportez-vous à la section « Installer le service View Composer », page 34.

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 6, « Configuration de certificats SSL pour des View Servers », page 69.

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 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 d'View, y compris un serveur réplica, un serveur de sécurité, Serveur de connexion View, View Agent ou Horizon Client.

Prérequis

- Vérifiez que votre installation répond aux 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 6, « Configuration de certificats SSL pour des View Servers », page 69.

- 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/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 **ODBC DSN Setup** 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.

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

8 Fournissez un certificat SSL.

Option	Action
Create default SSL certificate (Créer un certificat SSL par défaut)	Sélectionnez ce bouton radio pour créer un certificat SSL par défaut pour le service View Composer. Après l'installation, vous pouvez remplacer le certificat par défaut par un certificat SSL signé par une autorité de certification.
Use an existing SSL certificate (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 Horizon 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 View Composer Server 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 recommandations lorsque vous installez et configurez vCenter Server, 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 ne parvient pas à rechercher les machines virtuelles dans vCenter Server.

- Assurez-vous que les paramètres vSwitch sur l'hôte ESXi sont configurés avec suffisamment de ports afin de prendre en charge le nombre total de cartes réseau virtuelles configurées sur les machines virtuelles de clone lié exécutées sur l'hôte 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 version ultérieure, un cluster utilisé pour des clones liés View Composer peut contenir plus de 8 hôtes ESXi si les disques de réplica sont stockés sur des magasins de données VMFS5 ou version ultérieure 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 Serveur de connexion View 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 du Serveur de connexion View 5

Pour utiliser le Serveur de connexion View, 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 Serveur de connexion View

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

Lorsque vous installez le Serveur de connexion View, vous sélectionnez un type d'installation.

Installation standard	Génère une instance du Serveur de connexion View avec une nouvelle configuration View LDAP.
Installation de réplica	Génère une instance du Serveur de connexion View avec une configuration View LDAP copiée depuis une instance existante.
Installation de serveur de sécurité	Génère une instance du Serveur de connexion View qui ajoute une couche supplémentaire de sécurité entre Internet et votre réseau interne.

Conditions préalables d'installation pour le Serveur de connexion View

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

- Vous devez disposer d'une clé de licence valide pour View.
- Vous devez associer l'hôte de Serveur de connexion View à un domaine Active Directory. Le Serveur de connexion View prend en charge les niveaux fonctionnels de domaine AD DS (Active Directory Domain Services) suivants :
  - Windows Server 2003
  - Windows Server 2008
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2

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

  Remarque Le Serveur de connexion View ne fait ni ne requiert de mises à jour de schéma ou de configuration pour Active Directory.
- N'installez pas le 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 le Serveur de connexion View.
- N'installez pas le 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 le 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 le Serveur de connexion View avec une nouvelle configuration

Pour installer le 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 de 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 de View LDAP à l'aide de View Administrator. Le Serveur de connexion View conserve automatiquement certaines entrées de View LDAP.

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

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 permettant d'identifier votre organisation 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 View*.

Par défaut, le composant HTML Access est installé sur l'hôte du Serveur de connexion View lorsque vous installez Serveur de connexion View. Ce composant configure la page du portail utilisateur d'View pour afficher une icône d'HTML Access en plus de l'icône d'Horizon Client. L'icône supplémentaire permet aux utilisateurs de sélectionner HTML Access lorsqu'ils se connectent à leurs postes de travail.

Pour obtenir une présentation de la configuration du Serveur de connexion View pour HTML Access, consultez « Préparation du Serveur de connexion View et des serveurs de sécurité pour HTML Access » dans le document *Utilisation de HTML Access*, situé sur la page de documentation d'Horizon Client.

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 le Serveur de connexion View.
- Vérifiez que votre installation satisfait aux exigences décrites dans la section « Exigences de Serveur de connexion View », page 7
- Préparez votre environnement pour l'installation. Reportez-vous à la section « Conditions préalables d'installation pour le Serveur de connexion View », page 40.
- 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 de 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 du Serveur de connexion View sur la page de produits VMware à l'adresse http://www.vmware.com/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 de **Serveur standard View**.

6 Vérifiez que l'option **Installer HTML Access** est sélectionnée si vous prévoyez d'autoriser les utilisateurs à se connecter à leurs postes de travail à l'aide d'HTML Access.

Ce paramètre est sélectionné par défaut.

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

8 Choisissez comment configurer le service Pare-feu Windows.

Option	Action
Configure Windows Firewall automatically (Configurer le Pare-feu Windows automatiquement)	Laissez le programme d'installation configurer le Pare-feu Windows pour autoriser les connexions réseau requises.
Do not configure Windows Firewall (Ne pas configurer le Pare-feu Windows)	Configurez les règles de pare-feu Windows manuellement. Sélectionnez cette option uniquement si votre entreprise utilise ses propres règles prédéfinies pour la configuration du pare-feu Windows.

9 Autorisez un compte de View Administrators.

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

Option	Description
Authorize the local Administrators group (Autoriser le groupe d'administrateurs local)	Permet aux utilisateurs du groupe d'administrateurs local d'administrer View.
Authorize a specific domain user or domain group (Autoriser un utilisateur ou un groupe de domaine spécifique)	Permet à l'utilisateur ou au groupe de domaine spécifié d'administrer View.

10 Si vous avez spécifié un compte d'administrateurs de domaine View 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*.

11 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.

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

13 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 VMware Horizon View
- Composant de VMware Horizon View Framework
- Composant du bus de message VMware Horizon View
- Hôte de script VMware Horizon View
- Composant VMware Horizon View Security Gateway
- VMware Horizon View PCoIP Secure Gateway
- VMware Horizon View Blast Secure Gateway
- Composant Web VMware Horizon View
- VMware VDMDS, qui fournit des services d'annuaire View LDAP

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

Si le paramètre **Installer HTML Access** a été sélectionné pendant l'installation, le composant HTML Access est installé sur l'ordinateur Windows Server. Ce composant configure l'icône d'HTML Access sur la page du portail utilisateur View et active la règle **Serveur de connexion VMware Horizon View (Blast-In)** dans le pare-feu Windows. Cette règle de pare-feu permet aux navigateurs Web sur les périphériques client de se connecter au Serveur de connexion View sur le port TCP 8443.

Suivant

Configurez des certificats de serveur SSL pour le Serveur de connexion View. Reportez-vous à la section Chapitre 6, « Configuration de certificats SSL pour des View Servers », page 69.

Effectuez la configuration initiale sur le Serveur de connexion View. Reportez-vous à la section Chapitre 7, « Configuration d'View pour la première fois », page 91.

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 et que vous possédez un ensemble de collecteur de données configuré pour contrôler les données de performances, arrêtez l'ensemble de collecteur de données et redémarrez-le.

Installer le 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 le Serveur de connexion View.
- Vérifiez que votre installation satisfait aux exigences décrites dans la section « Exigences de Serveur de connexion View », page 7
- Préparez votre environnement pour l'installation. Reportez-vous à la section « Conditions préalables d'installation pour le Serveur de connexion View », page 40.
- 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 le 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 la 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 46.

Procédure

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

- Serveur de connexion VMware Horizon View
- Composant de VMware Horizon View Framework
- Composant du bus de message VMware Horizon View
- Hôte de script VMware Horizon View
- Composant VMware Horizon View Security Gateway
- VMware Horizon View PCoIP Secure Gateway
- VMware Horizon View Blast Secure Gateway
- Composant Web VMware Horizon View
- VMware VDMDS, qui fournit des services d'annuaire View LDAP

Si le paramètre **Installer HTML Access** a été sélectionné pendant l'installation, le composant HTML Access est installé sur l'ordinateur Windows Server. Ce composant configure l'icône d'HTML Access sur la page du portail utilisateur View et active la règle **Serveur de connexion VMware Horizon View (Blast-In)** dans le pare-feu Windows. Cette règle de pare-feu permet aux navigateurs Web sur les périphériques client de se connecter au Serveur de connexion View sur le port TCP 8443.

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

Suivant

Configurez des certificats de serveur SSL pour le Serveur de connexion View. Reportez-vous à la section Chapitre 6, « Configuration de certificats SSL pour des View Servers », page 69.

Si vous configurez View pour la première fois, effectuez la configuration initiale sur Serveur de connexion View. Reportez-vous à la section Chapitre 7, « Configuration d'View pour la première fois », page 91.

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 la forme *Propriété=valeur* de manière 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. Par exemple : `INSTALLDIR=""D:\abc\my folder""` Les guillemets délimitant le chemin permettent au programme d'installation MSI d'interpréter l'espace comme étant une partie valide du chemin.	`%ProgramFiles %\VMware\VMware View\Server`
VDM_SERVER_ INSTANCE_TYPE	Type d'installation de View server : ■ **1**. Installation standard ■ **2**. Installation de réplica ■ **3**. Installation d'un serveur de sécurité 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. Une valeur de 1 configure un pare-feu. Une valeur de 2 ne configure pas un pare-feu. 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. La valeur par défaut est le SID du groupe d'administrateurs local sur l'ordinateur de 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. 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.	Aucune
VDM_SERVER_RECOVERY_ PWD_REMINDER	Rappel du mot de passe de récupération de données. Cette propriété est facultative.	Aucune

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 copie les données de configuration de View LDAP depuis l'instance de Serveur de connexion View existante.

Après l'installation, les données de configuration de View LDAP identiques sont conservées sur toutes les instances du Serveur de connexion View du 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 une machine virtuelle ou physique sur laquelle sont installés d'autres composants logiciels d'View, notamment un serveur de sécurité, Serveur de connexion View, View Composer, View Agent ou Horizon Client.

Par défaut, le composant HTML Access est installé sur l'hôte du Serveur de connexion View lorsque vous installez Serveur de connexion View. Ce composant configure la page du portail utilisateur d'View pour afficher une icône d'HTML Access en plus de l'icône d'Horizon Client. L'icône supplémentaire permet aux utilisateurs de sélectionner HTML Access lorsqu'ils se connectent à leurs postes de travail.

Pour obtenir une présentation de la configuration du Serveur de connexion View pour HTML Access, consultez « Préparation du Serveur de connexion View et des serveurs de sécurité pour HTML Access » dans le document *Utilisation de HTML Access*, situé sur la page de documentation d'Horizon Client.

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 d'administrateur d'View. Vous spécifiez le compte ou le groupe avec le rôle d'administrateur d'View lorsque vous installez la première instance du 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 le Serveur de connexion View avec une nouvelle configuration », page 40.
- Si l'instance du 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 d'administrateur d'View 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 aux exigences décrites dans la section « Exigences de Serveur de connexion View », 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 le Serveur de connexion View », page 40.
- Si vous installez une instance de Serveur de connexion View répliquée correspondant à View 5.1 ou version ultérieure et que l'instance du Serveur de connexion View existante que vous répliquez correspond à View 5.0.*x* ou version antérieure, préparez un mot de passe de récupération de données. Reportez-vous à la section « Installer le Serveur de connexion View avec une nouvelle configuration », page 40.
- 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 du Serveur de connexion View sur la page de produits VMware à l'adresse http://www.vmware.com/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 de **Serveur réplica View**.

6 Vérifiez que l'option **Installer HTML Access** est sélectionnée si vous prévoyez d'autoriser les utilisateurs à se connecter à leurs postes de travail à l'aide d'HTML Access.

Ce paramètre est sélectionné par défaut.

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

8 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 du Serveur de connexion View existante que vous répliquez correspond à View 5.0.*x* ou version antérieure.

9 Choisissez comment configurer le service Pare-feu Windows.

Option	Action
Configure Windows Firewall automatically (Configurer le Pare-feu Windows automatiquement)	Laissez le programme d'installation configurer le Pare-feu Windows pour autoriser les connexions réseau requises.
Do not configure Windows Firewall (Ne pas configurer le Pare-feu Windows)	Configurez les règles de pare-feu Windows manuellement. Sélectionnez cette option uniquement si votre entreprise utilise ses propres règles prédéfinies pour la configuration du pare-feu Windows.

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

11 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 VMware Horizon View

- Composant de VMware Horizon View Framework
- Composant du bus de message VMware Horizon View
- Hôte de script VMware Horizon View
- Composant VMware Horizon View Security Gateway
- VMware Horizon View PCoIP Secure Gateway
- VMware Horizon View Blast Secure Gateway
- Composant Web VMware Horizon View
- VMware VDMDS, qui fournit des services d'annuaire View LDAP

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

Si le paramètre **Installer HTML Access** a été sélectionné pendant l'installation, le composant HTML Access est installé sur l'ordinateur Windows Server. Ce composant configure l'icône d'HTML Access sur la page du portail utilisateur View et active la règle **Serveur de connexion VMware Horizon View (Blast-In)** dans le pare-feu Windows. Cette règle de pare-feu permet aux navigateurs Web sur les périphériques client de se connecter au Serveur de connexion View sur le port TCP 8443.

Suivant

Configurez un certificat de serveur SSL pour l'instance de Serveur de connexion View. Reportez-vous à la section Chapitre 6, « Configuration de certificats SSL pour des View Servers », page 69.

Il n'est pas nécessaire d'effectuer de configuration initiale d'View sur une instance répliquée du 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 des connexions Horizon Client », page 106 et « Dimensionnement de paramètres de Windows Server pour prendre en charge votre déploiement », page 116.

Si vous réinstallez Serveur de connexion View et que vous possédez un ensemble de collecteur de données configuré pour contrôler les données de performances, arrêtez l'ensemble de collecteur de données et redémarrez-le.

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 le Serveur de connexion View avec une nouvelle configuration », page 40.

- 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 aux exigences décrites dans la section « Exigences de Serveur de connexion View », 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 le Serveur de connexion View », page 40.
- 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.
- Familiarisez-vous avec les options de ligne de commande du programme d'installation MSI. Reportez-vous à la section « Options de la 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 du Serveur de connexion View sur la page de produits VMware à l'adresse http://www.vmware.com/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 :

- Serveur de connexion VMware Horizon View
- Composant de VMware Horizon View Framework
- Composant du bus de message VMware Horizon View
- Hôte de script VMware Horizon View
- Composant VMware Horizon View Security Gateway
- VMware Horizon View PCoIP Secure Gateway
- VMware Horizon View Blast Secure Gateway
- Composant Web VMware Horizon View
- VMware VDMDS, qui fournit des services d'annuaire View LDAP

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

Si le paramètre **Installer HTML Access** a été sélectionné pendant l'installation, le composant HTML Access est installé sur l'ordinateur Windows Server. Ce composant configure l'icône d'HTML Access sur la page du portail utilisateur View et active la règle **Serveur de connexion VMware Horizon View (Blast-In)** dans le pare-feu Windows. Cette règle de pare-feu permet aux navigateurs Web sur les périphériques client de se connecter au Serveur de connexion View sur le port TCP 8443.

Suivant

Configurez un certificat de serveur SSL pour l'instance de Serveur de connexion View. Reportez-vous à la section Chapitre 6, « Configuration de certificats SSL pour des View Servers », page 69.

Il n'est pas nécessaire d'effectuer de configuration initiale d'View sur une instance répliquée du 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 des connexions Horizon Client », page 106 et « Dimensionnement de paramètres de Windows Server pour prendre en charge votre déploiement », page 116.

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 la forme *`Propriété=valeur`* de manière 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. Par exemple : `INSTALLDIR=""D:\abc\my folder""` Les guillemets délimitant le chemin permettent au programme d'installation MSI d'interpréter l'espace comme étant une partie valide du chemin. Cette propriété MSI est facultative.	`%ProgramFiles %\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	Type d'installation de View server : ■ **1**. Installation standard ■ **2**. Installation de réplica ■ **3**. Installation d'un serveur de sécurité Pour installer une instance répliquée, définissez `VDM_SERVER_INSTANCE_TYPE=2` 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. Par exemple : `ADAM_PRIMARY_NAME=cs1.companydomain.com` Cette propriété MSI est requise.	Aucune
ADAM_PRIMARY_PORT	Port View LDAP de l'instance de Serveur de connexion View existante que vous répliquez. Par exemple : `ADAM_PRIMARY_PORT=cs1.companydomain.com` Cette propriété MSI est facultative.	Aucune
FWCHOICE	Propriété MSI qui détermine de configurer un pare-feu pour l'instance de Serveur de connexion View. Une valeur de 1 configure un pare-feu. Une valeur de 2 ne configure pas un pare-feu. Par exemple : `FWCHOICE=1` 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. **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. 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.	Aucune
VDM_SERVER_RECOVERY_ PWD_REMINDER	Rappel du mot de passe de récupération de données. Cette propriété est facultative.	Aucune

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 d'View, y compris un serveur réplica, Serveur de connexion View, View Composer, View Agent ou Horizon Client.

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 *Planification de l'architecture de View*.

  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 aux exigences décrites dans la section « Exigences de Serveur de connexion View », page 7
- Préparez votre environnement pour l'installation. Reportez-vous à la section « Conditions préalables d'installation pour le Serveur de connexion View », page 40.
- 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 View » dans le document *Mises à niveau 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 108.
- 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 du Serveur de connexion View sur la page de produits VMware à l'adresse http://www.vmware.com/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 de **Serveur de sécurité View**.

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 Tapez le mot de passe de couplage du 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 le saisir dans le programme d'installation.

8 Dans la zone de texte **URL externe**, tapez l'URL externe du serveur de sécurité pour les points de terminaison 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.example.com:443`

9 Dans la zone de texte **URL externe PCoIP**, tapez l'URL externe du serveur de sécurité pour les points de terminaison 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 HTML Access pour se connecter à des postes de travail distants.

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
Configure Windows Firewall automatically (Configurer le Pare-feu Windows automatiquement)	Laissez le programme d'installation configurer le Pare-feu Windows pour autoriser les connexions réseau requises.
Do not configure Windows Firewall (Ne pas configurer le Pare-feu Windows)	Configurez les règles de pare-feu Windows manuellement. 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 Horizon View
- Composant de VMware Horizon View Framework
- Composant VMware Horizon View Security Gateway
- VMware Horizon View PCoIP Secure Gateway
- VMware Blast Secure Gateway

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

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

La règle **Serveur de connexion VMware Horizon View (Blast-In)** est activée sur le pare-feu Windows sur le serveur de sécurité. Cette règle de pare-feu permet aux navigateurs Web sur les périphériques client d'utiliser HTML Access pour se connecter au serveur de sécurité sur le port TCP 8443.

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 6, « Configuration de certificats SSL pour des View Servers », page 69.

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 des connexions Horizon Client », page 106 et « Dimensionnement de paramètres de Windows Server pour prendre en charge votre déploiement », page 116.

Si vous réinstallez le serveur de sécurité et que vous possédez un ensemble de collecteur de données pour contrôler les données de performances, arrêtez l'ensemble de collecteur de données et redémarrez-le.

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.

L'installation silencieuse vous permet de déployer efficacement des composants View dans une entreprise de grande taille.

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 *Planification de l'architecture de View*.

  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 aux exigences décrites dans la section « Exigences de Serveur de connexion View », page 7
- Préparez votre environnement pour l'installation. Reportez-vous à la section « Conditions préalables d'installation pour le Serveur de connexion View », page 40.
- 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 View » dans le document *Mises à niveau 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 108.
- 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 la 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 du Serveur de connexion View sur la page de produits VMware à l'adresse http://www.vmware.com/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 du serveur de sécurité sont installés sur l'ordinateur Windows Server :

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

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

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

La règle **Serveur de connexion VMware Horizon View (Blast-In)** est activée sur le pare-feu Windows sur le serveur de sécurité. Cette règle de pare-feu permet aux navigateurs Web sur les périphériques client d'utiliser HTML Access pour se connecter au serveur de sécurité sur le port TCP 8443.

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 6, « Configuration de certificats SSL pour des View Servers », page 69.

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 des connexions Horizon Client », page 106 et « Dimensionnement de paramètres de Windows Server pour prendre en charge votre déploiement », page 116.

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 la forme *Propriété=valeur* de manière 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. Par exemple : `INSTALLDIR=""D:\abc\my folder""` Les guillemets délimitant le chemin permettent au programme d'installation MSI d'interpréter l'espace comme étant une partie valide du chemin. Cette propriété MSI est facultative.	`%ProgramFiles %\VMware\VMware View\Server`
VDM_SERVER_INSTANCE_TYPE	Type d'installation de View server : ■ **1**. Installation standard ■ **2**. Installation de réplica ■ **3**. Installation d'un serveur de sécurité Pour installer un serveur de sécurité, définissez `VDM_SERVER_INSTANCE_TYPE=3` 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. Par exemple : `VDM_SERVER_NAME=cs1.internaldomain.com` Cette propriété MSI est requise.	Aucune
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. Par exemple : `VDM_SERVER_SS_EXTURL=https://view.companydomain.com:443` Cette propriété MSI est requise.	Aucune
VDM_SERVER_SS_PWD	Mot de passe de couplage de serveur de sécurité. Par exemple : `VDM_SERVER_SS_PWD=secret` Cette propriété MSI est requise.	Aucune
FWCHOICE	Propriété MSI qui détermine de configurer un pare-feu pour l'instance de Serveur de connexion View. Une valeur de 1 configure un pare-feu. Une valeur de 2 ne configure pas un pare-feu. Par exemple : `FWCHOICE=1` 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. Par exemple : `VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40` Cette propriété est requise si vous prévoyez d'utiliser le composant PCoIP Secure Gateway.	Aucune
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. Par exemple : `VDM_SERVER_SS_PCOIP_TCPPORT=4172` Cette propriété est requise si vous prévoyez d'utiliser le composant PCoIP Secure Gateway.	Aucune

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

Propriété MSI	Description	Valeur par défaut
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. Par exemple : `VDM_SERVER_SS_PCOIP_UDPPORT=4172` Cette propriété est requise si vous prévoyez d'utiliser le composant PCoIP Secure Gateway.	Aucune
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. Par exemple : `VDM_SERVER_SS_BSG_EXTURL=https://view.companydomain.com:8443` 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.	Aucune
VDM_SERVER_SS_FORCE_IPSEC	Force l'utilisation d'IPsec entre le serveur de sécurité et son instance de Serveur de connexion View couplée. 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. 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 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 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 le Serveur de connexion View, le programme d'installation peut éventuellement configurer 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 Horizon Client de se connecter à View via les ports mis à jour.

Si vous choisissez d'installer HTML Access avec le Serveur de connexion View, le programme d'installation configure la règle **Serveur de connexion VMware Horizon View (Blast-In)** dans le Pare-feu Windows pour ouvrir le port TCP 8443, utilisé par HTML Access.

Le tableau suivant répertorie les ports par défaut pouvant être ouverts automatiquement lors de l'installation. Les ports sont entrants sauf indication contraire.

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	Standard et réplica
JMSIR	TCP 4100	Standard et réplica
AJP13	TCP 8009	Standard et réplica
HTTP	TCP 80	Standard, réplica et serveur de sécurité
HTTPS	TCP 443	Standard, réplica et serveur de sécurité
PCoIP	TCP 4172 entrant ; UDP 4172 dans les 2 sens	Standard, réplica et serveur de sécurité
HTTPS	TCP 8443	Standard, réplica et serveur de sécurité. Une fois la connexion initiale à View établie, le navigateur Web d'un périphérique client se connecte à Blast Secure Gateway sur le port TCP 8443. Blast Secure Gateway doit être activé sur un serveur de sécurité ou sur une instance du Serveur de connexion View pour autoriser l'établissement de cette deuxième connexion.
HTTPS	TCP 8472	Standard et réplica Pour la fonctionnalité Cloud Pod Architecture : utilisé pour la communication entre les espaces.
HTTP	TCP 22389	Standard et réplica Pour la fonctionnalité Cloud Pod Architecture : utilisé pour la réplication LDAP globale.
HTTPS	TCP 22636	Standard et réplica Pour la fonctionnalité Cloud Pod Architecture : utilisé pour la réplication LDAP sécurisée globale.

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 **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. 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 de View existante en important un fichier LDIF de sauvegarde contenant les données de configuration de 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 de 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 de 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 de View LDAP à partir de l'autre instance.

Prérequis

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

  Consultez « Sauvegarde et restauration des données de configuration de View » dans le document *Administration de View*.

- Familiarisez-vous avec les étapes d'installation d'une nouvelle instance de Serveur de connexion View. Reportez-vous à la section « Installer le Serveur de connexion View avec une nouvelle configuration », page 40.

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 de View LDAP.

Par exemple :

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

Remarque À ce stade, la configuration de View n'est pas encore accessible. Les clients 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 de 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 la 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.

Pour plus d'informations sur MSI, rendez-vous sur le site Web de Microsoft. Pour plus d'informations sur les options de la ligne de commande MSI, rendez-vous sur le site Web de la bibliothèque MSDN (Microsoft Developer Network). 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 mode silencieux, commencez par activer le mode silencieux sur le programme de démarrage qui extrait le programme d'installation dans un répertoire temporaire et démarre une installation interactive.

Vous devez entrer sur la ligne de commande les options 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 du programme de démarrage, qui empêche l'affichage de boîtes de dialogue interactives. Par exemple : VMware-viewconnectionserver-*y.y.y-xxxxxx*.exe /s L'option /s est obligatoire pour que l'installation soit silencieuse.
/v"*MSI_command_line_options*"	Demande au programme d'installation de transmettre à MSI la chaîne de caractères comprise entre guillemets, que vous avez entrée sur la ligne de commande comme un ensemble d'options à interpréter. Vous devez délimiter votre chaîne de caractères de la ligne de commande par des guillemets. Placez un guillemet après /v et à la fin de la ligne de commande. Par exemple : VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"*command_line_options*" 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. Par exemple : VMware-viewconnectionserver-*y.y.y-xxxxxx*.exe /s /v"*command_line_options* INSTALLDIR=""d:\abc\my folder""" 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. L'option /v"*command_line_options*" est obligatoire pour exécuter une installation silencieuse.

Le contrôle de la suite de l'installation silencieuse se fait en transmettant les options de la ligne de commande et les 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 propres au composant View.

Tableau 5-8. Options de la ligne de commande 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. Par exemple, vous voulez peut-être installer View Agent en silence et n'utiliser que des options et des fonctions d'installation par défaut : VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn" Vous pouvez également utiliser l'option /qb pour afficher les pages de l'assistant d'installation dans une installation automatique non interactive. Pendant l'installation, les pages de l'assistant d'installation sont affichées, mais vous ne pouvez pas y répondre. L'option /qn ou /qb est obligatoire pour que l'installation soit silencieuse.
INSTALLDIR	Spécifie un autre chemin d'installation pour le composant View. 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. Cette propriété MSI est facultative.

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

Option ou propriété MSI	Description
ADDLOCAL	Détermine les fonctionnalités spécifiques du composant à installer. Dans une installation interactive, le programme d'installation de View affiche des options d'installation personnalisée à sélectionner et installe d'autres fonctionnalités automatiquement. La propriété ADDLOCAL vous permet de spécifier ces options et fonctionnalités sur la ligne de commande. Vous pouvez utiliser ADDLOCAL pour installer de manière sélective les options et fonctionnalités d'installation individuelle. Les fonctionnalités que vous ne spécifiez pas explicitement ne sont pas installées. Tapez ADDLOCAL=ALL pour installer toutes les fonctionnalités installées automatiquement (sur les systèmes d'exploitation invités pris en charge) et toutes les options d'installation personnalisée qui sont installées par défaut. Par exemple : VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=ALL" Les options d'installation par défaut et les fonctionnalités installées automatiquement seront installées si vous n'utilisez pas la propriété ADDLOCAL. Taper ADDLOCAL=ALL sans utiliser la propriété ADDLOCAL aboutit au même résultat. Pour spécifier des options et fonctionnalités d'installation individuelles, tapez une liste séparée par des virgules de noms d'option d'installation. Ne laissez pas d'espaces entre les noms. Utilisez le format ADDLOCAL=*valeur*,*valeur*,*valeur*.... Contrairement à une installation interactive, cette méthode installe uniquement les fonctionnalités spécifiées. Par exemple, vous voulez peut-être installer View Agent dans un système d'exploitation client avec les fonctions View Composer Agent et PCoIP : VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=Core,SVIAgent,PCoIP" **IMPORTANT** La fonctionnalité Core est requise si vous spécifiez des fonctionnalités individuelles avec ADDLOCAL=*value*,*value*,*value*.... La propriété MSI ADDLOCAL est facultative.
REBOOT	Vous pouvez utiliser l'option REBOOT=ReallySuppress pour autoriser l'exécution de tâches de configuration système avant le redémarrage du système. Cette propriété MSI est facultative.
/l*v *log_file*	Écrit des informations de journalisation dans le fichier journal spécifié avec une sortie détaillée. Par exemple : /l*v ""%TEMP%\vmmsi.log"" Cet exemple génère un fichier journal détaillé semblable à celui généré lors d'une installation interactive. Vous pouvez utiliser cette option pour enregistrer des fonctions personnalisées qui s'appliquent uniquement à votre installation. Vous pouvez utiliser les informations enregistrées pour spécifier les fonctionnalités d'installation lors d'installations silencieuses ultérieures. L'option /l*v est facultative.

Désinstallation silencieuse de composants 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 la ligne de commande Microsoft Windows Installer », page 64

Exemples

Désinstallez une instance de Serveur de connexion View.

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

Configuration de certificats SSL pour des View Servers

6

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 clientes à un serveur. 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 le serveur. 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 version ultérieure 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 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 83.

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 un serveur par un certificat signé par une autorité de certification, BSG utilise également le certificat signé par une autorité de certification.

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 Workspace est configuré pour prendre en charge View, les utilisateurs de Workspace peuvent se connecter à des postes de travail distants en sélectionnant des icônes de poste de travail sur le portail utilisateur d'Horizon.

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 à utiliser des certificats SSL signés par une autorité de certification », page 88.

Lorsque des points de terminaison clients se connectent à une instance de Serveur de connexion View ou à un serveur de sécurité, ils se voient présenter le certificat de serveur SSL du serveur 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 Server, 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.

Dans un espace d'instances de Serveur de connexion View répliquées, vous devez effectuer les tâches suivantes sur toutes les instances de l'espace.

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.

En outre, si les instances de Serveur de connexion View n'approuvent 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. Effectuez ces étapes 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 dans le serveur View Server, ils doivent être configurés pour les clients 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 clients 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 est configuré pour être utilisé avec une instance de Serveur de connexion View, celui-ci effectue également la vérification de la révocation de certificat sur le certificat du serveur SAML.

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.

Reportez-vous au document *Scénarios de configuration de certificats SSL pour View* pour voir un exemple indiquant comment utiliser `certreq` pour accomplir 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 à l'aide d'un modèle de certificat compatible uniquement avec une autorité de certification d'entreprise Windows Server 2008 ou version ultérieure.

IMPORTANT Ne générez pas de certificats pour des serveurs avec une valeur `KeyLength` inférieure à 1 024. Les points de terminaison clients ne valideront pas un certificat sur un serveur qui a été généré avec une valeur `KeyLength` inférieure à 1 024, et les clients ne parviendront pas à se connecter au serveur. Les validations de certificats exécutées par Serveur de connexion View échoueront également ; les serveurs affectés s'afficheront 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 75.

Obtenir un certificat signé auprès 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 Inscription de certificats Windows du magasin de certificats Windows.

Cette méthode de demande de certificat est appropriée si les communications entre les ordinateurs s'effectuent au sein de votre domaine interne. Par exemple, l'obtention d'un certificat signé auprès d'une autorité de certification de domaine Windows peut convenir pour des communications de serveur à serveur.

Si vos clients se connectent à des serveurs View Server à partir d'un réseau externe, demandez des certificats de serveur SSL qui sont signés par une autorité de certification tierce approuvée.

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 75.
- Vérifiez que vous disposez des informations d'identification appropriées pour demander un certificat pouvant être envoyé à un ordinateur ou à un service.

Procédure

1. Dans la fenêtre MMC sur l'hôte Windows Server, développez le nœud **Certificats (ordinateur local)** et sélectionnez le dossier **Personnel**.
2. Dans le menu **Action**, accédez à **Toutes les tâches > Demander un nouveau certificat** pour afficher l'assistant Inscription de certificats.
3. Sélectionnez une stratégie d'inscription de certificats.
4. Sélectionnez les certificats que vous souhaitez demander, choisissez l'option **Permettre l'exportation de la clé privée**, puis cliquez sur **Inscrire**.
5. Cliquez sur **Terminer**.

Le nouveau certificat signé est ajouté au dossier **Personnel > Certificats** dans le magasin de certificats Windows.

Suivant

- Vérifiez que le certificat et la chaîne de certificats de serveur ont été importés dans le magasin de certificats Windows.
- Pour une instance du Serveur de connexion View ou un serveur de sécurité, remplacez le nom convivial du certificat par **vdm**. Reportez-vous à la section « Modifier le nom convivial du certificat », page 76.
- Pour un serveur View Composer Server, liez le nouveau certificat au port qui est utilisé par View Composer. Reportez-vous à la section « Lier un nouveau certificat SSL au port utilisé par View Composer », page 78.

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.

Dans un espace d'instances répliquées du Serveur de connexion View, vous devez importer le certificat et la chaîne de certificats de serveur sur toutes les instances de l'espace.

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 75

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 75

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 ou le service du serveur de sécurité est installé.

3 Modifier le nom convivial du certificat page 76

Pour configurer une instance de Serveur de connexion View ou un serveur de sécurité pour qu'ils reconnaissent et utilisent un certificat SSL, vous devez remplacer le nom convivial du certificat par `vdm`.

4 Importer un certificat racine et des certificats intermédiaires dans un magasin de certificats Windows page 77

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 78

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 **Démarrer** et tapez **`mmc.exe`**.

2 Dans la fenêtre MMC, accédez à **Fichier > Ajouter/Supprimer un composant logiciel enfichable**.

3 Dans la fenêtre Ajouter ou supprimer des composants logiciels enfichables, sélectionnez **Certificats** et cliquez sur **Ajouter**.

4 Dans la fenêtre Composant logiciel enfichable Certificats, sélectionnez **Compte d'ordinateur**, cliquez sur **Suivant**, sélectionnez **Compte d'ordinateur**, puis cliquez sur **Terminer**.

5 Dans la fenêtre 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 ou le service du serveur de sécurité est installé.

Vous devez également effectuer cette tâche sur l'hôte Windows Server où 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, reportez-vous à la section « Décharger des connexions SSL sur des serveurs intermédiaires » dans le document *Administration de View*.

Prérequis

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 75.

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 étendues**.

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

Le nouveau certificat s'affiche 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 du certificat

Pour configurer une instance de Serveur de connexion View ou un serveur de sécurité pour qu'ils reconnaissent et utilisent un certificat SSL, vous devez remplacer le nom convivial du certificat par `vdm`.

Vous n'avez pas à modifier le nom convivial des certificats SSL qui sont utilisés par View Composer.

Prérequis

Vérifiez que le certificat du serveur est importé dans le dossier **Certificats (ordinateur local) > Personnel > 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 75.

Procédure

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

2 Cliquez avec le bouton droit sur le certificat qui est émis sur l'hôte de View Server, puis cliquez sur **Propriétés**.

3 Dans l'onglet Général, supprimez le texte **Nom convivial** et entrez **vdm**.

4 Cliquez sur **Appliquer** puis sur **OK**.

5 Vérifiez qu'aucun autre certificat de serveur dans le dossier **Personnel > Certificats** ne porte le nom convivial **vdm**.

   a Localisez tout autre certificat de serveur, cliquez avec le bouton droit sur le certificat, puis cliquez sur **Propriétés**.

   b Si le certificat porte le nom convivial **vdm**, supprimez le nom, cliquez sur **Appliquer**, puis sur **OK**.

Suivant

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

Une fois que tous les certificats de la chaîne ont été importés, vous devez redémarrer le service de Serveur de connexion View ou du serveur de sécurité pour que vos modifications prennent effet.

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.

Vous devez importer les certificats racine non approuvés dans toutes les instances du Serveur de connexion View répliquées d'un espace.

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 du Serveur de connexion View ou du serveur de sécurité, ils doivent être configurés pour les clients 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 est configuré pour être utilisé par une instance du Serveur de connexion View, les mêmes recommandations s'appliquent à l'authentificateur SAML 2.0. Si l'hôte du Serveur de connexion View n'approuve pas le certificat racine configuré pour un authentificateur SAML, ou si le certificat de serveur SAML 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 accédez au dossier **Autorités de certification racines 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 racines 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 points de terminaison clients pour approuver des certificats racine et intermédiaires

Si un certificat d'View Server est signé par une autorité de certification qui n'est pas approuvée par des ordinateurs clients et que des ordinateurs client accèdent à View Administrator, vous pouvez configurer tous les systèmes clients Windows d'un domaine afin qu'ils approuvent les certificats racine et intermédiaires. Pour cela, vous devez ajouter la clé publique du certificat racine à la stratégie de groupe Autorités de certification racines 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 serveur 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 périphériques clients exécutés sur d'autres systèmes d'exploitation que Windows, lisez les instructions suivantes sur la distribution des certificats racine et intermédiaires que les utilisateurs peuvent installer :

- Pour Horizon Client pour Mac OS X, consultez « Configurer Horizon Client pour Mac OS X pour approuver des certificats racine et intermédiaires », page 81.
- Pour Horizon Client pour iOS, consultez « Configurer Horizon Client pour qu'iOS approuve les certificats d'approbation racine et intermédiaires », page 81.

- Pour Horizon Client pour Android, consultez la documentation sur le site Web de Google, notamment le *Guide d'utilisation d'Android 3.0*
- Pour Horizon Client pour Linux, consultez la documentation Ubuntu

Prérequis

Vérifiez que le certificat du serveur a été généré avec une valeur `KeyLength` de 1 024 ou plus. Les points de terminaison clients ne valideront pas un certificat sur un serveur généré avec une valeur de `KeyLength` inférieure à 1 024, et les clients ne parviendront pas à se connecter au serveur.

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**. b Cliquez avec le bouton droit sur votre domaine et cliquez sur **Propriétés**. c Sous l'onglet **Stratégie de groupe**, cliquez sur **Ouvrir** pour ouvrir le plug-in Gestion de stratégie de groupe. 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**. 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 racines de confiance** et sélectionnez **Importer**. 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**. 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 Horizon Client pour Mac OS X pour approuver des certificats racine et intermédiaires

Si un certificat de serveur est signé par une autorité de certification qui n'est pas approuvée par des ordinateurs qui exécutent Horizon Client pour Mac OS X, vous pouvez configurer ces ordinateurs pour qu'ils approuvent les certificats racine et intermédiaires. Vous devez distribuer le certificat racine et tous les certificats intermédiaires de la chaîne d'approbation aux ordinateurs clients.

Procédure

1 Livrez le certificat racine et les certificats intermédiaires à l'ordinateur qui exécute Horizon Client pour Mac OS X.

2 Ouvrez le certificat racine sur l'ordinateur Mac OS X.

Le certificat affiche le message suivant : `Souhaitez-vous que votre ordinateur approuve les certificats signés par CA name à partir de maintenant ?`

3 Cliquez sur **Toujours approuver**

4 Tapez le mot de passe de l'utilisateur.

5 Répétez les étapes 2 à 4 pour les certificats intermédiaires dans la chaîne d'approbation.

Configurer Horizon Client pour qu'iOS approuve les certificats d'approbation racine et intermédiaires

Si un certificat de serveur est signé par une autorité de certification qui n'est pas approuvée par les iPads et les iPhones qui exécutent Horizon Client pour iOS, vous pouvez configurer le périphérique afin qu'il approuve les certificats racine et intermédiaires. Vous devez distribuer tous les certificats racine et intermédiaires dans la chaîne d'approbation vers les périphériques

Procédure

1 Envoyez les certificats racine et intermédiaires en tant que pièces jointes d'e-mail vers l'iPad.

2 Ouvrez la pièce jointe de l'e-mail pour chercher le certificat racine et sélectionnez **Installer**.

Le certificat affiche le message suivant :

```
Profil invérifiable. Impossible de vérifier l'authenticité de <varname
id="varname_805A68D3161D43FC915F64D02B50AAB3">Certificate name</varname>. L'installation de
ce profil modifiera les paramètres de votre iPad.

Certificat racine. L'installation du certificat <varname
id="varname_9C50C6DC3D644E2A8CD5252B3B97AE41">Certificate name</varname> l'ajoutera à la
liste des certificats approuvés sur votre iPad.
```

3 Sélectionnez **Installer** à nouveau.

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 Server et View Composer Server 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. Le serveur 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, le serveur 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 le serveur, 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 serveur 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 devrez peut-être configurer vos ordinateurs Serveur de connexion View pour qu'ils utilisent les paramètres proxy afin de s'assurer 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 utilisées pour des connexions clientes 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, reportez-vous à « Résolution de la vérification de la révocation des certificats du serveur de sécurité » dans le document *Administration de 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 ultérieures, 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 Horizon Client 2.0 (ou Horizon Client 5.2 pour Windows) ou versions ultérieures qui se connectent à PSG.

PSG fournit également un certificat SSL hérité par défaut qui est présenté aux clients exécutant des clients plus anciens ou des versions antérieures qui se connectent à PSG.

Les certificats par défaut fournissent des connexions sécurisées entre les points de terminaison 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 serveurs 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 le serveur 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 le serveur 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 84

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 85

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 86

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 87

Vous pouvez garantir que toutes les connexions clientes à PSG utilisent le certificat signé par une autorité de certification pour PSG plutôt que le 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 convient de forcer l'utilisation d'un certificat signé par une autorité de certification dans votre déploiement d'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'hôte de 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 Horizon 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 le serveur, 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 du serveur 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 serveur 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 84.
- 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 75.
- 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 75.
- Familiarisez-vous avec la modification du nom convivial du certificat. Reportez-vous à la section « Modifier le nom convivial du certificat », page 76.

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 client qui se connectent au serveur via PCoIP.

Remarque Cette procédure n'affecte pas les périphériques client hérités. PSG continue de présenter le certificat hérité par défaut aux périphériques client hérités qui se connectent au serveur 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 le serveur sur lequel il est exécuté. Si vous configurez PSG afin qu'il utilise le même certificat que le serveur, 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 84.
- 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 85.

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 le serveur, la valeur doit être **vdm**.

5 Redémarrez le service VMware Horizon View PCoIP Secure Gateway pour que vos modifications prennent effet.

Suivant

Vérifiez que les périphériques clients 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 clientes à PSG utilisent le certificat signé par une autorité de certification pour PSG plutôt que le 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 convient de forcer l'utilisation d'un certificat signé par une autorité de certification dans votre déploiement d'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 serveur via PCoIP.

Prérequis

Vérifiez que tous les périphériques clients qui se connectent à ce serveur, y compris les clients légers, exécutent Horizon Client 5.2 pour Windows ou Horizon Client 2.0 ou version ultérieure. 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 Horizon View PCoIP Secure Gateway pour que vos modifications prennent effet.

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 à utiliser des certificats SSL signés par une autorité de certification

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 à un domaine Web comme `www.mycorp.com`, ou vous pouvez demander un certificat de serveur SSL de remplacement pouvant être utilisé dans un domaine comme `*.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 spécifiques à un domaine sont utilisés dans des installations sécurisées. Les autorités de certification garantissent normalement une meilleure protection contre les pertes de certificats spécifiques à un domaine que contre les pertes de certificats de remplacement. Si vous utilisez un certificat de remplacement partagé avec d'autres services, la sécurité du produit VMware Horizon dépend également de la sécurité de ces autres services. Si vous utilisez un certificat de remplacement, vous devez vous assurer que la clé privée est transférable entre 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.

Problèmes de certificat de dépannage sur le Serveur de connexion View et le serveur de sécurité

Des problèmes de certificat sur un serveur View Server vous empêchent de vous connecter à View Administrator ou provoquent l'affichage d'un indicateur de santé rouge pour un serveur.

Problème

Vous ne pouvez pas vous connecter à View Administrator sur l'instance du Serveur de connexion View concernée par le problème. Lorsque vous vous connectez à View Administrator sur une autre instance du Serveur de connexion View du même espace, vous constatez que l'indicateur de santé figurant sur le tableau de bord est affiché en rouge pour le problème concernant l'instance du Serveur de connexion View.

Si, lorsque vous cliquez sur l'indicateur de santé rouge, dans l'autre instance du Serveur de connexion View, le message `Certificat SSL : non valide` et `État :` (vide) s'affiche, cela signifie qu'aucun certificat valide n'a été trouvé. Le fichier journal de View contient une entrée de journal de type ERREUR avec le message suivant : `Aucun certificat correspondant dans le magasin de clés`.

Les données du journal de View sont situées dans `C:\ProgramData\VMware\VDM\logs\log-*.txt` sur l'instance du Serveur de connexion View.

Cause

Il se peut qu'un certificat ne se soit pas correctement installé sur un serveur View Server pour l'une des raisons suivantes :

- Le certificat ne se trouve pas dans le dossier Personnel du magasin de certificats de l'ordinateur local Windows.
- Le magasin de certificats ne dispose d'aucune clé privée pour le certificat.

- Le certificat ne dispose pas d'un nom convivial de **vdm**.
- Le certificat a été généré à partir d'un modèle de certificat v3, pour un serveur Windows Server 2008 ou version ultérieure. View ne parvient pas à détecter une clé privée, mais si vous utilisez le composant logiciel enfichable Certificat pour vérifier le magasin de certificats Windows, celui-ci indique qu'il existe une clé privée.

Solution

- Vérifiez que le certificat est importé dans le dossier Personnel du magasin de certificats de l'ordinateur local Windows.

  Reportez-vous à la section « Importer un certificat de serveur signé dans un magasin de certificats Windows », page 75.
- Vérifiez que le certificat contient une clé privée.

  Reportez-vous à la section « Importer un certificat de serveur signé dans un magasin de certificats Windows », page 75.
- Vérifiez que le certificat dispose d'un nom convivial de **vdm**.

  Reportez-vous à la section « Modifier le nom convivial du certificat », page 76.
- Si le certificat a été généré à partir d'un modèle de certificat v3, obtenez un certificat valide et signé d'une autorité de certification qui n'utilise pas de modèle v3.

  Reportez-vous à la section « Obtention d'un certificat SSL signé auprès d'une autorité de certification », page 72.

Configuration d' View pour la première fois 7

Après l'installation du logiciel View Server et la configuration de certificats SSL pour les serveurs, vous devez prendre des mesures supplémentaires pour configurer un environnement View fonctionnel.

Vous configurez des comptes d'utilisateurs pour vCenter Server et View Composer, installez une clé de licence View, ajoutez vCenter Server et View Composer à votre environnement View, configurez PCoIP Secure Gateway et un tunnel sécurisé et, éventuellement, dimensionnez les paramètres Windows Server pour prendre en charge votre 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, vous devez configurer un compte d'utilisateur autorisé à effectuer des opérations dans vCenter Server. Pour utiliser View Composer, vous devez accorder à l'utilisateur de vCenter Server ces privilèges supplémentaires.

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 21.

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.
- 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 et View Composer

Pour configurer un compte d'utilisateur qui accorde à View l'autorisation d'effectuer des opérations sur vCenter Server, vous devez attribuer 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 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 Serveur de connexion View ou un domaine approuvé. Reportez-vous à la section « Création d'un compte d'utilisateur pour vCenter Server », page 21.
- Familiarisez-vous avec les privilèges de vCenter Server qui sont requis pour ce compte d'utilisateur. Reportez-vous à la section « Privilèges requis pour l'utilisateur de vCenter Server », page 93.
- 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 94.

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 Serveur de connexion View et View Composer ont besoin pour effectuer des opérations vCenter Server.

     Dans vSphere Client, cliquez sur **Accueil > Rôles > Ajouter un rôle**, entrez un nom de rôle, comme **`Administrateur de View Composer`** et sélectionnez des privilèges pour ce rôle.

     Ce rôle doit posséder tous les privilèges dont Serveur de connexion View et View Composer ont besoin pour fonctionner dans vCenter Server.
   - Si vous utilisez View sans View Composer, vous pouvez créer un rôle encore plus limité avec les privilèges minimum dont Serveur de connexion View a besoin pour effectuer des opérations vCenter Server.

     Dans vSphere Client, cliquez sur **Accueil > Rôles > Ajouter un rôle**, entrez un nom de rôle, comme **`Administrateur de View Manager`**, et sélectionnez des privilèges pour ce rôle.

2 Dans vSphere Client, cliquez avec le bouton droit sur le serveur vCenter Server dans le niveau supérieur de l'inventaire, cliquez sur **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 ajoutez vCenter Server à View, spécifiez l'utilisateur de vCenter Server. Reportez-vous à la section « Ajouter des instances de vCenter Server à View », page 96.

Privilèges requis pour l'utilisateur de vCenter Server

L'utilisateur de vCenter Server doit disposer de privilèges vCenter Server suffisants pour permettre à View d'effectuer des opérations dans vCenter Server. Créez un rôle View Manager pour l'utilisateur de vCenter Server avec les privilèges requis.

Tableau 7-1. Privilège requis pour le rôle View Manager

Groupe de privilèges	Privilèges à activer
Dossier	**Create Folder (Créer un dossier)** **Delete Folder (Supprimer un dossier)**
Magasin de données	**Allocate space (Allouer de l'espace)**
Machine virtuelle	Dans **Configuration** : ■ **Add or remove device (Ajouter ou supprimer un périphérique)** ■ **Avancé** ■ **Modify device settings (Modifier des paramètres de périphérique)** Dans **Interaction** : ■ **Désactiver** ■ **Activer** ■ **Réinitialiser** ■ **Interrompre** Dans **Inventaire** : ■ **Create new (Créer un nouveau)** ■ **Créer à partir de l'existant** ■ **Supprimer** Dans **Approvisionnement** : ■ **Customize (Personnaliser)** ■ **Deploy template (Déployer un modèle)** ■ **Read customization specifications (Lire des spécifications de personnalisation)**
Resource (Ressource)	**Assign virtual machine to resource pool (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** : ■ **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 supplémentaires à ceux requis pour prendre en charge View. Créez un rôle View Composer pour l'utilisateur de vCenter Server avec les privilèges de View Manager et ces privilèges supplémentaires.

Tableau 7-2. Privilèges de View Composer

Groupe de privilèges	Privilèges à activer
Magasin de données	**Allocate space (Allouer de l'espace)** **Browse datastore (Parcourir le magasin de données)** **Low level file operations (Opérations de fichier de niveau faible)**
Virtual machine (Machine virtuelle)	**Inventaire** (tous) **Configuration** (tous) **Gestion des snapshots** (tous) Dans **Approvisionnement** : ■ **Clone virtual machine (Cloner la machine virtuelle)** ■ **Allow disk access (Autoriser l'accès au disque)**
Resource (Ressource)	**Assign virtual machine to resource pool (Attribuer une machine virtuelle au pool de ressources)** Le privilège suivant est requis pour exécuter des opérations de rééquilibrage de View Composer. **Migrer une machine virtuelle désactivée**
Global	**Enable methods (Activer des méthodes)** **Disable methods (Désactiver des méthodes)** **System tag (Balise système)** 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. **Agir comme vCenter Server**
Réseau	(tous)

Première configuration de Serveur de connexion View

Une fois vous avez installé Serveur de connexion View, vous devez installer une licence produit et ajouter des serveurs vCenter Server et des services View Composer à View. 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 et s'affichent automatiquement dans View Administrator.

View Administrator et Serveur de connexion View

View Administrator fournit une interface de gestion pour View.

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 Serveur de connexion View autonome ou à un groupe d'instances de Serveur de connexion View répliquées.

  Vous pouvez utiliser le nom d'hôte ou 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 Serveur de connexion View autonome ou chaque groupe d'instances de Serveur de connexion View répliquées.

Vous pouvez également utiliser View Administrator pour gérer des serveurs de sécurité associés à Serveur de connexion View. Chaque serveur de sécurité est associé à une instance de Serveur de connexion View.

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.

Si vous ouvrez votre navigateur sur l'hôte de Serveur de connexion View, utilisez **`https://127.0.0.1`** pour vous connecter et non **`https://localhost`**. Cette méthode renforce la sécurité en évitant les attaques DNS potentielles sur la résolution de `localhost`.

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. 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 **Configuration de View > Administrateurs** afin de modifier la liste des utilisateurs et des groupes ayant un rôle d'administrateur View.

Installer la clé de licence produit

Avant de pouvoir utiliser le Serveur de connexion View, vous devez entrer une clé de licence produit.

Lors de votre première ouverture de session, View Administrator affiche la page Product Licensing and Usage (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 de View LDAP.

Remarque Le Serveur de connexion View nécessite une clé de licence valide. À partir de View 4.0, la clé de licence produit est une clé à 25 caractères.

Procédure

1 Dans View Administrator, sélectionnez **Configuration de View > Licence produit et utilisation**.

2 Dans le volet **Licence**, cliquez sur **Modifier la licence**.

3 Saisissez le numéro de série de licence et cliquez sur **OK**.

4 Vérifiez la date d'expiration de la licence.

5 Vérifiez que les licences d'utilisation à distance des postes de travail et des applications, et de View Composer sont activées ou désactivées en fonction de l'édition de VMware Horizon que la licence produit vous autorise à utiliser.

Les fonctionnalités et les capacités de VMware Horizon avec View ne sont pas toutes disponibles dans toutes les éditions. Pour comparer les fonctionnalités de chaque édition, consultez http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf.

Ajouter des instances de vCenter Server à View

Vous devez configurer View afin qu'il se connecte aux instances de vCenter Server dans votre déploiement de View. vCenter Server crée et gère les machines virtuelles que View utilise dans les pools de postes de travail.

Si vous exécutez des instances de vCenter Server dans un groupe Linked Mode, vous devez ajouter séparément chaque instance de vCenter Server à View.

View 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.

- Configurez un utilisateur de vCenter Server autorisé à effectuer dans vCenter Server les opérations nécessaires à la prise en charge de View. Pour utiliser View Composer, vous devez accorder à l'utilisateur des privilèges supplémentaires.

  Reportez-vous à la section « Configurer un utilisateur de vCenter Server pour View et View Composer », page 92.

- 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 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 racines 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.

  Reportez-vous à « Importer un certificat racine et des certificats intermédiaires dans un magasin de certificats Windows », page 77.

- 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.

- Si vous effectuez une mise à niveau vers vSphere 5.5 ou version ultérieure, vérifiez que des autorisations ont été explicitement attribuées au compte d'administrateur du domaine que vous utilisez en tant qu'utilisateur de vCenter Server pour permettre à un utilisateur local de vCenter Server de se connecter à celui-ci.

- Familiarisez-vous avec les paramètres qui déterminent les limites d'opérations maximales pour vCenter Server et View Composer. Reportez-vous aux sections « Limites d'opérations simultanées pour vCenter Server et View Composer », page 103 et « Définition d'un taux d'opérations d'alimentation simultanées pour prendre en charge les tempêtes d'ouverture de session des postes de travail distants », page 104.

Procédure

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

2 Sous l'onglet **Serveurs vCenter Server**, cliquez sur **Ajouter**.

3 Dans la zone de texte **Adresse du serveur** des paramètres de vCenter Server, entrez le nom de domaine complet de l'instance de vCenter Server.

  Le FQDN inclut le nom d'hôte et le nom de domaine. Par exemple, dans le nom de domaine complet ***myserverhost.companydomain.com***, ***myserverhost*** correspond au nom d'hôte et ***companydomain.com*** au domaine.

  Remarque Si vous entrez un serveur à l'aide d'un nom DNS ou d'une URL, View n'effectue pas de recherche DNS pour vérifier si un administrateur a précédemment ajouté ce serveur à View 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 104.

Si View 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 Serveur de connexion View 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.

VMware recommande d'avoir un mappage un-à-un entre chaque service View Composer et instance de vCenter Server.

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 21.
- Vérifiez que vous avez configuré Serveur de connexion View 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 », page 96.
- 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**. 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**. b Dans la zone de texte de l'adresse du serveur View Composer Server, saisissez le nom de domaine complet (FQDN) de l'hôte de View Composer. c Saisissez le nom de l'utilisateur de View Composer. Par exemple : **`domain.com\user`** ou **`user@domain.com`** d Saisissez le mot de passe de l'utilisateur de View Composer. 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 104.

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 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. De l'espace peut être récupéré lorsque les machines virtuelles sont mises sous tension et que les utilisateurs interagissent avec leurs postes de travail distants.

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 professionnels de l'information qui installent des applications utilisateur sur des postes de travail distants dédiés peuvent perdre leurs applications personnelles si les postes de travail distants 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 provisionnement.

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 version ultérieure, lorsqu'une machine virtuelle parente est la version matérielle virtuelle 9 ou version ultérieure, 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 version ultérieure, et uniquement sur des machines disposant de la version matérielle virtuelle 9 ou version ultérieure.

- 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, notamment tous les hôtes ESXi d'un cluster, sont à la version 5.1 avec le correctif de téléchargement ESXi 5.1 ESXi510-201212001 ou version ultérieure.

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 version ultérieure. Vous devez sélectionner **Activer la récupération d'espace** si vous effectuez une mise à niveau vers View 5.2 ou version ultérieure depuis View 5.1 ou 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 nombreuses machines virtuelles 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 fonctionnalité peut être désactivée ou activée lorsque vous créez ou modifiez un pool de postes de travail. Pour fonctionner sur un pool de postes de travail, View Storage Accelerator doit être activé pour vCenter Server et pour le pool de postes de travail individuel.

Vous pouvez activer View Storage Accelerator sur des pools de postes de travail contenant des clones liés et sur des pools contenant des machines virtuelles complètes.

View Composer Array Integration n'est pas pris en charge dans les pools de postes de travail 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 une banque de données distincte des clones liés. Bien que les avantages de performance liés à 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 obtenus en stockant les réplicas sur une banque de données distincte. 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 affecter le privilège **Général > Agir comme vCenter Server** dans vCenter Server.

  Reportez-vous à la section « Configuration de comptes d'utilisateur pour vCenter Server et View Composer », page 91.

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 du 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 des connexions Horizon Client », page 106.

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 *Configuration de pools de postes de travail et d'applications View*.

Limites d'opérations simultanées pour vCenter Server et View Composer

Lorsque vous ajoutez vCenter Server à View ou que vous modifiez les paramètres de vCenter Server, vous pouvez configurer plusieurs options définissant le nombre maximal d'opérations simultanées exécutées par vCenter Server et View Composer.

Vous configurez ces options dans le volet Paramètres avancés de la page d'informations sur vCenter Server.

Tableau 7-3. Limites d'opérations simultanées pour vCenter Server et View Composer

Paramètre	Description
Nombre maximal d'opérations d'approvisionnement de vCenter simultanées	Détermine le nombre maximal de demandes simultanées que Serveur de connexion View peut créer pour approvisionner et supprimer des machines virtuelles complètes dans cette instance de vCenter Server. La valeur par défaut est 20. Ce paramètre s'applique uniquement à des machines virtuelles complètes.
Opérations d'alimentation simultanées max.	Détermine le nombre maximal d'opérations d'alimentation (démarrage, arrêt, interruption, etc.) pouvant se dérouler simultanément sur des machines virtuelles gérées par Serveur de connexion View dans cette instance de vCenter Server. La valeur par défaut est 50. Pour obtenir des recommandations sur le calcul d'une valeur pour ce paramètre, consultez « Définition d'un taux d'opérations d'alimentation simultanées pour prendre en charge les tempêtes d'ouverture de session des postes de travail distants », page 104. Ce paramètre s'applique à des machines virtuelles complètes et à des clones liés.
Nombre maximal 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 des clones liés gérés par cette instance de View Composer. La valeur par défaut est 12. Les sessions actives des postes de travail distants doivent être fermées avant que l'opération de maintenance puisse commencer. Si vous forcez les utilisateurs à fermer leur session dès que l'opération de maintenance commence, le nombre maximal d'opérations simultanées sur les postes de travail distants nécessitant une fermeture de session correspond à la moitié de la valeur configurée. Par exemple, si vous définissez ce paramètre sur 24 et forcez les utilisateurs à fermer leur session, le nombre maximal d'opérations simultanées sur les postes de travail distants nécessitant une fermeture de session est de 12. Ce paramètre ne s'applique qu'aux clones liés.
Nombre maximal d'opérations d'approvisionnement de View Composer simultanées	Détermine le nombre maximal d'opérations de création et de suppression pouvant se dérouler simultanément sur des clones liés gérés par cette instance de View Composer. La valeur par défaut est 8. Ce 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 distants

Le paramètre **Opérations d'alimentation simultanées max** régit le nombre maximal d'opérations d'alimentation simultanées qui peuvent se produire sur des machines virtuelles de poste de travail distant dans une instance de vCenter Server. Cette limite est fixée à 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, reportez-vous à la section « Recommandations sur la planification et les éléments de conception d'architecture » dans le document *Planification de l'architecture de 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.

Le système 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 de View Composer à View, vous devez vérifier que les certificats SSL utilisés pour les instances de vCenter Server et de View Composer sont valides et approuvés par le Serveur de connexion View. Si les certificats par défaut installés avec vCenter Server et View Composer sont toujours en place, vous devez déterminer s'il convient ou non d'accepter les empreintes de ces certificats.

Si une instance de vCenter Server ou de View Composer est configurée avec un certificat signé par une autorité de certification, et si le certificat racine est approuvé par le Serveur de connexion View, vous n'avez pas à accepter l'empreinte du 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 6, « Configuration de certificats SSL pour des View Servers », page 69.

Vous ajoutez d'abord vCenter Server et View Composer dans View Administrator à l'aide de l'assistant Ajouter vCenter Server. Si un certificat n'est pas approuvé et si vous n'acceptez pas son empreinte, vous ne pouvez pas ajouter vCenter Server et View Composer.

Une fois ces serveurs ajoutés, vous pouvez les reconfigurer dans la boîte de dialogue Modifier vCenter Server.

Remarque Vous devez également accepter une empreinte de certificat lorsque vous mettez à niveau une version antérieure et lorsqu'un certificat de vCenter Server ou de 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 de 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 qu'utilisera une instance du Serveur de connexion View. Si le certificat de serveur SAML n'est pas approuvé par le Serveur de connexion View, vous devez déterminer s'il convient ou non d'accepter l'empreinte de certificat. Si vous n'acceptez pas l'empreinte, vous ne pouvez pas configurer l'authentificateur SAML dans View. Une fois l'authentificateur SAML configuré, vous pouvez le reconfigurer dans la boîte de dialogue Modifier le 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 Vérifiez l'empreinte de certificat qui a été configurée pour l'instance de vCenter Server ou de View Composer.

   a Sur l'hôte de vCenter Server ou de View Composer, démarrez le composant logiciel enfichable MMC et ouvrez le magasin de certificats Windows.

   b Accédez au certificat de vCenter Server ou de View Composer.

   c Cliquez sur l'onglet Détails du certificat pour afficher l'empreinte numérique de certificat.

   De la même façon, vérifiez l'empreinte de certificat d'un authentificateur SAML. Le cas échéant, exécutez les étapes précédentes sur l'hôte de l'authentificateur SAML.

4 Vérifiez que l'empreinte dans la fenêtre Informations sur le certificat correspond à l'empreinte de l'instance de vCenter Server ou de View Composer.

   De la même façon, vérifiez que les empreintes correspondent pour un authentificateur SAML.

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**. Corrigez les certificats incompatibles. Par exemple, vous avez peut-être fourni une adresse IP incorrecte pour vCenter Server ou View Composer.

Configuration des connexions Horizon Client

Les points de terminaison clients communiquent avec un hôte de Serveur de connexion View ou de serveur de sécurité sur des connexions sécurisées.

La connexion cliente initiale, utilisée pour l'authentification utilisateur et la sélection d'applications et de postes de travail distants, est créée sur HTTPS lorsqu'un utilisateur fournit un nom de domaine à Horizon 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 se sont pas encore connectés à l'application ou au poste de travail distant.

Lorsque des utilisateurs se connectent à des applications et des postes de travail distants, le 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 applications et des postes de travail distants avec le protocole d'affichage PCoIP, le client peut établir une autre connexion à PCoIP Secure Gateway sur l'hôte de Serveur de connexion View ou du serveur de sécurité. PCoIP Secure Gateway garantit que seuls les utilisateurs authentifiés peuvent communiquer avec des applications et des postes de travail distants sur PCoIP.

Vous pouvez également fournir des connexions sécurisées aux utilisateurs externes qui utilisent HTML Access pour se connecter à des postes de travail distants. Blast Secure Gateway vérifie que seuls des utilisateurs authentifiés peuvent communiquer avec des postes de travail distants. Avec HTML Access, le logiciel Horizon Client n'a pas à être installé sur les périphériques de point de terminaison des utilisateurs.

Selon le type de périphérique client utilisé, des canaux supplémentaires sont établis pour effectuer d'autres trafics comme la redirection USB des données vers le périphérique client. Ces canaux de données acheminent le trafic par le tunnel sécurisé s'il est activé.

Lorsque le tunnel sécurisé et les passerelles sécurisées sont désactivés, les sessions de postes de travail et d'applications sont établies directement entre le périphérique client et la machine distante, contournant 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 et d'applications 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 le tunnel sécurisé, PCoIP Secure Gateway et, si vos utilisateurs se connectent à l'aide de HTML Access, Blast Secure Gateway. Vous pouvez désactiver le tunnel sécurisé et les passerelles sécurisées pour permettre aux clients internes connectés via un réseau local d'établir des connexions directes à des applications et des postes de travail distants.

Si vous activez uniquement le tunnel sécurisé ou uniquement une passerelle sécurisée, une session peut utiliser une connexion directe pour certains trafics mais envoyer d'autres trafics par le biais de l'hôte de Serveur de connexion View ou du serveur de sécurité, selon le type de client utilisé.

SSL est requis pour toutes les connexions client aux hôtes de Serveur de connexion View et du serveur de sécurité.

Configurer PCoIP Secure Gateway et les connexions 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 les applications et postes de travail distants.

Les clients utilisant le protocole d'affichage PCoIP peuvent utiliser PCoIP Secure Gateway. Les clients utilisant le protocole d'affichage RDP peuvent utiliser le tunnel sécurisé.

Pour en savoir plus sur la configuration de Blast Secure Gateway, consultez « Configurer un accès HTML sécurisé », page 108.

Important Une configuration de réseau classique qui fournit des connexions sécurisées pour 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 Serveurs de connexion 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	Désélectionnez **Utiliser une connexion par tunnel sécurisé à la machine**.
Activer le tunnel sécurisé	Sélectionnez **Utiliser une connexion par tunnel sécurisé à la machine**.

Le tunnel sécurisé est activé par défaut.

4 Configurez l'utilisation de PCoIP Secure Gateway.

Option	Description
Activer PCoIP Secure Gateway	Sélectionnez **Utiliser PCoIP Secure Gateway pour les connexions PCoIP à la machine**.
Désactiver PCoIP Secure Gateway	Désélectionnez **Utiliser PCoIP Secure Gateway pour les connexions PCoIP à la machine**.

Par défaut, PCoIP Secure Gateway est désactivé.

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 pour fournir un accès HTML sécurisé à des postes de travail distants.

Blast Secure Gateway vérifie que seuls les utilisateurs authentifiés peuvent communiquer avec des postes de travail distants à l'aide de HTML Access. Horizon 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 distant, contournant ainsi 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 distants à l'aide du portail d'applications d'Workspace, vérifiez qu'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 Sur l'onglet **Serveurs de connexion**, sélectionnez une 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 HTML Access à la machine**
Désactiver Blast Secure Gateway	Décochez la case **Utiliser Blast Secure Gateway pour un HTML Access à la machine**

Blast Secure Gateway est activé par défaut.

4 Cliquez sur **OK** pour enregistrer vos modifications.

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-example.com:443`
- `https://view.example.com:443`
- `https://example.com:1234`
- `https://10.20.30.40:443`

Pour utiliser des adresses comme celles-ci dans View, vous devez configurer l'hôte de Serveur de connexion View ou du serveur de sécurité pour renvoyer une URL externe au lieu du nom de domaine complet 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 une instance de Serveur de connexion View 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 PCoIP Secure Gateway et les connexions par tunnel sécurisé », page 107.
- 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 108.

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 : `192.0.2.1:4172`

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

- 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 PCoIP Secure Gateway et les connexions par tunnel sécurisé », page 107.
- 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 108.

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**.

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://myserver.example.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 : `192.0.2.2:4172`

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 de Serveur de connexion View, de serveur de sécurité, de PCoIP Secure Gateway et de View Composer.

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 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 du Serveur de connexion View ou un serveur de sécurité en modifiant le fichier `locked.properties` sur l'ordinateur serveur. 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 serveur 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 afin qu'il ouvre les ports par défaut requis. Si vous modifiez la carte réseau ou un numéro de port sur lequel il écoute, vous devez reconfigurer manuellement votre pare-feu Windows afin qu'il ouvre les ports mis à jour pour que les périphériques clients puissent se connecter au serveur.

Si vous modifiez le numéro de port SSL et que vous souhaitez que la redirection HTTP continue à fonctionner, vous devez également modifier le numéro de port pour la redirection HTTP. Reportez-vous à la section « Modifier le numéro de port pour la redirection HTTP vers le Serveur de connexion », page 115.

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 serveur contient plusieurs cartes réseau, sélectionnez-en une 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 distants, 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 Horizon 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 Server pour ouvrir le port mis à jour.

Modifier le numéro de port pour la redirection HTTP vers le Serveur de connexion

Si vous remplacez le port 443 par défaut sur View Server, et que vous voulez autoriser la redirection HTTP pour les clients View qui tentent de se connecter au port 80, vous devez configurer le fichier `locked.properties` sur View Server.

Remarque Cette procédure n'a aucun effet si vous déchargez SSL sur un périphérique intermédiaire. Avec le déchargement SSL en place, le port HTTP sur View Server fournit le service aux clients.

Prérequis

Vérifiez que vous avez modifié le numéro de port par défaut 443. Si vous utilisez les valeurs par défaut configurées lors de l'installation, vous n'avez pas à effectuer cette procédure pour conserver la règle de redirection HTTP.

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 les lignes suivantes au fichier `locked.properties` :

```
frontMappingHttpDisabled.1=5:*:moved:https::port
frontMappingHttpDisabled.2=3:/error/*:file:docroot
frontMappingHttpDisabled.3=1:/admin*:missing
frontMappingHttpDisabled.4=1:/view-vlsi*:missing
```

Dans les lignes précédentes, la variable *port* est le numéro de port auquel le client doit se connecter.

Si vous n'ajoutez pas les lignes précédentes, le *port* reste 443.

3 Redémarrez le service Serveur de connexion View ou le service du serveur de sécurité pour que vos modifications prennent effet.

Empêcher la redirection HTTP pour les connexions clientes au Serveur de connexion

Les tentatives de clients View de se connecter à des View Server via HTTP sont redirigées en silence vers HTTPS. Dans certains déploiements, vous voulez peut-être empêcher les utilisateurs d'entrer **`http://`** dans leurs navigateurs Web et les forcer à utiliser HTTPS. Pour empêcher la redirection HTTP pour les clients View, vous devez configurer le fichier `locked.properties` sur View Server.

Remarque Cette procédure n'a aucun effet si vous déchargez SSL sur un périphérique intermédiaire. Avec le déchargement SSL en place, le port HTTP sur View Server fournit le service aux clients.

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 les lignes suivantes au fichier `locked.properties` :

```
frontMappingHttpDisabled.1=5:*:missing
frontMappingHttpDisabled.2=3:/error/*:file:docroot
```

3 Redémarrez le service Serveur de connexion View ou le service du serveur de sécurité pour que vos modifications prennent effet.

Activer l'accès à distance pour afficher les compteurs de performances sur les serveurs de connexion

Les compteurs de performances View sont disponibles localement sur un serveur de connexion, mais ils reviennent à 0 lorsqu'un autre ordinateur y accède. Pour activer un accès à distance aux compteurs de performances View sur les serveurs de connexion, vous devez configurer le port de l'infrastructure des serveurs de connexion dans le registre.

Procédure

1 Démarrez l'éditeur du Registre Windows.

2 Accédez à la clé de registre `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Node Manager`.

3 Ajoutez une nouvelle valeur de chaîne (REG_SZ), `Management Port`.

4 Définissez la valeur de `Management Port` sur **`32111`**.

Dimensionnement de paramètres de Windows Server pour prendre en charge votre déploiement

Pour prendre en charge un déploiement important de postes de travail distants, 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 R2 et Windows Server 2012 R2, 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.

Dimensionnement de la mémoire de Serveur de connexion View

Sur un ordinateur Serveur de connexion View, 10 Go de mémoire sont recommandés pour le déploiement de 50 postes de travail distants ou plus. Un ordinateur Windows Server avec au moins 10 Go de mémoire est configuré automatiquement pour prendre en charge environ 2 000 sessions par tunnel simultanées, soit le maximum pris en charge par Serveur de connexion View.

Configurez moins de 10 Go de mémoire uniquement pour les petits déploiements de test de concept. Avec un minimum requis de 4 Go de mémoire, une configuration peut prendre en charge environ 500 sessions par tunnel simultanées, ce qui est plus qu'adéquat pour prendre en charge les petits déploiements de test de concept.

Toutefois, du fait que votre déploiement est susceptible de s'étendre au fur et à meure que des utilisateurs sont ajoutés à l'environnement, VMware vous recommande de toujours configurer au moins 10 Go de mémoire. Faites une exception uniquement lorsque vous savez que l'environnement ne s'étendra pas et que la mémoire n'est pas disponible.

Si vous installez Serveur de connexion View avec une mémoire inférieure à 10 Go, View fournit des recommandations relatives à la mémoire en générant des messages d'avertissement une fois l'installation terminée. Un événement déclenché toutes les 12 heures indique que l'instance de Serveur de connexion View est configurée avec une petite quantité de mémoire physique.

Si vous augmentez la mémoire d'un ordinateur à 10 Go pour prendre en charge un déploiement plus important, redémarrez Serveur de connexion View pour vous assurer que la taille de segment JVM augmente automatiquement à la valeur recommandée. Vous n'avez pas besoin de réinstaller Serveur de connexion View.

IMPORTANT Ne modifiez pas la taille de segment JVM sur des ordinateurs Windows Server 64 bits. Modifier cette valeur peut rendre le comportement de Serveur de connexion View instable. Sur des ordinateurs 64 bits, le service de Serveur de connexion View définit la taille de segment JVM pour concorder avec la mémoire physique.

Pour connaître la configuration matérielle et de mémoire pour Serveur de connexion View, reportez-vous à la section « Exigences matérielles de Serveur de connexion View », page 8

Pour obtenir des recommandations matérielles et de mémoire pour utiliser Serveur de connexion View dans un déploiement important, consultez la section « Configuration de machine virtuelle et nombre maximal dans Serveur de connexion View » du document *Planification de l'architecture de View*.

Configurer les paramètres du fichier d'échange du système

Vous pouvez optimiser la mémoire virtuelle sur les ordinateurs Windows Server sur lesquels vos instances du Serveur de connexion View 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 Serveur de connexion View est installé, naviguez vers la boîte de dialogue Mémoire virtuelle.

   Par défaut, **Taille personnalisée** est sélectionné. Une taille de fichier d'échange initiale et maximale apparaît.

2 Cliquez sur **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.

Configuration du reporting d'événements 8

Vous pouvez créer une base de données des événements pour enregistrer des informations sur des événements d'View. 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 du Serveur de connexion View 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 du Serveur de connexion View a accès. Pour afficher 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 28

- 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 31

Procédure

1 Ajoutez une nouvelle base de données au serveur et donnez-lui un nom descriptif tel que ViewEvents.

   Pour une base de données Oracle 11g ou 10g, fournissez également un préfixe d'Identificateur système Oracle (SID) que vous utiliserez lorsque vous configurerez la base de données d'événements dans View Administrator.

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 indiquées dans « Configurer la base de données des évévements », page 121.

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 119.
- 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 **Configuration du réseau SQL Server *YYYY***.

2 Sélectionnez **Protocoles pour *server_name***.

3 Dans la liste de protocoles, cliquez avec le bouton droit sur **TCP/IP** et sélectionnez **Propriétés**.

4 Définissez la propriété **Activé** sur **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 au Serveur de connexion View. Suivez les instructions de la section « Configurer la base de données des évévements », page 121.

Configurer la base de données des évévements

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 de 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, reportez-vous au document *Intégration de 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. Reportez-vous à 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 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, reportez-vous à 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 119.

  Pour une base de données Oracle 11g ou 10g, vous devez utiliser l'identificateur du système Oracle (SID) comme nom de base de données lorsque vous configurez la base de données d'événements dans View Administrator.
- 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 119.

  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 le 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 est établie.

   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 de 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 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

L

M

N

O

P

R

S