

Installation d'Horizon 7

13 décembre 2018

VMware Horizon 7 7.7



vmware®

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

<https://docs.vmware.com/fr/>

Les dernières mises à jour produit se trouvent également sur le site Web de VMware.

Si vous avez des commentaires à propos de cette documentation, envoyez-les à l'adresse suivante :

docfeedback@vmware.com

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

VMware France SAS.
Tour Franklin
100-101 Terrasse Boieldieu
92042 Paris La Défense 8 Cedex
France
www.vmware.com/fr

Copyright © 2011–2018 VMware, Inc. Tous droits réservés. [Informations sur le copyright et les marques commerciales.](#)

Table des matières

Installation de Horizon 7 6

1 Configuration requise pour les composants serveur 7

Exigences du Serveur de connexion Horizon 7

Exigences d' Horizon Administrator 10

Exigences de View Composer 10

2 Configuration requise pour les systèmes d'exploitation client 13

Systèmes d'exploitation pris en charge pour Horizon Agent 13

Systèmes d'exploitation pris en charge pour Horizon Persona Management autonome 14

Prise en charge du protocole d'affichage à distance et logicielle 14

3 Installation de Horizon 7 dans un environnement IPv6 23

Configuration d' Horizon 7 dans un environnement IPv6 23

Versions de vSphere, de base de données et d'Active Directory prises en charge dans un environnement IPv6 24

Systèmes d'exploitation pris en charge pour les serveurs Horizon 7 dans un environnement IPv6 25

Systèmes d'exploitation Windows pris en charge pour les postes de travail et les hôtes RDS dans un environnement IPv6 25

Clients pris en charge dans un environnement IPv6 26

Protocoles de communication à distance pris en charge dans un environnement IPv6 26

Types d'authentification pris en charge dans un environnement IPv6 26

Autres fonctionnalités prises en charge dans un environnement IPv6 27

4 Installation d' Horizon 7 en mode FIPS 30

Présentation de la configuration d' Horizon 7 en mode FIPS 30

Configuration requise pour le mode FIPS 31

5 Préparation d'Active Directory 33

Configuration de domaines et de relations d'approbation 34

Création d'une UO pour des postes de travail distants 35

Création d'UO et de groupes pour des comptes de client en mode kiosque 36

Création de groupes pour les utilisateurs 36

Création d'un compte d'utilisateur pour vCenter Server 36

Création d'un compte d'utilisateur pour un serveur View Composer Server autonome 37

Créer un compte d'utilisateur pour les opérations AD de View Composer 37

Créer un compte d'utilisateur pour les opérations Instant Clone 38

Configurer la stratégie Groupes restreints 39

Utilisation des fichiers de modèle d'administration de stratégie de groupe Horizon 7	40
Préparer Active Directory pour l'authentification par carte à puce	40
Désactiver des chiffrements faibles dans les protocoles SSL/TLS	44

6 Installation de View Composer 46

Préparer une base de données View Composer	46
Configuration d'un certificat SSL pour View Composer	56
Installer le service View Composer	57
Activer TLSv1.0 sur des connexions vCenter et ESXi depuis View Composer	59
Configuration de votre infrastructure pour View Composer	60

7 Installation du Serveur de connexion Horizon 62

Installation du logiciel Serveur de connexion Horizon	62
Conditions préalables d'installation pour le Serveur de connexion Horizon	63
Installer le Serveur de connexion Horizon avec une nouvelle configuration	64
Installer une instance répliquée du Serveur de connexion Horizon	73
Configurer un mot de passe de couplage de serveur de sécurité	81
Installer un serveur de sécurité	82
Avantages du dispositif Unified Access Gateway sur VPN	92
Règles de pare-feu pour le Serveur de connexion Horizon	93
Réinstaller le Serveur de connexion Horizon avec une configuration de sauvegarde	95
Options de la ligne de commande Microsoft Windows Installer	97
Désinstallation de composants d' Horizon 7 en silence à l'aide d'options de ligne de commande MSI	100

8 Configuration de certificats TLS pour des serveurs Horizon 7 102

Comprendre les certificats TLS pour les serveurs Horizon 7	103
Présentation des tâches de configuration des certificats TLS	105
Obtention d'un certificat TLS signé auprès d'une autorité de certification	106
Configurer le Serveur de connexion Horizon, le serveur de sécurité ou View Composer pour utiliser un nouveau certificat TLS	108
Configurer des points de terminaison clients pour approuver des certificats racine et intermédiaires	115
Configuration de la vérification de la révocation des certificats sur des certificats de serveur	118
Configurer PCoIP Secure Gateway pour utiliser un nouveau certificat TLS	119
Configuration d'Horizon Administrator pour approuver un certificat de vCenter Server ou View Composer	125
Avantages à utiliser des certificats TLS signés par une autorité de certification	125
Problèmes de certificat de dépannage sur le Serveur de connexion Horizon et le serveur de sécurité	126

9 Activation d' Horizon 7 pour les licences d'abonnement 128

VMware Horizon 7 Cloud Connector	128
----------------------------------	-----

- Déployer le dispositif virtuel Horizon 7 Cloud Connector avec Horizon 7 129
- Configurer un certificat signé par une autorité de certification pour le dispositif virtuel Horizon 7 Cloud Connector 131

10 Configuration d' Horizon 7 pour la première fois 133

- Configuration de comptes utilisateur pour vCenter Server, View Composer et les clones instantanés 133
- Configuration du Serveur de connexion Horizon pour la première fois 139
- Configuration des connexions Horizon Client 154
- Remplacement des ports par défaut pour les services Horizon 7 165
- Dimensionnement de paramètres de Windows Server pour prendre en charge votre déploiement 171

11 Configuration du reporting d'événements 174

- Ajouter une base de données et un utilisateur de base de données pour des événements Horizon 7 174
- Préparer une base de données SQL Server pour le reporting d'événements 175
- Configurer la base de données des événements 176
- Configurer la journalisation des événements pour des serveurs Syslog 178

Installation de Horizon 7

Installation d'Horizon 7 explique comment installer les composants serveur et client de VMware Horizon[®] 7.

Public cible

Ces informations sont destinées à toute personne souhaitant installer VMware Horizon 7. 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'Horizon 7 doivent satisfaire à des exigences matérielles et logicielles spécifiques.

Ce chapitre contient les rubriques suivantes :

- [Exigences du Serveur de connexion Horizon](#)
- [Exigences d'Horizon Administrator](#)
- [Exigences de View Composer](#)

Exigences du Serveur de connexion Horizon

Le Serveur de connexion Horizon 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 Horizon a des exigences matérielles, de système d'exploitation, d'installation et de logiciels pris en charge spécifiques.

- [Configuration matérielle requise du Serveur de connexion Horizon](#)

Vous devez installer tous les types d'installation du Serveur de connexion Horizon, y compris les installations standard, de réplica, de serveur de sécurité et de serveur d'inscription, sur une machine physique ou virtuelle dédiée répondant à des exigences matérielles spécifiques.
- [Systèmes d'exploitation pris en charge pour le Serveur de connexion Horizon](#)

Vous devez installer le Serveur de connexion Horizon sur un système d'exploitation Windows Server pris en charge.
- [Exigences du logiciel de virtualisation du Serveur de connexion Horizon](#)

Le Serveur de connexion Horizon requiert certaines versions du logiciel de virtualisation VMware.
- [Exigences de réseau pour des instances répliquées du Serveur de connexion Horizon](#)

Lorsque vous installez des instances répliquées du Serveur de connexion Horizon, 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 du Serveur de connexion Horizon. L'accès d'un utilisateur peut être refusé lors de la connexion à une instance du Serveur de connexion Horizon avec une configuration périmée.

Configuration matérielle requise du Serveur de connexion Horizon

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

Tableau 1-1. Configuration matérielle requise du Serveur de connexion Horizon

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 R2 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 R2 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 du Serveur de connexion Horizon 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 Horizon doit disposer d'une adresse IP qui ne change pas. Dans un environnement IPv4, configurez une adresse IP statique. Dans un environnement IPv6, les machines obtiennent automatiquement des adresses IP qui ne changent pas.

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

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

Les systèmes d'exploitation suivants prennent en charge tous les types d'installation du Serveur de connexion Horizon, 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 Horizon

Système d'exploitation	Version	Édition
Windows Server 2008 R2 SP1	64 bits	Standard Enterprise Datacenter
Windows Server 2012 R2	64 bits	Standard Datacenter
Windows Server 2016	64 bits	Standard Datacenter

Note Windows Server 2008 R2 sans Service Pack n'est plus pris en charge.

Exigences du logiciel de virtualisation du Serveur de connexion Horizon

Le Serveur de connexion Horizon requiert certaines versions du logiciel de virtualisation VMware.

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

Pour plus d'informations sur les versions d'Horizon 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 du Serveur de connexion Horizon

Lorsque vous installez des instances répliquées du Serveur de connexion Horizon, 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 du Serveur de connexion Horizon. L'accès d'un utilisateur peut être refusé lors de la connexion à une instance du Serveur de connexion Horizon avec une configuration périmée.

Important Pour utiliser un groupe d'instances du Serveur de connexion répliquées dans un réseau étendu, un réseau métropolitain ou autre réseau non local dans des scénarios dans lesquels un déploiement d'Horizon doit s'étendre sur des centres de données, vous devez utiliser la fonctionnalité Architecture Cloud Pod. Vous pouvez relier 25 espaces afin de fournir un seul vaste environnement de gestion et d'échange de postes de travail pour cinq sites géographiquement distants et fournir des postes de travail et des applications à 50 000 sessions au maximum. Pour plus d'informations, reportez-vous au document *Administration d'Architecture Cloud Pod dans Horizon 7*.

Exigences d' Horizon Administrator

Les administrateurs utilisent Horizon Administrator pour configurer le Horizon Connection Server, 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 Horizon Administrator doivent satisfaire un certain nombre d'exigences.

Horizon Administrator est une application Web installée lorsque vous installez le Serveur de connexion. Vous pouvez accéder à Horizon Administrator et l'utiliser avec les navigateurs Web suivants :

- Internet Explorer 9 (non recommandé)
- Internet Explorer 10
- Internet Explorer 11
- Firefox (dernières versions prises en charge)
- Chrome (dernières versions prises en charge)
- Firefox 6 et versions ultérieures
- Microsoft Edge (Windows 10)

Pour utiliser Horizon Administrator avec votre navigateur Web, vous devez installer Adobe Flash Player 10.1 ou version ultérieure. Votre système client doit avoir un accès à Internet pour permettre l'installation d'Adobe Flash Player.

L'ordinateur sur lequel vous lancez Horizon Administrator doit approuver les certificats racine et intermédiaires du serveur qui héberge le Serveur de connexion. 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 bien connue, vous devez suivre les instructions de [Configurer des points de terminaison clients pour approuver des certificats racine et intermédiaires](#).

Pour que le texte s'affiche correctement, Horizon 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, 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](#)

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

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 et la base de données d'événements

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. Il est également possible de configurer une base de données d'événements pour consigner des informations du Horizon Connection Server sur des événements Horizon.

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 SP1	64 bits	Standard Enterprise Datacenter
Windows Server 2012 R2	64 bits	Standard Datacenter
Windows Server 2016	64 bits	Standard Datacenter

Note Windows Server 2008 R2 sans Service Pack n'est plus pris en charge.

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](#).

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
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 disposer d'une adresse IP qui ne change pas. Dans un environnement IPv4, configurez une adresse IP statique. Dans un environnement IPv6, les machines obtiennent automatiquement des adresses IP qui ne changent pas.

Exigences de base de données pour View Composer et la base de données d'événements

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. Il est également possible de configurer une base de données d'événements pour consigner des informations du Horizon Connection Server sur des événements Horizon.

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 les matrices d'interopérabilité des produits VMware à l'adresse http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. 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 View Composer.

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.

Pour obtenir les informations les plus récentes sur les bases de données prises en charge, reportez-vous aux matrices d'interopérabilité des produits VMware à l'adresse http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. Pour en savoir plus sur l'**interopérabilité entre les solutions et les bases de données**, après avoir sélectionné le produit et la version, à l'étape Ajouter une base de données, pour afficher une liste de toutes les bases de données prises en charge, sélectionnez **Toutes** et cliquez sur **Ajouter**.

Configuration requise pour les systèmes d'exploitation client

2

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

Ce chapitre contient les rubriques suivantes :

- [Systèmes d'exploitation pris en charge pour Horizon Agent](#)
- [Systèmes d'exploitation pris en charge pour Horizon Persona Management autonome](#)
- [Prise en charge du protocole d'affichage à distance et logicielle](#)

Systèmes d'exploitation pris en charge pour Horizon Agent

Le composant Horizon Agent (appelé View Agent dans les versions précédentes) facilite l'utilisation des fonctionnalités de gestion de sessions, d'authentification unique, de redirection de périphériques, etc. Vous devez installer Horizon Agent sur l'ensemble des machines virtuelles, des systèmes physiques et des hôtes RDS.

Les types et éditions des systèmes d'exploitation client pris en charge dépendent de la version de Windows. Pour obtenir les mises à jour de la liste de systèmes d'exploitation Windows 10 pris en charge, consultez l'article de la base de connaissances de VMware <http://kb.vmware.com/kb/2149393>. Pour les systèmes d'exploitation Windows autres que Windows 10, consultez l'article <http://kb.vmware.com/kb/2150295> dans la base de connaissances de VMware.

Pour voir la liste des fonctionnalités d'expérience à distance prises en charge sur les systèmes d'exploitation Windows sur lesquels Horizon Agent est installé, consultez l'article <http://kb.vmware.com/kb/2150305> dans la base de connaissances de VMware.

Pour utiliser l'option de configuration d'Horizon Persona Management avec Horizon Agent, vous devez installer Horizon Agent sur des machines virtuelles Windows 10, Windows 8, Windows 8.1, Windows 7, Windows Server 2012 R2, Windows Server 2008 R2 ou Windows Server 2016. Cette option ne fonctionne pas sur les ordinateurs physiques ou sur les hôtes RDS.

Vous pouvez installer la version autonome d'Horizon Persona Management sur des ordinateurs physiques. Reportez-vous à la section [Systèmes d'exploitation pris en charge pour Horizon Persona Management autonome](#).

Note Pour utiliser le protocole d'affichage VMware Blast, vous devez installer Horizon Agent sur une machine virtuelle à session unique ou sur un hôte RDS. L'hôte RDS peut être une machine physique ou une machine virtuelle. Le protocole d'affichage VMware Blast ne fonctionne pas sur un ordinateur physique mono-utilisateur, à l'exception de l'édition Entreprise de Windows 10 RS4 et versions ultérieures.

Pour améliorer la sécurité, VMware recommande de configurer les suites de chiffrement afin de supprimer les vulnérabilités connues. Pour plus d'instructions sur la configuration d'une stratégie de domaine sur les suites de chiffrement pour les machines Windows qui exécutent View Composer ou Horizon Agent, reportez-vous à la section [Désactiver des chiffrements faibles dans les protocoles SSL/TLS](#).

Systèmes d'exploitation pris en charge pour Horizon Persona Management autonome

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

Note Pour configurer Persona Management pour les postes de travail Horizon, installez Horizon Agent avec l'option de configuration **Persona Management**. Le logiciel Persona Management autonome est conçu uniquement pour les systèmes non-Horizon.

Pour afficher la liste des systèmes d'exploitation pris en charge pour le logiciel Horizon Persona Management, consultez l'article de la base de connaissances de VMware <http://kb.vmware.com/kb/2150295>.

Le logiciel Persona Management autonome n'est pas pris en charge sur 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**

PCoIP (PC-over-IP) offre une expérience de poste de travail optimisée pour fournir une application publiée 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**

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.

- **VMware Blast Extreme**

Optimisé pour le cloud mobile, VMware Blast Extreme prend en charge la plus large gamme de périphériques clients compatibles avec H.264. De tous les protocoles d'affichage, VMware Blast est celui qui offre la consommation de CPU la plus faible pour une durée de vie de la batterie plus longue sur les périphériques mobiles. VMware Blast Extreme peut compenser une augmentation de la latence ou une réduction de la bande passante et peut exploiter les transports réseau TCP et UDP.

PCoIP

PCoIP (PC-over-IP) offre une expérience de poste de travail optimisée pour fournir une application publiée 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.

Le protocole d'affichage PCoIP peut être utilisé pour des applications publiées et des 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 ou un dispositif Access Point dans la zone DMZ de l'entreprise.
- Le cryptage AES (Advanced Encryption Standard) 128 bits est pris en charge et est activé par défaut. Vous pouvez toutefois modifier le chiffrement de clé de cryptage sur AES-256.
- Les connexions à des postes de travail Windows disposant des versions de système d'exploitation Horizon Agent répertoriées dans la section [Systèmes d'exploitation pris en charge pour Horizon Agent](#) 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 un poste de données distant ou une application publiée. 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. Sur certains clients, il est possible d'utiliser jusqu'à 4 moniteurs avec une résolution pouvant atteindre 2 560 x 1 600 par écran ou jusqu'à 3 moniteurs de résolution 4K (3 840 x 2 160) pour les postes de travail à distance Windows 7 dont l'option Aero est désactivée. La rotation d'affichage et l'ajustement automatique sont également pris en charge.

Lorsque la fonction 3D est activée, jusqu'à deux moniteurs peuvent être pris en charge avec une résolution allant jusqu'à 1 920 x 1 200 ou un moniteur avec une résolution 4K (3 840 x 2 160).

- 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 Horizon 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 au document *Planification de l'architecture Horizon 7*.

Pour plus d'informations sur les périphériques client prenant en charge des fonctions PCoIP spécifiques, allez sur <https://docs.vmware.com/fr/VMware-Horizon-Client/index.html>.

Paramètres de système d'exploitation client recommandés

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 vous voulez lire la vidéo en Flash haute définition ou en mode plein écran, le poste de travail requiert un CPU virtuel 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://docs.vmware.com/fr/VMware-Horizon-Client/index.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. (Seuls les protocoles d'affichage PCoIP et VMware Blast sont pris en charge pour les applications publiées.) Microsoft RDP fournit les fonctions suivantes :

- 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.

Pour prendre en charge les connexions TLSv1.1 et TLSv1.2 à Windows 7 et Windows Server 2008 R2, vous devez appliquer le correctif Microsoft KB3080079.

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://docs.vmware.com/fr/VMware-Horizon-Client/index.html>.

Note Les périphériques 3.x clients mobiles utilisent uniquement le protocole d'affichage PCoIP. Les clients 4.x clients mobiles utilisent uniquement le protocole d'affichage PCoIP ou VMware Blast.

VMware Blast Extreme

Optimisé pour le cloud mobile, VMware Blast Extreme prend en charge la plus large gamme de périphériques clients compatibles avec H.264. De tous les protocoles d'affichage, VMware Blast est celui qui offre la consommation de CPU la plus faible pour une durée de vie de la batterie plus longue sur les périphériques mobiles. VMware Blast Extreme peut compenser une augmentation de la latence ou une réduction de la bande passante et peut exploiter les transports réseau TCP et UDP.

Le protocole d'affichage VMware Blast peut être utilisé pour des applications publiées et pour des postes de travail distants qui utilisent des machines virtuelles ou des postes de travail à session partagée sur un hôte RDS. L'hôte RDS peut être une machine physique ou une machine virtuelle. Le protocole d'affichage VMware Blast ne fonctionne pas sur un ordinateur physique mono-utilisateur, à l'exception de l'édition Entreprise de Windows 10 RS4 et versions ultérieures.

Note Les films et les applications TV ne sont pas pris en charge pour les ordinateurs physiques exécutant Windows 10 RS4.

Fonctionnalités de VMware Blast Extreme

Les fonctionnalités clés de VMware Blast Extreme incluent les éléments suivants :

- Les utilisateurs à l'extérieur du pare-feu d'entreprise peuvent utiliser ce protocole avec le réseau privé virtuel (VPN) d'entreprise ou établir une connexion chiffrée et sécurisée avec un serveur de sécurité ou un dispositif Access Point dans la zone DMZ de l'entreprise.
- Le cryptage AES (Advanced Encryption Standard) 128 bits est pris en charge et est activé par défaut. Vous pouvez toutefois modifier le chiffrement de clé de cryptage sur AES-256.
- Les connexions à des postes de travail Windows disposant des versions de système d'exploitation Horizon Agent répertoriées dans la section [Systèmes d'exploitation pris en charge pour Horizon Agent](#) 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 compteurs de performances affichés à l'aide de PerfMon sur les agents Windows fournissent une représentation précise de l'état actuel du système qui s'actualise également à un rythme constant pour les éléments suivants :
 - Session Blast
 - Imagerie
 - Audio
 - CDR
 - USB : les compteurs USB affichés à l'aide de PerfMon sur les agents Windows sont valides si le trafic USB est configuré pour utiliser VVC (VMware Virtual Channel).
 - Skype Entreprise : les compteurs sont uniquement destinés au trafic de contrôle.
 - Presse-papiers
 - RTAV
 - Fonctionnalités de redirection de port série et de scanner
 - Impression virtuelle
 - HTML5 MMR
 - Windows Media MMR : les compteurs de performances s'affichent uniquement si vous avez configuré cette fonctionnalité pour utiliser VVC (VMware Virtual Channel).
- Continuité du réseau pendant une perte momentanée de réseau sur les clients Windows.
- 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 un poste de données distant ou une application publiée. 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. Sur certains clients, il est possible d'utiliser jusqu'à quatre moniteurs avec une résolution pouvant atteindre 2 560 x 1 600 par écran ou jusqu'à trois moniteurs avec une résolution 4K (3 840 x 2 160) pour les postes de travail distants Windows 7 dont l'option Aero est désactivée. La rotation d'affichage et l'ajustement automatique sont également pris en charge.

Lorsque la fonctionnalité 3D est activée, jusqu'à deux moniteurs peuvent être pris en charge avec une résolution pouvant atteindre 1 920 x 1 200 ou un moniteur avec une résolution 4K (3 840 x 2 160).

- 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 Horizon Agent est installé).
- Les connexions à des machines physiques sans moniteur sont prises en charge avec les cartes graphiques NVIDIA. Pour de meilleures performances, utilisez une carte graphique prenant en charge le codage H.264.

Si vous disposez d'un GPU discret de complément et d'un GPU intégré, le système d'exploitation peut être défini par défaut sur le GPU intégré. Pour résoudre ce problème, vous pouvez désactiver ou supprimer le périphérique dans le Gestionnaire de périphériques. Si le problème persiste, vous pouvez installer le pilote graphique WDDM pour le GPU intégré ou désactiver le GPU intégré dans le BIOS système. Consultez la documentation de votre système pour savoir comment désactiver le GPU intégré.



Attention La désactivation du GPU intégré peut entraîner une perte d'accès future à des fonctionnalités, telles que l'accès de la console à la configuration BIOS ou au chargeur de démarrage NT.

Pour plus d'informations sur les périphériques clients prenant en charge des fonctionnalités VMware Blast Extreme spécifiques, accédez à <https://docs.vmware.com/fr/VMware-Horizon-Client/index.html>.

Wake-on-LAN

Wake-on-LAN est pris en charge pour les machines physiques avec l'édition Entreprise de Windows 10 RS4 et versions ultérieures. Avec cette fonctionnalité, les utilisateurs peuvent réveiller des machines physiques lors de la connexion avec Horizon Connection Server. La fonctionnalité Wake-on-LAN présente les conditions préalables suivantes :

- Wake-on-LAN (WoL) n'est pris en charge que dans les environnements IPv4.
- La machine physique doit être configurée pour se réveiller lors de la réception de paquets Wake-on-LAN lorsque Wake-on-LAN est activé dans les paramètres du BIOS, ainsi que dans les paramètres de carte réseau.
- Le port de destination 9 est utilisé pour les paquets WoL provenant du Serveur de connexion.
- Les paquets WoL sont des paquets de diffusion dirigés par adresse IP qui doivent être en mesure d'atteindre Horizon Agent lorsqu'ils sont envoyés depuis Horizon Connection Server. Wake-on-LAN fonctionne dans les scénarios suivants :
 - Le Serveur de connexion et Horizon Agent sur la machine physique se trouvent sur le même sous-réseau dans un environnement LAN.
 - Tous les routeurs entre le Serveur de connexion et Horizon Agent sont configurés pour autoriser le paquet de diffusion dirigé par adresse IP pour le sous-réseau cible de la machine physique que vous voulez réveiller.

Note La fonctionnalité Wake-on-LAN ne prend pas en charge les pools d'attribution flottante d'un agent Windows 10 physique. Le paquet WoL n'est envoyé qu'à des pools d'attribution dédiée autorisés avec un utilisateur particulier.

Paramètres de système d'exploitation client recommandés

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 vous voulez lire la vidéo en Flash haute définition ou en mode plein écran, le poste de travail requiert un CPU virtuel 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 physiques sur un hôte vSphere ou de dédier un GPU physique à un seul poste de travail virtuel.

Pour les applications 3D, deux écrans maximum sont pris en charge et la résolution d'écran maximale est 1 920 x 1 200. Le système d'exploitation invité sur les postes de travail distants doit être Windows 7 ou version ultérieure.

Exigences matérielles des systèmes client

Pour plus d'informations sur les exigences en termes de processeur et de mémoire pour le type spécifique de poste de travail ou de périphérique client mobile, accédez à l'adresse <https://docs.vmware.com/fr/VMware-Horizon-Client/index.html>.

Installation de Horizon 7 dans un environnement IPv6

3

Horizon 7 prend en charge IPv6, en plus d'IPv4. L'environnement doit être exclusivement IPv6 ou exclusivement IPv4. Horizon 7 ne prend pas en charge un environnement mixte IPv6 et IPv4.

Certaines fonctionnalités Horizon 7 prises en charge dans les environnements IPv4 ne le sont pas dans les environnements IPv6. Horizon 7 ne prend pas en charge la mise à niveau d'un environnement IPv4 vers un environnement IPv6. En outre, Horizon 7 ne prend pas en charge de migrations entre les environnements IPv4 et IPv6.

Important Pour exécuter Horizon 7 dans un environnement IPv6, vous devez spécifier IPv6 lors de l'installation de tous les composants Horizon 7.

Ce chapitre contient les rubriques suivantes :

- [Configuration d'Horizon 7 dans un environnement IPv6](#)
- [Versions de vSphere, de base de données et d'Active Directory prises en charge dans un environnement IPv6](#)
- [Systèmes d'exploitation pris en charge pour les serveurs Horizon 7 dans un environnement IPv6](#)
- [Systèmes d'exploitation Windows pris en charge pour les postes de travail et les hôtes RDS dans un environnement IPv6](#)
- [Clients pris en charge dans un environnement IPv6](#)
- [Protocoles de communication à distance pris en charge dans un environnement IPv6](#)
- [Types d'authentification pris en charge dans un environnement IPv6](#)
- [Autres fonctionnalités prises en charge dans un environnement IPv6](#)

Configuration d' Horizon 7 dans un environnement IPv6

Pour exécuter Horizon 7 dans un environnement IPv6, vous devez connaître les conditions requises et les choix spécifiques à IPv6 lorsque vous effectuez certaines tâches administratives.

Avant d'installer Horizon 7, vous devez disposer d'un environnement IPv6 opérationnel. Les tâches administratives Horizon 7 suivantes ont des options spécifiques à IPv6.

- Installation du Serveur de connexion Horizon. Reportez-vous à la section [Installer le Serveur de connexion Horizon avec une nouvelle configuration](#).

- Installation du serveur réplica View. Reportez-vous à la section [Installer une instance répliquée du Serveur de connexion Horizon](#).
- Installation du serveur de sécurité View. Reportez-vous à la section [Installer un serveur de sécurité](#).
- Configuration de l'URL externe PCoIP. Reportez-vous à la section [Configuration d'URL externes pour Secure Gateway et les connexions par tunnel](#).
- Configuration de l'URL externe PCoIP. Reportez-vous à la section [Définir les URL externes d'une instance du Serveur de connexion](#).
- Déplacement de l'URL externe PCoIP. Reportez-vous à la section [Définir les URL externes d'une instance du Serveur de connexion](#).
- Installation d'Horizon Agent. Consultez les rubriques d'installation d'Horizon Agent du document *Configuration de pools de postes de travail et d'applications*.
- Installation d'Horizon Client. Reportez-vous à la section [Clients pris en charge dans un environnement IPv6](#).

Note Horizon 7 ne nécessite pas l'entrée d'une adresse IPv6 dans des tâches administratives. Lorsque vous pouvez indifféremment spécifier un nom de domaine complet ou une adresse IPv6, il est fortement recommandé de spécifier un nom de domaine complet pour éviter d'éventuelles erreurs.

Versions de vSphere, de base de données et d'Active Directory prises en charge dans un environnement IPv6

Dans un environnement IPv6, Horizon 7 prend en charge des versions spécifiques de vSphere, de serveur de base de données et d'Active Directory.

Les versions suivantes de vSphere sont prises en charge dans un environnement IPv6.

- 6.7
- 6.5 U2
- 6.5
- 6.0
- 5.5 U2

Les versions suivantes de serveur de base de données sont prises en charge dans un environnement IPv6.

Serveur de base de données	Version	Édition
SQL Server 2012 SP3	32/64 bits	Standard, Entreprise
SQL Server 2012 SP4	32/64 bits	Standard, Entreprise
SQL Server 2012 Express	32/64 bits	Libre
SQL Server 2014 alwayson	32/64 bits	Standard, Entreprise
SQL Server 2014 SP2	32/64 bits	Standard, Entreprise

Serveur de base de données	Version	Édition
SQL Server 2016	64 bits	Standard, Enterprise, Express
SQL Server 2016 AlwaysOn	64 bits	Standard, Enterprise, Express
SQL Server 2017	64 bits	Standard, Enterprise, Express, Developer
Oracle 11g R2	32/64 bits	Standard, Standard Edition One, Enterprise
Oracle 12c R2	32/64 bits	Standard, Standard Edition One, Enterprise

Les versions suivantes d'Active Directory sont prises en charge dans un environnement IPv6.

- Microsoft Active Directory 2008 R2
- Microsoft Active Directory 2012 R2

Systèmes d'exploitation pris en charge pour les serveurs Horizon 7 dans un environnement IPv6

Dans un environnement IPv6, vous devez installer des serveurs Horizon 7 sur des systèmes d'exploitation Windows Server spécifiques.

Les serveurs Horizon 7 incluent des instances du Serveur de connexion, des serveurs de réplica, des serveurs de sécurité et des instances de Horizon 7 Composer.

Système d'exploitation	Édition
Windows Server 2016	Standard, Entreprise
Windows Server 2008 R2 SP1	Standard, Entreprise
Windows Server 2012 R2	Standard

Systèmes d'exploitation Windows pris en charge pour les postes de travail et les hôtes RDS dans un environnement IPv6

Dans un environnement IPv6, Horizon 7 prend en charge des systèmes d'exploitation Windows spécifiques pour les machines de poste de travail et les hôtes RDS. Les hôtes RDS fournissent aux utilisateurs des applications et des postes de travail basés sur une session.

Les types et éditions des systèmes d'exploitation client pris en charge dépendent de la version de Windows. Pour obtenir les mises à jour de la liste de systèmes d'exploitation Windows 10 pris en charge, consultez l'article de la base de connaissances de VMware <http://kb.vmware.com/kb/2149393>. Pour les systèmes d'exploitation Windows autres que Windows 10, consultez l'article <http://kb.vmware.com/kb/2150295> dans la base de connaissances de VMware.

Pour voir la liste des fonctionnalités d'expérience à distance prises en charge sur les systèmes d'exploitation Windows sur lesquels Horizon Agent est installé, consultez l'article <http://kb.vmware.com/kb/2150305> dans la base de connaissances de VMware.

Clients pris en charge dans un environnement IPv6

Dans un environnement IPv6, Horizon 7 prend en charge les clients qui s'exécutent sur des systèmes d'exploitation de poste de travail spécifiques.

Tableau 3-1. Systèmes d'exploitation Windows pris en charge

Système d'exploitation	Version	Édition
Windows 7 et Windows 7 SP1	32 bits ou 64 bits	Home, Entreprise, Professionnel et Ultimate
Windows 8 et Windows 8.1	32 bits ou 64 bits	Pro , Entreprise et Industry Embedded
Windows 10	32 bits ou 64 bits	Famille, Professionnel, Professionnel pour stations de travail, Entreprise et IoT entreprise

Sur les périphériques iOS, iOS 9.2 ou version ultérieure est pris en charge avec Horizon Client 4.1 ou version ultérieure.

Sur les périphériques Android et macOS, Horizon Client 4.9 ou version ultérieure est requis.

Les types de clients suivants ne sont pas pris en charge.

- Clients qui s'exécutent sur Linux, Chrome OS, Windows 10 UWP ou Windows Store
- iOS 9.1 ou version antérieure
- Client ultra léger PColP

Protocoles de communication à distance pris en charge dans un environnement IPv6

Dans un environnement IPv6, Horizon 7 prend en charge des protocoles de communication à distance spécifiques.

Les types de protocoles de communication à distance suivants sont pris en charge :

- RDP
- RDP avec tunnel sécurisé
- PColP
- PColP via PColP Secure Gateway
- VMware Blast
- VMware Blast via Blast Secure Gateway
- Blast Extreme Adaptive Transport (BEAT)

Types d'authentification pris en charge dans un environnement IPv6

Dans un environnement IPv6, Horizon 7 prend en charge des types d'authentification spécifique.

Les types d'authentification suivants sont pris en charge :

- Authentification par mot de passe à l'aide d'Active Directory
- Carte à puce
- Single Sign-On

Les types d'authentification suivants ne sont pas pris en charge :

- SecurID
- RADIUS
- SAML

Autres fonctionnalités prises en charge dans un environnement IPv6

Dans un environnement IPv6, Horizon 7 prend en charge certaines fonctionnalités qui ne sont pas mentionnées dans les rubriques précédentes.

Les fonctionnalités suivantes sont prises en charge :

- Pools d'applications
- Sortie audio
- Pools de postes de travail automatisés de machines virtuelles complètes ou clones liés Horizon 7 Composer

Note Les pools de postes de travail automatisés d'Instant Clones ne sont pas pris en charge.

- Blast Extreme Adaptive Transport (BEAT)
- Programme d'amélioration du produit (customer experience improvement program, CEIP)
- Récupération d'espace disque
- Événements
- Redirection multimédia HTML5
- Sauvegarde LDAP
- Pools de postes de travail manuels, notamment les machines virtuelles vCenter Server, les ordinateurs physiques et les machines virtuelles non gérées par vCenter Server
- snapshots NFS natifs (VAAI)
- Horizon Performance Tracker
- Gestion de persona
- Pools de postes de travail RDS
- Hôte RDS 3D

- Administration basée sur des rôles
- Collaboration de session
- Single Sign-on, notamment la fonctionnalité Se connecter en tant qu'utilisateur actuel
- Tableau de bord de santé du système
- ThinApp
- Unity Touch
- redirection USB
- Horizon 7 Composer Agent
- Horizon 7 Storage Accelerator
- Sauvegarde de base de données Horizon 7 Composer
- Impression virtuelle
- Audio VMware
- Vidéo VMware
- Pack de virtualisation VMware pour Skype Entreprise

Les fonctionnalités suivantes ne sont pas prises en charge :

- Redirection de lecteur client
- Transparence IP de client (uniquement 64 bits)
- Architecture Cloud Pod
- Pont de périphérique
- Association de fichiers
- Redirection d'URL Flash
- accès HTML
- Log Insight
- Lync
- Audio/Vidéo en temps réel (RTAV)
- Redirection de scanner
- Redirection de port série
- Syslog
- Carte hôte TERA Teradici
- TSMRR
- Redirection d'URL
- vSAN

- Volumes virtuels
- vRealize Operations Desktop Agent
- Pack de virtualisation VMware pour Skype Entreprise en mode de secours

Installation d' Horizon 7 en mode FIPS

4

Horizon 7 peut effectuer des opérations cryptographiques à l'aide d'algorithmes compatibles FIPS (Federal Information Processing Standard, norme de traitement d'informations fédérales) 140-2. Il est possible d'activer l'utilisation de ces algorithmes en installant Horizon 7 en mode FIPS.

Le mode FIPS ne prend pas en charge toutes les fonctionnalités d'Horizon 7. De plus, Horizon 7 ne prend pas en charge la mise à niveau depuis une installation non-FIPS vers une installation FIPS.

Note Afin de s'assurer qu'Horizon 7 s'exécute en mode FIPS, vous devez activer FIPS lorsque vous installez tous les composants d'Horizon 7.

Ce chapitre contient les rubriques suivantes :

- [Présentation de la configuration d'Horizon 7 en mode FIPS](#)
- [Configuration requise pour le mode FIPS](#)

Présentation de la configuration d' Horizon 7 en mode FIPS

Pour configurer Horizon 7 en mode FIPS, vous devez tout d'abord activer le mode FIPS dans l'environnement Windows. Installez ensuite tous les composants d'Horizon 7 en mode FIPS.

L'option permettant d'installer Horizon 7 en mode FIPS n'est disponible que si le mode FIPS est activé dans l'environnement Windows. Pour plus d'informations sur l'activation du mode FIPS sous Windows, consultez <https://support.microsoft.com/en-us/kb/811833>.

Note Horizon Administrator n'indique pas si Horizon 7 est exécuté en mode FIPS.

Pour installer Horizon 7 en mode FIPS, effectuez les tâches administratives suivantes.

- Lors de l'installation du Serveur de connexion, sélectionnez l'option du mode FIPS. Reportez-vous à la section [Installer le Serveur de connexion Horizon avec une nouvelle configuration](#).
- Lors de l'installation d'un serveur réplique, sélectionnez l'option du mode FIPS. Reportez-vous à la section [Installer une instance répliquée du Serveur de connexion Horizon](#).
- Avant d'installer un serveur de sécurité, désélectionnez le paramètre global **Utiliser IPSec pour les connexions du serveur de sécurité** dans Horizon Administrator et configurez IPsec manuellement. Reportez-vous à la section <http://kb.vmware.com/kb/2000175>.

- Lors de l'installation d'un serveur de sécurité, sélectionnez l'option du mode FIPS. Reportez-vous à la section [Installer un serveur de sécurité](#).
- Lorsqu'un système Windows est configuré pour l'opération FIPS et qu'Horizon 7 est configuré pour communiquer entre un Serveur de connexion et un serveur de sécurité avec IPSec, l'installation du serveur de sécurité échoue. Dans un environnement IPv4, spécifiez l'URL externe PCoIP sous la forme d'une adresse IP avec le numéro de port 4172. Dans un environnement IPv6, vous pouvez spécifier une adresse IP ou un nom de domaine complet, et le numéro de port 4172. Dans les deux cas, n'incluez pas de nom de protocole.

Par exemple, dans un environnement IPv4 : 10.20.30.40:4172

Les clients doivent pouvoir utiliser l'URL pour accéder au serveur de sécurité.

- Désactivez les chiffrements faibles pour les machines View Composer et Horizon Agent. Reportez-vous à la section [Désactiver des chiffrements faibles dans les protocoles SSL/TLS](#).
- Lors de l'installation de View Composer, sélectionnez l'option du mode FIPS. Reportez-vous à la section [Chapitre 6 Installation de View Composer](#).
- Lors de l'installation d'Horizon Agent, sélectionnez l'option du mode FIPS. Consultez les rubriques d'installation d'Horizon Agent dans le document *Configuration des postes de travail virtuels dans Horizon 7* ou *Configuration d'applications et de postes de travail publiés dans Horizon 7*.
- Pour les clients Windows, activez le mode FIPS sur le système d'exploitation client et sélectionnez l'option du mode FIPS lors de l'installation Horizon Client pour Windows. Reportez-vous au document *Guide d'installation et de configuration de VMware Horizon Client pour Windows*.
- Pour les clients Linux, activez le mode FIPS sur le système d'exploitation client. Reportez-vous au document *Guide d'installation et de configuration de VMware Horizon Client pour Linux*.

Configuration requise pour le mode FIPS

Pour prendre en charge le mode FIPS, votre déploiement de Horizon 7 doit satisfaire aux exigences suivantes.

vSphere

- vCenter Server 6.0 ou une version ultérieure
- ESXi 6.0 ou une version ultérieure

Poste de travail distant

- Toutes les plates-formes Windows qui possèdent un certificat FIPS. Pour plus d'informations, reportez-vous à la section « Validation de FIPS 140 » sur le site Web Microsoft TechNet.
- View Agent 6.2 ou version ultérieure ou Horizon Agent 7.0 ou version ultérieure, pour les plates-formes Windows uniquement

Horizon Client

- Toutes les plates-formes Windows qui possèdent un certificat FIPS. Pour plus d'informations, reportez-vous à la section « Validation de FIPS 140 » sur le site Web Microsoft TechNet.

**Protocole
cryptographique**

- Horizon Client pour Windows 3.5 ou version ultérieure
- TLSv1.2

Préparation d'Active Directory

Horizon 7 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 Horizon 7.

Horizon 7 prend en charge les niveaux fonctionnels de domaine des services de domaine Active Directory (AD DS) suivants :

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Ce chapitre contient les rubriques suivantes :

- [Configuration de domaines et de relations d'approbation](#)
- [Création d'une UO pour des postes de travail distants](#)
- [Création d'UO et de groupes pour des comptes de client en mode kiosque](#)
- [Création de groupes pour les utilisateurs](#)
- [Création d'un compte d'utilisateur pour vCenter Server](#)
- [Création d'un compte d'utilisateur pour un serveur View Composer Server autonome](#)
- [Créer un compte d'utilisateur pour les opérations AD de View Composer](#)
- [Créer un compte d'utilisateur pour les opérations Instant Clone](#)
- [Configurer la stratégie Groupes restreints](#)
- [Utilisation des fichiers de modèle d'administration de stratégie de groupe Horizon 7](#)
- [Préparer Active Directory pour l'authentification par carte à puce](#)
- [Désactiver des chiffrements faibles dans les protocoles SSL/TLS](#)

Configuration de domaines et de relations d'approbation

Vous devez associer chaque hôte du Serveur de connexion à un domaine Active Directory. L'hôte ne doit pas être un contrôleur de domaine.

Active Directory gère également les machines Horizon Agent, notamment les machines mono-utilisateur et les hôtes RDS, ainsi que les utilisateurs et les groupes dans votre déploiement d'Horizon 7. Vous pouvez autoriser des utilisateurs et des groupes à accéder à des applications et des postes de travail distants, et vous pouvez sélectionner des utilisateurs et des groupes comme administrateurs dans Horizon Administrator.

Vous pouvez placer des machines Horizon Agent, des serveurs View Composer, des utilisateurs et des groupes, dans les domaines Active Directory suivants :

- Le domaine du Serveur de connexion
- Un domaine différent ayant une relation de confiance bidirectionnelle avec le domaine du Serveur de connexion
- Un domaine dans une forêt différente de celle du domaine du Serveur de connexion qui est approuvée par le domaine du Serveur de connexion dans une relation de confiance unidirectionnelle externe ou de domaine
- Un domaine dans une forêt différente de celle du domaine du Serveur de connexion qui est approuvée par le domaine du Serveur de connexion dans une relation de confiance de forêt transitive unidirectionnelle ou bidirectionnelle

Les utilisateurs sont authentifiés à l'aide d'Active Directory par le domaine du Serveur de connexion et par des domaines d'utilisateurs supplémentaires avec lesquels un accord d'approbation existe.

Si vos utilisateurs et vos groupes se trouvent dans des domaines approuvés unidirectionnels, vous devez fournir des informations d'identification secondaires pour les utilisateurs administrateurs dans Horizon Administrator. Les administrateurs doivent disposer d'informations d'identification secondaires pour pouvoir accéder aux domaines approuvés unidirectionnels. Un domaine approuvé unidirectionnel peut être un domaine externe ou un domaine dans une approbation de forêt transitive.

Les informations d'identification secondaires sont requises uniquement pour les sessions Horizon Administrator, pas pour les sessions de poste de travail ou d'application des utilisateurs finaux. Seuls les utilisateurs administrateurs requièrent des informations d'identification secondaires.

Vous pouvez fournir des informations d'identification secondaires en utilisant la commande `vdmadmin -T`.

- Vous configurez des informations d'identification secondaires pour des utilisateurs administrateurs individuels.
- Pour une approbation de forêt, vous pouvez configurer des informations d'identification secondaires pour le domaine racine de forêt. Le Serveur de connexion peut ensuite énumérer les domaines enfants dans l'approbation de forêt.

Pour plus d'informations, reportez-vous à la section « Fournir des informations d'identification secondaires aux administrateurs à l'aide de l'option -T » dans le document *Administration d'Horizon 7*.

L'authentification par carte à puce et SAML des utilisateurs n'est pas prise en charge dans les domaines approuvés unidirectionnels.

Note 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 du Serveur de connexion traverse des relations d'approbation en commençant par son propre domaine.

Pour un petit ensemble de domaines bien connectés, le Serveur de connexion peut déterminer rapidement la liste complète de domaines, mais le temps que cela prend augmente, car le nombre de domaines s'accroît ou 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 du Serveur de connexion recherche et qu'elle affiche aux utilisateurs. Consultez le document *Administration d'Horizon 7* pour plus d'informations.

Si une approbation de forêt est configurée avec des exclusions de suffixe de noms, les exclusions configurées sont utilisées pour filtrer la liste de domaines enfants de forêt. Le filtrage d'exclusion de suffixe de noms est appliqué en plus du filtrage spécifié avec la commande `vdmadmin`.

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'Horizon 7 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 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.

Consultez le document *Administration d'Horizon 7* 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 Horizon 7 pour vos utilisateurs finaux et un autre groupe nommé Administrateurs de Horizon 7 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 Horizon Administrator.

Vous devez accorder au compte d'utilisateur les privilèges pour effectuer certaines opérations dans vCenter Server. Vous pouvez créer un rôle vCenter Server avec des privilèges appropriés et attribuer ce rôle à l'utilisateur de vCenter Server. La liste de privilèges que vous ajoutez au rôle de vCenter Server varie, selon que vous utilisez Horizon 7 avec ou sans View Composer. Reportez-vous à la section [Configuration de comptes utilisateur pour vCenter Server, View Composer et les clones instantanés](#) pour plus d'informations sur la configuration de ces privilèges.

Si vous installez View Composer sur la même machine que vCenter Server, vous devez ajouter l'utilisateur de vCenter Server au groupe Administrateurs local sur la machine vCenter Server. Cette exigence permet à Horizon 7 de s'authentifier sur le service View Composer.

Si vous installez View Composer sur une autre machine que vCenter Server, vous n'avez pas besoin de définir l'utilisateur de vCenter Server comme un administrateur local sur la machine vCenter Server. Cependant, vous devez créer un compte d'utilisateur de serveur View Composer Server autonome qui doit être un administrateur local sur la machine View Composer.

Création d'un compte d'utilisateur pour un serveur View Composer Server autonome

Si vous n'installez pas View Composer sur la même machine que vCenter Server, vous devez créer un compte d'utilisateur de domaine dans Active Directory que Horizon 7 peut utiliser pour s'authentifier sur le service View Composer de la machine autonome.

Le compte d'utilisateur doit se trouver dans le même domaine que votre hôte du Serveur de connexion ou dans un domaine approuvé. Vous devez ajouter le compte d'utilisateur au groupe Administrateurs local sur la machine View Composer autonome.

Vous spécifiez ce compte d'utilisateur lorsque vous configurez les paramètres de View Composer dans Horizon Administrator et sélectionnez **Serveur View Composer Server autonome**. Reportez-vous à la section [Configurer les paramètres de View Composer](#).

Créer un compte d'utilisateur pour les opérations AD de View Composer

Si vous utilisez View Composer, vous devez créer un compte d'utilisateur dans Active Directory qui permet à View Composer d'effectuer certaines opérations dans Active Directory. 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 du Serveur de connexion 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

Note Le nombre d'autorisations requises est moins important si vous sélectionnez le paramètre **Autoriser la réutilisation de comptes d'ordinateurs préexistants** pour un pool de postes de travail. Assurez-vous que les autorisations suivantes sont attribuées au compte d'utilisateur :

- 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.

Étape suivante

Spécifiez le compte dans Horizon Administrator lorsque vous configurez des domaines View Composer dans l'assistant d'ajout d'une instance de vCenter Server et lorsque vous configurez et déployez des pools de postes de travail de clone lié.

Créer un compte d'utilisateur pour les opérations Instant Clone

Avant de déployer des clones instantanés, vous devez créer un compte d'utilisateur qui possède l'autorisation d'effectuer certaines opérations dans Active Directory.

Sélectionnez ce compte lorsque vous ajoutez un administrateur de domaine Instant Clone avant de déployer des pools de postes de travail Instant Clone. Pour plus d'informations, consultez « Ajouter un administrateur de domaine Instant Clone » dans le document *Configuration des postes de travail virtuels dans Horizon 7*.

Procédure

- 1 Dans Active Directory, créez un compte d'utilisateur dans le même domaine que le serveur de connexion ou dans un domaine approuvé.
- 2 Ajoutez les autorisations **Créer des objets ordinateur**, **Supprimer des objets ordinateur** et **Écrire toutes les propriétés** au compte du conteneur pour les comptes d'ordinateur Instant Clone.

La liste suivante montre 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

Assurez-vous que les autorisations s'appliquent au bon conteneur et à tous les objets enfants du conteneur.

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.

Conditions préalables

Créez un groupe pour les utilisateurs de postes de travail distants de votre domaine dans Active Directory.

Procédure

- 1 Sur le serveur Active Directory, accédez au plug-in de gestion de stratégie de groupe.

Version d'AD	Chemin de navigation
Windows 2003	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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.

Version d'AD	Chemin de navigation
Windows 2012 R2	<ol style="list-style-type: none"> 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.
Windows 2016	<ol style="list-style-type: none"> 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 Horizon 7

Horizon 7 inclut plusieurs fichiers de modèle d'administration (ADMX) de stratégie de groupe spécifiques d'un composant.

Tous les fichiers ADMX qui fournissent les paramètres de stratégie de groupe pour Horizon 7 sont disponibles dans VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip, où x.x.x est la version et yyyyyy le numéro de build. Vous pouvez télécharger le fichier sur le site de téléchargements de VMware à l'adresse <https://my.vmware.com/web/vmware/downloads>. Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut le fichier ZIP.

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.

Pour plus d'informations sur l'utilisation des paramètres de stratégie de groupe d'Horizon 7, consultez les documents *Administration d'Horizon 7* et *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

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**

Comme les ouvertures de session par carte à puce reposent sur des noms d'utilisateur principaux (UPN), les comptes Active Directory d'utilisateurs et d'administrateurs qui utilisent des cartes à puce pour s'authentifier dans Horizon 7 doivent avoir un UPN valide.

- **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.

- **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.

- **Ajouter le certificat racine au magasin Enterprise NTAAuth**

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 NTAAuth 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 Active Directory d'utilisateurs et d'administrateurs qui utilisent des cartes à puce pour s'authentifier dans Horizon 7 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.

Note 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.

Conditions préalables

- 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, accédez au plug-in de gestion de stratégie de groupe.

Version d'AD	Chemin de navigation
Windows 2003	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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.
Windows 2012 R2	<ol style="list-style-type: none"> 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.
Windows 2016	<ol style="list-style-type: none"> 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.

Étape suivante

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](#).

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, accédez au plug-in de gestion de stratégie de groupe.

Version d'AD	Chemin de navigation
Windows 2003	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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.

Version d'AD	Chemin de navigation
Windows 2012 R2	<ol style="list-style-type: none"> Sélectionnez Démarrer > Outils d'administration > Gestion de stratégie de groupe. Développez votre domaine, cliquez avec le bouton droit sur Stratégie de domaine par défaut et cliquez sur Modifier.
Windows 2016	<ol style="list-style-type: none"> Sélectionnez Démarrer > Outils d'administration > Gestion de stratégie de groupe. Développez votre domaine, cliquez avec le bouton droit sur Stratégie de domaine par défaut et cliquez sur Modifier.

- Développez la section **Configuration ordinateur** et ouvrez la stratégie de **Paramètres Windows\Paramètres de sécurité\Clé publique**.
- Cliquez avec le bouton droit sur **Autorités de certification intermédiaires** et sélectionnez **Importer**.
- Suivez les invites de l'assistant pour importer le certificat intermédiaire (par exemple, `intermediateCA.cer`) et cliquez sur **OK**.
- 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 NTAAuth

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 NTAAuth 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 NTAAuth.

Par exemple : `certutil -dspublish -f path_to_root_CA_cert NTAAuthCA`

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

Désactiver des chiffrements faibles dans les protocoles SSL/TLS

Pour améliorer la sécurité, il est possible de configurer le GPO (objet de stratégie de groupe) de la stratégie du domaine afin de s'assurer que les machines View Composer et Windows exécutant View Agent ou Horizon Agent n'utilisent pas de chiffrements faibles lorsqu'elles communiquent à l'aide du protocole SSL/TLS.

Procédure

- 1 Sur le serveur Active Directory, modifiez les objets de stratégie de groupe (GPO) en sélectionnant **Démarrer > Outils d'administration > Gestion de stratégie de groupe**, puis en cliquant avec le bouton droit sur GPO et en sélectionnant **Édition**.
- 2 Dans l'éditeur de la gestion des stratégies du groupe accédez à **Configuration de l'ordinateur > Stratégies > Modèles d'administration > Réseau > Paramètres de configuration SSL**.
- 3 Double-cliquez sur **Ordre des suites de chiffrement SSL**.
- 4 Dans la fenêtre Ordre des suites de chiffrement SSL cliquez sur **Activé**.
- 5 Dans le volet Options, remplacez la totalité du contenu du champ Suites de chiffrement SSL avec la liste de chiffrement suivante :

```
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA
```

Les suites de chiffrement sont répertoriées ci-dessus sur des lignes distinctes pour plus de clarté. Lorsque vous collez la liste dans le champ de texte, les suites de chiffrement doivent être sur une même ligne, sans espaces après les virgules.

- 6 Quittez l'éditeur de la gestion des règles du groupe.
- 7 Redémarrez les machines View Composer et View Agent ou Horizon Agent pour que la nouvelle stratégie de groupe prenne effet.

Installation de View Composer

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.

Note Avant d'installer View Composer, vérifiez que vous avez préparé Active Directory.

Ce chapitre contient les rubriques suivantes :

- [Préparer une base de données View Composer](#)
- [Configuration d'un certificat SSL pour View Composer](#)
- [Installer le service View Composer](#)
- [Activer TLSv1.0 sur des connexions vCenter et ESXi depuis View Composer](#)
- [Configuration de votre infrastructure pour View Composer](#)

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 et la base de données d'événements](#).

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](#)

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](#)

View Composer peut stocker des informations de poste de travail de clone lié dans une base de données Oracle 12c ou 11g. 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.

Procédure

1 [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.

2 [\(Facultatif\) Définir les autorisations de base de données SQL Server en créant manuellement des rôles de base de données](#)

En utilisant cette méthode recommandée, l'administrateur de la base de données View Composer peut définir des autorisations pour les administrateurs View Composer à accorder par le biais de rôles de base de données Microsoft SQL Server.

3 [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.

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.

Conditions préalables

- 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 [Exigences de base de données pour View Composer et la base de données d'événements](#).
- Vérifiez que vous utilisez SQL Server Management Studio pour créer et administrer la base de données. Vous pouvez également utiliser SQL Server Management Studio Express, que vous pouvez télécharger et installer depuis le site Web suivant.

<http://www.microsoft.com/en-us/download/details.aspx?id=7593>

Procédure

- 1 Sur l'ordinateur View Composer, sélectionnez **Démarrer > Tous les programmes > Microsoft SQL Server 2014, Microsoft SQL Server 2012 ou Microsoft SQL Server 2008**.

- 2 Sélectionnez **SQL Server Management Studio** et connectez-vous à l'instance de SQL Server.

- 3 Dans le volet Explorateur d'objets, cliquez avec le bouton droit sur l'entrée Bases de données et sélectionnez **Nouvelle base de données**.

Vous pouvez utiliser les valeurs par défaut pour les paramètres Initial size et Autogrowth de la base de données et des fichiers journaux.

- 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 ajoute votre base de données à l'entrée Bases de données du volet Explorateur d'objets.

- 6 Quittez Microsoft SQL Server Management Studio.

Étape suivante

Facultativement, suivez les instructions de la section ([Facultatif](#)) [Définir les autorisations de base de données SQL Server en créant manuellement des rôles de base de données](#)

Suivez les instructions de la section [Ajouter une source de données ODBC à SQL Server](#).

(Facultatif) Définir les autorisations de base de données SQL Server en créant manuellement des rôles de base de données

En utilisant cette méthode recommandée, l'administrateur de la base de données View Composer peut définir des autorisations pour les administrateurs View Composer à accorder par le biais de rôles de base de données Microsoft SQL Server.

VMware recommande cette méthode car elle évite d'avoir à configurer le rôle **db_owner** pour les administrateurs View Composer qui installent et mettent à niveau View Composer.

Dans cette procédure, vous pouvez fournir vos propres choix pour le nom de connexion à la base de données, le nom d'utilisateur et les rôles de base de données. L'utilisateur **[vcmpuser]** et les rôles de base de données, **VCMP_ADMIN_ROLE** et **VCMP_USER_ROLE**, sont des exemples de noms. Le schéma **dbo** est créé lorsque vous créez la base de données View Composer. Vous devez utiliser le nom de schéma **dbo**.

Conditions préalables

- Vérifiez qu'une base de données View Composer est créée. Reportez-vous à la section [Ajouter une base de données View Composer à SQL Server](#).

Procédure

- 1 Connectez-vous à une session Microsoft SQL Server Management Studio en tant que sysadmin (SA) ou avec un compte d'utilisateur ayant les privilèges **sysadmin**.
- 2 Créez un utilisateur qui obtiendra les autorisations de bases de données SQL Server appropriées.

```
use ViewComposer
go
CREATE LOGIN [vcmpuser] WITH PASSWORD=N'vcmpuser!0', DEFAULT_DATABASE=ViewComposer,
DEFAULT_LANGUAGE=us_english, CHECK_POLICY=OFF
go
CREATE USER [vcmpuser] for LOGIN [vcmpuser]
go
use MSDB
go
CREATE USER [vcmpuser] for LOGIN [vcmpuser]
go
```

- 3 Dans la base de données View Composer, créez le rôle de base de données **VCMP_ADMIN_ROLE**.
- 4 Dans la base de données View Composer, accordez des privilèges au rôle **VCMP_ADMIN_ROLE**.
 - a Accordez les autorisations de schéma **ALTER**, **REFERENCES** et **INSERT** sur le schéma **dbo**.
 - b Accordez les autorisations **CREATE TABLE**, **CREATE VIEW** et **CREATE PROCEDURES**.
- 5 Dans la base de données View Composer, créez le rôle **VCMP_USER_ROLE**.
- 6 Dans la base de données View Composer, accordez les autorisations de schéma **SELECT**, **INSERT**, **DELETE**, **UPDATE** et **EXECUTE** sur le schéma **dbo** au rôle **VCMP_USER_ROLE**.

- 7 Accordez le rôle **VCMP_USER_ROLE** à l'utilisateur **[vcmpuser]**.
- 8 Accordez le rôle **VCMP_ADMIN_ROLE** à l'utilisateur **[vcmpuser]**.
- 9 Dans la base de données MSDB, créez le rôle de base de données **VCMP_ADMIN_ROLE**.
- 10 Accordez des privilèges au rôle **VCMP_ADMIN_ROLE** dans MSDB.
 - a Dans les tables MSDB syscategories, sysjobsteps et sysjobs, accordez l'autorisation **SELECT** à l'utilisateur **[vcmpuser]**.
 - b Dans les procédures stockées MSDB sp_add_job, sp_delete_job, sp_add_jobstep, sp_update_job, sp_add_jobserver, sp_add_jobschedule et sp_add_category, accordez l'autorisation **EXECUTE** au rôle **VC_ADMIN_ROLE**.
- 11 Dans la base de données MSDB, accordez le rôle **VCMP_ADMIN_ROLE** à l'utilisateur **[vcmpuser]**.
- 12 Créez le DSN ODBC à l'aide de l'identifiant de connexion SQL Server **vcmpuser**.
- 13 Installez View Composer.
- 14 Dans la base de données MSDB, révoquez le rôle **VC_ADMIN_ROLE** à l'utilisateur **[vcmpuser]**.
Après avoir révoqué le rôle, vous pouvez le conserver inactif ou le supprimer pour plus de sécurité.

Pour la procédure de création d'un DSN ODBC, reportez-vous à [Ajouter une source de données ODBC à SQL Server](#).

Pour la procédure d'installation de View Composer, reportez-vous à [Installer le service View Composer](#).

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.

Conditions préalables

Effectuez les étapes décrites dans la section [Ajouter une base de données View Composer à SQL Server](#).

Procédure

- 1 Sur l'ordinateur sur lequel View Composer sera installé, sélectionnez **Démarrer > Outils d'administration > Sources 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
Intégrer l'authentification Windows	Sélectionnez cette option si vous utilisez une instance locale de SQL Server. Cette option est aussi connue sous le nom d'authentification approuvée. Intégrer l'authentification Windows est pris 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. Si vous définissez manuellement des autorisations de base de données SQL Server et les avez attribuées à un utilisateur, authentifiez-vous avec cet utilisateur. Par exemple, authentifiez-vous avec l'utilisateur vcmpuser . Sinon, authentifiez-vous en tant que sysadmin (SA) ou un compte d'utilisateur disposant des privilèges sysadmin .

- 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**.

Étape suivante

Installez le nouveau service View Composer. Reportez-vous à la section [Installer le service View Composer](#).

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 12c ou 11g. 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 12c ou 11g](#)

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 12c ou 11g existante.

- [Utiliser une instruction SQL pour ajouter une base de données View Composer à une instance d'Oracle](#)

- [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.

- [Ajouter une source de données ODBC à Oracle 12c ou 11g](#)

Lorsque vous avez ajouté une base de données View Composer à une instance d'Oracle 12c ou 11g, 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 12c ou 11g

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 12c ou 11g existante.

Conditions préalables

Vérifiez qu'une version prise en charge d'Oracle 12c ou 11g est installée sur l'ordinateur local ou distant. Reportez-vous à la section [Exigences de base de données pour View Composer et la base de données d'événements](#).

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 12c	Sélectionnez Démarrer > Tous les programmes > Oracle-OraDb12c_home > Outils de configuration et de migration > Assistant de configuration de base de données.
Oracle 11g	Sélectionnez Démarrer > Tous les programmes > Oracle-OraDb11g_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**.

Étape suivante

Suivez les instructions de la section [Ajouter une source de données ODBC à Oracle 12c ou 11g](#).

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

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

Conditions préalables

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 12c ou 11g.

Vérifiez qu'une version prise en charge d'Oracle 12c ou 11g est installée sur l'ordinateur local ou distant. Pour plus d'informations, reportez-vous à [Exigences de base de données pour View Composer et la base de données d'événements](#).

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.

Étape suivante

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](#).

Suivez les instructions de la section [Ajouter une source de données ODBC à Oracle 12c ou 11g](#)

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.

Conditions préalables

Vérifiez qu'une base de données View Composer a été créée dans une instance d'Oracle 12c ou 11g.

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 12c ou 11g

Lorsque vous avez ajouté une base de données View Composer à une instance d'Oracle 12c ou 11g, 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.

Conditions préalables

Vérifiez que vous avez effectué les étapes décrites dans la section [Ajouter une base de données View Composer à Oracle 12c ou 11g](#) ou [Utiliser une instruction SQL pour ajouter une base de données View Composer à une instance d'Oracle](#).

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.

Note 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**.

Étape suivante

Installez le nouveau service View Composer. Reportez-vous à la section [Installer le service View Composer](#).

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 8 Configuration de certificats TLS pour des serveurs Horizon 7](#).

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. Horizon 7 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 une même machine virtuelle ou physique avec d'autres composants logiciels d'Horizon 7, y compris un serveur réplica, un serveur de sécurité, un Serveur de connexion, Horizon Agent ou Horizon Client.

Pour améliorer la sécurité, nous recommandons de configurer les suites de chiffrement afin de supprimer les vulnérabilités connues. Pour plus d'instructions sur la configuration d'une stratégie de domaine sur les suites de chiffrement pour les machines Windows qui exécutent View Composer ou Horizon Agent, reportez-vous à la section [Désactiver des chiffrements faibles dans les protocoles SSL/TLS](#).

Conditions préalables

- Vérifiez que votre installation répond aux exigences de View Composer décrites dans la section [Exigences de View Composer](#)
- Vérifiez qu'aucun autre composant d'Horizon 7, notamment Serveur de connexion, serveur de sécurité, Horizon Agent ou Horizon Client, n'est installé sur la machine sur laquelle vous prévoyez d'installer View Composer.
- 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 8 Configuration de certificats TLS pour des serveurs Horizon 7](#).
- 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 disposer de 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**

Note 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 Horizon 7. Pour plus d'informations sur la gestion des suites de chiffrement, consultez votre documentation Microsoft.

Étape suivante

Si vous disposez d'une version antérieure de vCenter Server, reportez-vous à la section [Activer TLSv1.0 sur des connexions vCenter et ESXi depuis View Composer](#).

Si vous définissez manuellement des autorisations de base de données SQL Server et les attribuez à un utilisateur, vous pouvez révoquer à cet utilisateur le rôle d'administrateur de base de données. Pour plus de détails, reportez-vous à la dernière étape de la procédure de la section [\(Facultatif\) Définir les autorisations de base de données SQL Server en créant manuellement des rôles de base de données](#).

Activer TLSv1.0 sur des connexions vCenter et ESXi depuis View Composer

Le protocole de sécurité TLSv1.0 est désactivé par défaut sur les composants d'Horizon 7 et versions ultérieures. Si votre déploiement inclut une version antérieure de vCenter Server qui prend en charge uniquement TLSv1.0, vous devrez peut-être activer TLSv1.0 pour les connexions de View Composer après avoir installé ou effectué une mise à niveau vers View Composer 7.0 ou une version ultérieure.

Certaines versions de maintenance antérieures de vCenter Server 5.0, 5.1 et 5.5 ne prennent en charge que TLSv1.0, qui n'est plus activé par défaut dans Horizon 7 et versions ultérieures. S'il n'est pas possible de mettre à niveau vCenter Server vers une version prenant en charge TLSv1.1 ou TLSv1.2, vous pouvez activer TLSv1.0 pour les connexions de View Composer.

Si vos hôtes ESXi n'exécutent pas ESXi 6.0 U1b ou version ultérieure, et si vous ne pouvez pas effectuer la mise à niveau, vous devrez peut-être activer les connexions TLSv1.0 aux hôtes ESXi depuis View Composer.

Conditions préalables

- Vérifiez que View Composer 7.0 ou une version ultérieure est installé.
- Vérifiez que vous pouvez vous connecter à la machine View Composer en tant qu'administrateur pour utiliser l'Éditeur du Registre Windows.

Procédure

- 1 Sur la machine qui héberge View Composer, ouvrez l'Éditeur du Registre Windows (regedit.exe).
- 2 Accédez à
HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS
1.0\Client

Si cette clé n'existe pas déjà, créez-la.

- 3 Supprimez la valeur **Activé** si elle existe.
- 4 Créez ou modifiez la valeur **DWORD DisabledByDefault** et définissez-la sur **0**.
- 5 Redémarrez le service VMware Horizon View Composer.
Les connexions TLSv1.0 entre View Composer et vCenter sont maintenant activées.
- 6 Dans le Registre Windows sur la machine View Composer, accédez à HKLM\SOFTWARE\VMware, Inc.\VMware View Composer.
- 7 Créez ou modifiez la valeur String **EnableTLS1.0** et définissez-la sur **1**.
- 8 Si l'hôte View Composer est une machine 64 bits, accédez à HKLM\SOFTWARE\WOW6432Node\VMware, Inc\VMware View Composer.
- 9 Créez ou modifiez la valeur String **EnableTLS1.0** et définissez-la sur **1**.
- 10 Redémarrez le service VMware Horizon View Composer.
Les connexions TLSv1.0 entre View Composer et les hôtes ESXi sont maintenant activées.

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 Horizon Administrator pour modifier les informations de dossier.

Si vous modifiez ces informations dans vCenter Server, Horizon 7 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.
- Utilisez vSphere DRS. DRS distribue efficacement des machines virtuelles de clone lié à vos hôtes.

Note 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 Horizon

7

Pour utiliser le Serveur de connexion, vous installez le logiciel sur des ordinateurs pris en charge, configurez les composants requis et, éventuellement, optimisez les composants.

Ce chapitre contient les rubriques suivantes :

- [Installation du logiciel Serveur de connexion Horizon](#)
- [Conditions préalables d'installation pour le Serveur de connexion Horizon](#)
- [Installer le Serveur de connexion Horizon avec une nouvelle configuration](#)
- [Installer une instance répliquée du Serveur de connexion Horizon](#)
- [Configurer un mot de passe de couplage de serveur de sécurité](#)
- [Installer un serveur de sécurité](#)
- [Avantages du dispositif Unified Access Gateway sur VPN](#)
- [Règles de pare-feu pour le Serveur de connexion Horizon](#)
- [Réinstaller le Serveur de connexion Horizon avec une configuration de sauvegarde](#)
- [Options de la ligne de commande Microsoft Windows Installer](#)
- [Désinstallation de composants d'Horizon 7 en silence à l'aide d'options de ligne de commande MSI](#)

Installation du logiciel Serveur de connexion Horizon

En fonction des besoins en termes de performances, de disponibilité et de sécurité de votre déploiement d'Horizon 7, vous pouvez installer une instance unique du Serveur de connexion, des instances répliquées du Serveur de connexion et des serveurs de sécurité. Vous devez installer au moins une instance du Serveur de connexion.

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

Installation standard

Génère une instance du Serveur de connexion avec une nouvelle configuration View LDAP.

Installation de réplica

Génère une instance du Serveur de connexion avec une configuration View LDAP copiée depuis une instance existante.

Installation de serveur de sécurité

Génère une instance du Serveur de connexion qui ajoute une couche supplémentaire de sécurité entre Internet et votre réseau interne.

Installation du serveur d'inscription

Installe un serveur d'inscription obligatoire pour la fonctionnalité d'authentification unique réelle afin de permettre aux utilisateurs connectés à VMware Identity Manager de se connecter à une application ou un poste de travail distant sans avoir à fournir leurs informations d'identification Active Directory. Le serveur d'inscription demande les certificats de courte durée qui sont utilisés pour l'authentification.

Note Comme cette fonctionnalité requiert qu'une autorité de certification soit également configurée, et qu'une configuration spécifique soit effectuée, la procédure d'installation du serveur d'inscription est fournie dans le document *Administration d'Horizon 7*, au chapitre « Authentification des utilisateurs sans demander les informations d'identification » plutôt que dans ce document d'installation.

Conditions préalables d'installation pour le Serveur de connexion Horizon

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

- Vous devez disposer d'une clé de licence valide pour Horizon 7.
- Vous devez associer l'hôte du Serveur de connexion à un domaine Active Directory. Le Serveur de connexion prend en charge les niveaux fonctionnels de domaine AD DS (Active Directory Domain Services) suivants :
 - Windows Server 2008
 - Windows Server 2008 R2
 - Windows Server 2012
 - Windows Server 2012 R2
 - Windows Server 2016

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

Note Le Serveur de connexion ne fait ni ne requiert de mises à jour de schéma ou de configuration pour Active Directory.

- N'installez pas le Serveur de connexion 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.
- N'installez pas le Serveur de connexion 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 doit disposer d'une adresse IP qui ne change pas. Dans un environnement IPv4, configurez une adresse IP statique. Dans un environnement IPv6, les machines obtiennent automatiquement des adresses IP qui ne changent pas.
- Pour exécuter le programme d'installation du Serveur de connexion Horizon, vous devez utiliser un compte d'utilisateur de domaine avec des privilèges d'administrateur sur le système.
- Lorsque vous installez le Serveur de connexion, vous autorisez un compte Administrateurs. Vous pouvez spécifier le groupe d'administrateurs local ou un compte d'utilisateur ou de groupe de domaine. Horizon 7 attribue des droits d'administration complets, y compris le droit d'installer des instances répliquées du Serveur de connexion, 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 Horizon avec une nouvelle configuration

Pour installer le Serveur de connexion en tant que serveur unique ou en tant que première instance d'un groupe d'instances de Serveur de connexion 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 d'Horizon Administrator. Le Serveur de connexion conserve automatiquement certaines entrées de View LDAP.

Le logiciel du Serveur de connexion ne peut pas coexister sur une machine virtuelle ou physique sur laquelle sont installés d'autres composants logiciels d'Horizon 7, notamment un serveur réplica, un serveur de sécurité, View Composer, Horizon Agent ou Horizon Client.

Lorsque vous installez le Serveur de connexion avec une nouvelle configuration, vous pouvez participer à un programme d'amélioration du produit. 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 Horizon Administrator. Pour consulter la liste des champs dont les données sont collectées, y compris les champs qui restent anonymes, reportez-vous à la section « Informations collectées par le programme d'amélioration du produit » dans le document *Administration d'Horizon 7*.

Par défaut, le composant HTML Access est installé sur l'hôte du Serveur de connexion lorsque vous installez le Serveur de connexion. Ce composant configure la page du portail utilisateur d'Horizon 7 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 voir un aperçu de la configuration du Serveur de connexion pour HTML Access, consultez le document *Guide d'installation et de configuration de VMware Horizon HTML Access* sur la page de Documentation d'Horizon Client.

Conditions préalables

- 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.
- Vérifiez que votre installation satisfait aux exigences décrites dans la section [Exigences du Serveur de connexion Horizon](#)
- Préparez votre environnement pour l'installation. Reportez-vous à la section [Conditions préalables d'installation pour le Serveur de connexion Horizon](#).
- Si vous prévoyez d'autoriser un utilisateur ou un groupe de domaine en tant que compte Administrateurs, vérifiez que vous avez créé le compte de domaine dans Active Directory.
- Préparez un mot de passe de récupération de données. Lorsque vous sauvegardez le Serveur de connexion, la configuration de View LDAP est exportée sous forme de données LDIF cryptées. Pour restaurer la configuration Horizon 7 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 Horizon 7 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 le Serveur de connexion.

- Familiarisez-vous avec les ports réseau qui doivent être ouverts sur le Pare-feu Windows pour les instances du Serveur de connexion. Reportez-vous à la section [Règles de pare-feu pour le Serveur de connexion Horizon](#).
- Si vous prévoyez de coupler un serveur de sécurité avec cette instance du serveur de connexion, 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 et requièrent que le Pare-feu Windows avec sécurité avancée soit activé.
- Si votre topologie réseau inclut un pare-feu principal entre un serveur de sécurité et l'instance du Serveur de connexion, 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](#).

Procédure

- 1 Téléchargez le fichier du programme d'installation du Serveur de connexion sur le site de téléchargement de VMware à l'adresse <https://my.vmware.com/web/vmware/downloads>.

Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut le Serveur de connexion.

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 du Serveur de connexion, 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 Sélectionnez la version du protocole Internet (**IPv4** ou **IPv6**).

Vous devez installer tous les composants Horizon 7 avec la même version IP.

- 7 Sélectionnez si le mode FIPS doit être activé ou désactivé.

Cette option n'est disponible que si le mode FIPS est activé dans Windows.

- 8 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'un navigateur Web.

Si **IPv4** est coché, ce paramètre est sélectionné par défaut. Si **IPv6** est coché, ce paramètre ne s'affiche pas, car HTML Access n'est pas pris en charge dans un environnement IPv6.

- 9 Tapez un mot de passe de récupération de données et éventuellement un rappel de mot de passe.
- 10 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.

11 Autorisez un compte Administrateurs d'Horizon.

Seuls les membres de ce compte peuvent ouvrir une session sur Horizon Administrator, disposer de droits d'administration complets et installer des instances répliquées du Serveur de connexion et d'autres serveurs Horizon 7.

Option	Description
Authorize the local Administrators group (Autoriser le groupe d'administrateurs local)	Permet aux utilisateurs du groupe d'administrateurs local d'administrer Horizon 7.
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 Horizon 7

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

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

- 13 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.

- 14 Effectuez l'assistant d'installation pour terminer l'installation du Serveur de connexion.

- 15 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 du Serveur de connexion, l'installation peut avoir activé des fonctionnalités du système d'exploitation pour la première fois. Dans ce cas, des correctifs supplémentaires peuvent être nécessaires.

Les services Horizon 7 sont installés sur l'ordinateur Windows Server :

- Serveur de connexion VMware Horizon
- 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 d'Horizon 7*.

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 Horizon 7 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 clients de se connecter au Serveur de connexion sur le port TCP 8443.

Étape suivante

Configurez des certificats de serveur SSL pour le Serveur de connexion. Reportez-vous à la section [Chapitre 8 Configuration de certificats TLS pour des serveurs Horizon 7](#).

Si vous disposez d'une version antérieure de vCenter Server, reportez-vous à la section [Activer TLSv1.0 sur des connexions vCenter depuis un Serveur de connexion](#).

Effectuez la configuration initiale sur le Serveur de connexion. Reportez-vous à la section [Chapitre 10 Configuration d'Horizon 7 pour la première fois](#).

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

Si vous réinstallez le Serveur de connexion 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 Horizon en silence

Vous pouvez utiliser la fonctionnalité d'installation silencieuse de MSI (Microsoft Windows Installer) pour effectuer une installation standard du Serveur de connexion 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 Horizon 7 dans une entreprise de grande taille.

Conditions préalables

- 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.
- Vérifiez que votre installation satisfait aux exigences décrites dans la section [Exigences du Serveur de connexion Horizon](#)
- Préparez votre environnement pour l'installation. Reportez-vous à la section [Conditions préalables d'installation pour le Serveur de connexion Horizon](#).
- Si vous prévoyez d'autoriser un utilisateur ou un groupe de domaine en tant que compte Administrateurs d'Horizon, 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, 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 du Serveur de connexion. Reportez-vous à la section [Règles de pare-feu pour le Serveur de connexion Horizon](#).
- Si vous prévoyez de coupler un serveur de sécurité avec cette instance du serveur de connexion, 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 et requièrent que le Pare-feu Windows avec sécurité avancée soit activé.
- Si votre topologie réseau inclut un pare-feu principal entre un serveur de sécurité et l'instance du Serveur de connexion, 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](#).
- Vérifiez que l'ordinateur Windows sur lequel vous installez le Serveur de connexion dispose de la version 2.0 ou ultérieure 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](#).
- Familiarisez-vous avec les propriétés d'installation silencieuse disponibles avec une installation standard du Serveur de connexion. Reportez-vous à la section [Propriétés de l'installation silencieuse pour une installation standard du Serveur de connexion Horizon](#).

Procédure

- 1 Téléchargez le fichier du programme d'installation du Serveur de connexion sur le site de téléchargement de VMware à l'adresse <https://my.vmware.com/web/vmware/downloads>.

Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut le Serveur de connexion.

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 Horizon 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 du Serveur de connexion, l'installation peut avoir activé des fonctionnalités du système d'exploitation pour la première fois. Dans ce cas, des correctifs supplémentaires peuvent être nécessaires.

Les services Horizon 7 sont installés sur l'ordinateur Windows Server :

- Serveur de connexion VMware Horizon
- 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 Horizon 7 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 clients de se connecter au Serveur de connexion sur le port TCP 8443.

Pour plus d'informations sur ces services, consultez le document *Administration d'Horizon 7*.

Étape suivante

Configurez des certificats de serveur SSL pour le Serveur de connexion. Reportez-vous à la section [Chapitre 8 Configuration de certificats TLS pour des serveurs Horizon 7](#).

Si vous disposez d'une version antérieure de vCenter Server, reportez-vous à la section [Activer TLSv1.0 sur des connexions vCenter depuis un Serveur de connexion](#).

Si vous configurez Horizon 7 pour la première fois, effectuez la configuration initiale sur le Serveur de connexion. Reportez-vous à la section [Chapitre 10 Configuration d'Horizon 7 pour la première fois](#).

Propriétés de l'installation silencieuse pour une installation standard du Serveur de connexion Horizon

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

Tableau 7-1. Propriétés MSI pour l'installation silencieuse du Serveur de connexion dans une installation standard

Propriété MSI	Description	Valeur par défaut
INSTALLDIR	Chemin d'accès et dossier dans lequel le logiciel Serveur de connexion est installé. Par exemple : <code>INSTALLDIR=""D:\abc\my folder""</code> 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 d'Horizon Server : <ul style="list-style-type: none"> 1. Installation standard 2. Installation de réplica 3. Installation de serveur de sécurité 5. Installation du serveur d'inscription Par exemple, pour effectuer une installation standard, définissez <code>VDM_SERVER_INSTANCE_TYPE=1</code>	1
FWCHOICE	Propriété MSI qui détermine s'il faut configurer un pare-feu pour l'instance du Serveur de connexion. Une valeur de 1 configure un pare-feu. Une valeur de 2 ne configure pas un pare-feu. Par exemple : <code>FWCHOICE=1</code>	1
VDM_INITIAL_ADMIN_SID	SID de l'utilisateur ou du groupe d'administrateurs Horizon initial qui est autorisé avec des droits d'administration complets dans Horizon. La valeur par défaut est le SID du groupe d'administrateurs local sur l'ordinateur du Serveur de connexion. 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 Horizon 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.	Aucun
VDM_SERVER_RECOVERY_PWD_REMINDER	Rappel du mot de passe de récupération de données. Cette propriété est facultative.	aucune
VDM_IP_PROTOCOL_UTILISATION	Spécifie la version IP que les composants Horizon utilisent pour la communication. Les valeurs possibles sont IPv4 et IPv6 .	IPv4

Tableau 7-1. Propriétés MSI pour l'installation silencieuse du Serveur de connexion dans une installation standard (Suite)

Propriété MSI	Description	Valeur par défaut
VDM_FIPS_ENABLED	Indiquez si le mode FIPS doit être activé ou désactivé. Une valeur de 1 active le mode FIPS. Une valeur de 0 désactive le mode FIPS. Si cette propriété est définie sur 1 et que Windows n'est pas en mode FIPS, le programme d'installation échouera.	0
HTMLACCESS	Contrôle l'installation du composant additionnel HTML Access. Définissez cette propriété sur 1 pour configurer HTML Access ou omettez la propriété si HTML Access n'est pas nécessaire.	1

Activer TLSv1.0 sur des connexions vCenter depuis un Serveur de connexion

Le protocole de sécurité TLSv1.0 est désactivé par défaut sur les composants d'Horizon 7 et versions ultérieures. Si votre déploiement inclut une version antérieure de vCenter Server qui prend en charge uniquement TLSv1.0, vous devrez peut-être activer TLSv1.0 pour les connexions du Serveur de connexion après avoir installé ou effectué une mise à niveau vers le Serveur de connexion 7.0 ou une version ultérieure.

Certaines versions de maintenance antérieures de vCenter Server 5.1 et 5.5 ne prennent en charge que TLSv1.0, qui n'est plus activé par défaut dans Horizon 7 et versions ultérieures. S'il n'est pas possible de mettre à niveau vCenter Server vers une version prenant en charge TLSv1.1 ou TLSv1.2, vous pouvez activer TLSv1.0 pour les connexions du Serveur de connexion.

Conditions préalables

- Si vous effectuez une mise à niveau vers Horizon 7, exécutez cette procédure avant afin de réduire le nombre de redémarrages nécessaires du service. Au cours d'une mise à niveau, le service Serveur de connexion est redémarré, et un redémarrage est obligatoire pour appliquer les modifications de configuration décrites dans cette procédure. Si vous effectuez une mise à niveau avant de réaliser cette procédure, vous devrez redémarrer le service une seconde fois.
- Pour plus d'informations sur l'utilisation de l'utilitaire ADSI Edit sur votre version du système d'exploitation Windows, consultez le site Web Microsoft TechNet.

Procédure

- 1 Démarrez l'utilitaire ADSI Edit sur votre hôte du Serveur de connexion.
- 2 Dans l'arborescence de la console, sélectionnez **Se connecter à**.
- 3 Dans la zone de texte **Sélectionnez ou entrez un nom unique ou un contexte d'attribution de noms**, tapez le nom unique **DC=vmware**, **DC=vmware**, **DC=int**.
- 4 Dans le volet Ordinateur, sélectionnez ou tapez **localhost:389** ou le nom de domaine complet du Serveur de connexion, suivi du port 389.

Par exemple : **localhost:389** ou **mycomputer.example.com:389**

- 5 Développez l'arborescence de l'Éditeur ADSI, développez **OU=Properties**, sélectionnez **OU=Global** et double-cliquez sur **CN=Common** dans le volet de droite.
- 6 Dans la boîte de dialogue Propriétés, modifiez l'attribut **pae-ClientSSLSecureProtocols** pour ajouter la valeur suivante

`\LIST:TLSv1.2,TLSv1.1,TLSv1`

Veillez à inclure la barre oblique inversée au début de la ligne.
- 7 Cliquez sur **OK**.
- 8 S'il s'agit d'une nouvelle installation, redémarrez le service Serveur de connexion sur chaque instance du Serveur de connexion afin d'appliquer la modification de configuration.

Si vous prévoyez de réaliser une mise à niveau, vous n'avez pas à redémarrer le service, car le processus de mise à niveau le redémarre automatiquement.

Installer une instance répliquée du Serveur de connexion Horizon

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

Lorsque vous installez une instance répliquée, Horizon 7 copie les données de configuration de View LDAP depuis l'instance du Serveur de connexion existante.

Après l'installation, les données de configuration de View LDAP identiques sont conservées sur toutes les instances du Serveur de connexion 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.

Note 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'Horizon 7, notamment un serveur de sécurité, un Serveur de connexion, View Composer, Horizon Agent ou Horizon Client.

Par défaut, le composant HTML Access est installé sur l'hôte du Serveur de connexion lorsque vous installez le Serveur de connexion. Ce composant configure la page du portail utilisateur d'Horizon 7 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 voir un aperçu de la configuration du Serveur de connexion pour HTML Access, consultez le document *Guide d'installation et de configuration de VMware Horizon HTML Access* sur la page de Documentation d'Horizon Client.

Conditions préalables

- Vérifiez qu'au moins une instance du Serveur de connexion est installée et configurée sur le réseau.
- Pour installer l'instance répliquée, vous devez ouvrir une session en tant qu'utilisateur avec le rôle Administrateurs. Vous spécifiez le compte ou le groupe avec le rôle Administrateurs lorsque vous installez la première instance du Serveur de connexion. 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 Horizon avec une nouvelle configuration](#).
- Si l'instance du Serveur de connexion existante se trouve dans un domaine différent de celui de l'instance répliquée, l'utilisateur de domaine doit également disposer de privilèges d'administrateur 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, 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 du Serveur de connexion Horizon](#)
- Vérifiez que les ordinateurs sur lesquels vous installez des instances répliquées du Serveur de connexion sont connectés sur un réseau LAN haute performance. Reportez-vous à la section [Exigences de réseau pour des instances répliquées du Serveur de connexion Horizon](#).
- Préparez votre environnement pour l'installation. Reportez-vous à la section [Conditions préalables d'installation pour le Serveur de connexion Horizon](#).
- Si vous installez une instance du Serveur de connexion répliquée correspondant à Horizon 7 5.1 ou version ultérieure et que l'instance du Serveur de connexion existante que vous répliquez correspond à Horizon 7 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 Horizon avec une nouvelle configuration](#).
- Familiarisez-vous avec les ports réseau qui doivent être ouverts sur le Pare-feu Windows pour les instances du Serveur de connexion. Reportez-vous à la section [Règles de pare-feu pour le Serveur de connexion Horizon](#).
- Si vous prévoyez de coupler un serveur de sécurité avec cette instance du serveur de connexion, 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 et requièrent que le Pare-feu Windows avec sécurité avancée soit activé.

- Si votre topologie réseau inclut un pare-feu principal entre un serveur de sécurité et l'instance du Serveur de connexion, 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](#).

Procédure

- 1 Téléchargez le fichier du programme d'installation du Serveur de connexion sur le site de téléchargement de VMware à l'adresse <https://my.vmware.com/web/vmware/downloads>.

Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut le Serveur de connexion.

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 du Serveur de connexion, 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 Sélectionnez la version du protocole Internet (**IPv4** ou **IPv6**).

Vous devez installer tous les composants Horizon 7 avec la même version IP.

- 7 Sélectionnez si le mode FIPS doit être activé ou désactivé.

Cette option n'est disponible que si le mode FIPS est activé dans Windows.

- 8 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.

Si **IPv4** est coché, ce paramètre est sélectionné par défaut. Si **IPv6** est coché, ce paramètre ne s'affiche pas, car HTML Access n'est pas pris en charge dans un environnement IPv6.

- 9 Saisissez le nom d'hôte ou l'adresse IP de l'instance du Serveur de connexion existante que vous répliquez.

- 10 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 existante que vous répliquez correspond à Horizon 7 5.0.x ou version antérieure.

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 de l'instance répliquée.

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 du Serveur de connexion, l'installation peut avoir activé des fonctionnalités du système d'exploitation pour la première fois. Dans ce cas, des correctifs supplémentaires peuvent être nécessaires.

Les services Horizon 7 sont installés sur l'ordinateur Windows Server :

- Serveur de connexion VMware Horizon
- 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 d'Horizon 7*.

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 Horizon 7 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 clients de se connecter au Serveur de connexion sur le port TCP 8443.

Étape suivante

Configurez un certificat de serveur SSL pour l'instance du Serveur de connexion. Reportez-vous à la section [Chapitre 8 Configuration de certificats TLS pour des serveurs Horizon 7](#).

Il n'est pas nécessaire d'effectuer de configuration initiale d'Horizon 7 sur une instance répliquée du Serveur de connexion. L'instance répliquée hérite de sa configuration depuis l'instance du Serveur de connexion existante.

Toutefois, il peut être nécessaire de configurer des paramètres de connexion client pour cette instance du Serveur de connexion, 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](#) et [Dimensionnement de paramètres de Windows Server pour prendre en charge votre déploiement](#).

Si vous réinstallez le Serveur de connexion 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 du Serveur de connexion Horizon en silence

Vous pouvez utiliser la fonction d'installation silencieuse de MSI (Microsoft Windows Installer) pour installer une instance répliquée du Serveur de connexion 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 Horizon 7 dans une entreprise de grande taille.

Conditions préalables

- Vérifiez qu'au moins une instance du Serveur de connexion 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 Administrateurs. Vous spécifiez le compte Administrateurs lorsque vous installez la première instance du Serveur de connexion. 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 Horizon avec une nouvelle configuration](#).
- Si l'instance du Serveur de connexion existante se trouve dans un domaine différent de celui de l'instance répliquée, l'utilisateur de domaine doit également disposer de privilèges d'administrateur 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, 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 du Serveur de connexion Horizon](#)
- Vérifiez que les ordinateurs sur lesquels vous installez des instances répliquées du Serveur de connexion sont connectés sur un réseau LAN haute performance. Reportez-vous à la section [Exigences de réseau pour des instances répliquées du Serveur de connexion Horizon](#).

- Préparez votre environnement pour l'installation. Reportez-vous à la section [Conditions préalables d'installation pour le Serveur de connexion Horizon](#).
- Familiarisez-vous avec les ports réseau qui doivent être ouverts sur le Pare-feu Windows pour les instances du Serveur de connexion. Reportez-vous à la section [Règles de pare-feu pour le Serveur de connexion Horizon](#).
- Si vous prévoyez de coupler un serveur de sécurité avec cette instance du serveur de connexion, 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 et requièrent que le Pare-feu Windows avec sécurité avancée soit activé.
- Si votre topologie réseau inclut un pare-feu principal entre un serveur de sécurité et l'instance du Serveur de connexion, 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](#).
- 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](#).
- Familiarisez-vous avec les propriétés d'installation silencieuse disponibles avec une installation de réplica du Serveur de connexion. Reportez-vous à la section [Propriétés de l'installation silencieuse pour une instance répliquée du Serveur de connexion Horizon](#).

Procédure

- 1 Téléchargez le fichier du programme d'installation du Serveur de connexion sur le site de téléchargement de VMware à l'adresse <https://my.vmware.com/web/vmware/downloads>.

Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut le Serveur de connexion.

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 du Serveur de connexion répliquée correspondant à la version View 5.1 ou ultérieure et que l'instance du Serveur de connexion 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 Horizon 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 du Serveur de connexion, l'installation peut avoir activé des fonctionnalités du système d'exploitation pour la première fois. Dans ce cas, des correctifs supplémentaires peuvent être nécessaires.

Les services Horizon 7 sont installés sur l'ordinateur Windows Server :

- Serveur de connexion VMware Horizon
- 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 d'Horizon 7*.

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 Horizon 7 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 clients de se connecter au Serveur de connexion sur le port TCP 8443.

Étape suivante

Configurez un certificat de serveur SSL pour l'instance du Serveur de connexion. Reportez-vous à la section [Chapitre 8 Configuration de certificats TLS pour des serveurs Horizon 7](#).

Il n'est pas nécessaire d'effectuer de configuration initiale d'Horizon 7 sur une instance répliquée du Serveur de connexion. L'instance répliquée hérite de sa configuration depuis l'instance du Serveur de connexion existante.

Toutefois, il peut être nécessaire de configurer des paramètres de connexion client pour cette instance du Serveur de connexion, 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](#) et [Dimensionnement de paramètres de Windows Server pour prendre en charge votre déploiement](#).

Propriétés de l'installation silencieuse pour une instance répliquée du Serveur de connexion Horizon

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

Tableau 7-2. Propriétés MSI pour l'installation silencieuse d'une instance répliquée du Serveur de connexion Horizon

Propriété MSI	Description	Valeur par défaut
INSTALLDIR	<p>Chemin d'accès et dossier dans lequel le logiciel Serveur de connexion est installé.</p> <p>Par exemple : <code>INSTALLDIR=""D:\abc\my folder""</code></p> <p>Les guillemets délimitant le chemin permettent au programme d'installation MSI d'interpréter l'espace comme étant une partie valide du chemin.</p> <p>Cette propriété MSI est facultative.</p>	<p>%ProgramFiles</p> <p>%\VMware\VMware</p> <p>View\Server</p>
VDM_SERVER_INSTANCE_TYPE	<p>Type d'installation du Serveur de connexion :</p> <ul style="list-style-type: none"> ■ 1. Installation standard ■ 2. Installation de réplica ■ 3. Installation de serveur de sécurité <p>Pour installer une instance répliquée, définissez <code>VDM_SERVER_INSTANCE_TYPE=2</code></p> <p>Cette propriété MSI est requise lors de l'installation d'un réplica.</p>	1

Tableau 7-2. Propriétés MSI pour l'installation silencieuse d'une instance répliquée du Serveur de connexion Horizon (Suite)

Propriété MSI	Description	Valeur par défaut
ADAM_PRIMARY_NAME	Nom d'hôte ou adresse IP de l'instance du Serveur de connexion existante que vous répliquez. Par exemple : ADAM_PRIMARY_NAME=cs1.companydomain.com Cette propriété MSI est requise.	aucune
FWCHOICE	Propriété MSI qui détermine s'il faut configurer un pare-feu pour l'instance du Serveur de connexion. 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_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. Note Le mot de passe de récupération de données n'est pas défini dans View LDAP si l'instance du Serveur de connexion standard que vous répliquez est View 5.0 ou version antérieure. Si l'instance du Serveur de connexion que vous répliquez est View 5.1 ou version ultérieure, 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
VDM_IP_PROTOCOL_UTILISATION	Spécifie la version IP que les composants d'Horizon 7 utilisent pour la communication. Les valeurs possibles sont IPv4 et IPv6 .	IPv4
VDM_FIPS_ENABLED	Indiquez si le mode FIPS doit être activé ou désactivé. Une valeur de 1 active le mode FIPS. Une valeur de 0 désactive le mode FIPS. Si cette propriété est définie sur 1 et que Windows n'est pas en mode FIPS, le programme d'installation échouera.	0

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 du Serveur de connexion, 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 du Serveur de connexion. Le mot de passe devient non valide une fois que vous l'avez fourni au programme d'installation du Serveur de connexion.

Note Vous ne pouvez pas coupler une version antérieure d'un serveur de sécurité avec la version actuelle du Serveur de connexion. Si vous configurez un mot de passe de couplage sur la version actuelle du Serveur de connexion 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 Horizon Administrator, sélectionnez **Configuration de View > Serveurs**.
- 2 Sous l'onglet Serveurs de connexion, sélectionnez l'instance du Serveur de connexion 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.

Étape suivante

Installez un serveur de sécurité. Reportez-vous à la section [Installer un serveur de sécurité](#).

Important Si vous ne fournissez pas le mot de passe de couplage de serveur de sécurité au programme d'installation du Serveur de connexion 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 du Serveur de connexion 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 du Serveur de connexion.

Le logiciel du serveur de sécurité ne peut pas coexister sur une machine virtuelle ou physique sur laquelle sont installés d'autres composants logiciels d'Horizon 7, notamment un serveur réplica, un Serveur de connexion, View Composer, Horizon Agent ou Horizon Client.

Conditions préalables

- 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 couplées avec des serveurs de sécurité seront dédiées aux utilisateurs du réseau externe. Pour plus d'informations, consultez le document *Planification de l'architecture Horizon 7*.

Important Si vous utilisez un équilibrage de charge, il doit avoir une adresse IP qui ne change pas. Dans un environnement IPv4, configurez une adresse IP statique. Dans un environnement IPv6, les machines obtiennent automatiquement des adresses IP qui ne changent pas.

- Vérifiez que votre installation satisfait aux exigences décrites dans la section [Exigences du Serveur de connexion Horizon](#)
- Préparez votre environnement pour l'installation. Reportez-vous à la section [Conditions préalables d'installation pour le Serveur de connexion Horizon](#).
- Vérifiez que l'instance du Serveur de connexion à coupler avec le serveur de sécurité est installée et configurée et exécute une version du Serveur de connexion qui est compatible avec la version du serveur de sécurité. Reportez-vous à la section « Matrice de compatibilité des composants Horizon 7 » dans le document *Mises à niveau d'Horizon 7*.
- Vérifiez que l'instance du Serveur de connexion à coupler avec le serveur de sécurité est accessible à l'ordinateur sur lequel vous prévoyez d'installer le serveur de sécurité.

Note Après une mise à niveau du Serveur de connexion vers Horizon 7 version 7.5, les serveurs de sécurité sur lesquels le protocole IPsec est désactivé doivent être réinstallés. Si l'adresse IP d'un serveur de sécurité change, il doit être réinstallé. Le couplage de serveur de sécurité ne fonctionne pas correctement si le serveur de sécurité se trouve derrière le composant NAT dynamique.

- 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](#).
- Familiarisez-vous avec le format des URL externes. Reportez-vous à la section [Configuration d'URL externes pour Secure Gateway et les connexions par tunnel](#).
- 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 Horizon](#).
- Si votre topologie réseau inclut un pare-feu principal entre le serveur de sécurité et le Serveur de connexion, 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](#).

- 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 [Supprimer des règles IPsec pour le serveur de sécurité](#).
- Si vous installez Horizon 7 en mode FIPS, vous devez désélectionner le paramètre global **Utiliser IPsec pour les connexions du serveur de sécurité** dans Horizon Administrator, car il est nécessaire de configurer IPsec manuellement en mode FIPS après avoir installé un serveur de sécurité.

Procédure

- 1 Téléchargez le fichier du programme d'installation du Serveur de connexion sur le site de téléchargement de VMware à l'adresse <https://my.vmware.com/web/vmware/downloads>.

Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut le Serveur de connexion.

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 du Serveur de connexion, 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 Sélectionnez la version du protocole Internet (**IPv4** ou **IPv6**).

Vous devez installer tous les composants Horizon 7 avec la même version IP.

- 7 Sélectionnez si le mode FIPS doit être activé ou désactivé.

Cette option n'est disponible que si le mode FIPS est activé dans Windows.

- 8 Saisissez le nom de domaine complet ou l'adresse IP de l'instance du Serveur de connexion à coupler avec le serveur de sécurité dans la zone de texte **Serveur**.

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

- 9 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 Horizon Administrator pour configurer un nouveau mot de passe et le saisir dans le programme d'installation.

- 10 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`

- 11** 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.

Dans un environnement IPv4, spécifiez l'URL externe PCoIP sous la forme d'une adresse IP avec le numéro de port 4172. Dans un environnement IPv6, vous pouvez spécifier une adresse IP ou un nom de domaine complet, et le numéro de port 4172. Dans les deux cas, n'incluez pas de nom de protocole.

Par exemple, dans un environnement IPv4 : 10.20.30.40:4172

Les clients doivent pouvoir utiliser l'URL pour accéder au serveur de sécurité.

- 12** 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.

- 13** 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.

- 14** 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 d'Horizon 7*.

Le serveur de sécurité s'affiche dans le volet Serveurs de sécurité dans Horizon 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.

Note 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 [Supprimer des règles IPsec pour le serveur de sécurité](#).

Étape suivante

Configurez un certificat de serveur SSL pour le serveur de sécurité. Reportez-vous à la section [Chapitre 8 Configuration de certificats TLS pour des serveurs Horizon 7](#).

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](#) et [Dimensionnement de paramètres de Windows Server pour prendre en charge votre déploiement](#).

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 Horizon 7 dans une entreprise de grande taille.

Conditions préalables

- 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 couplées avec des serveurs de sécurité seront dédiées aux utilisateurs du réseau externe. Pour plus d'informations, consultez le document *Planification de l'architecture Horizon 7*.

Important Si vous utilisez un équilibrage de charge, il doit avoir une adresse IP qui ne change pas. Dans un environnement IPv4, configurez une adresse IP statique. Dans un environnement IPv6, les machines obtiennent automatiquement des adresses IP qui ne changent pas.

- Vérifiez que votre installation satisfait aux exigences décrites dans la section [Exigences du Serveur de connexion Horizon](#)
- Préparez votre environnement pour l'installation. Reportez-vous à la section [Conditions préalables d'installation pour le Serveur de connexion Horizon](#).

- Vérifiez que l'instance du Serveur de connexion à coupler avec le serveur de sécurité est installée et configurée et exécute une version du Serveur de connexion qui est compatible avec la version du serveur de sécurité. Reportez-vous à la section « Matrice de compatibilité des composants Horizon 7 » dans le document *Mises à niveau d'Horizon 7*.
- Vérifiez que l'instance du Serveur de connexion à coupler avec le serveur de sécurité est accessible à l'ordinateur sur lequel vous prévoyez d'installer le serveur de sécurité.

Note Après une mise à niveau du Serveur de connexion vers Horizon 7 version 7.5, les serveurs de sécurité sur lesquels le protocole IPsec est désactivé doivent être réinstallés. Si l'adresse IP d'un serveur de sécurité change, il doit être réinstallé. Le couplage de serveur de sécurité ne fonctionne pas correctement si le serveur de sécurité se trouve derrière le composant NAT dynamique.

- 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](#).
- Familiarisez-vous avec le format des URL externes. Reportez-vous à la section [Configuration d'URL externes pour Secure Gateway et les connexions par tunnel](#).
- 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 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 Horizon](#).
- Si votre topologie réseau inclut un pare-feu principal entre le serveur de sécurité et le Serveur de connexion, 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](#).
- 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 [Supprimer des règles IPsec pour le serveur de sécurité](#).
- 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](#).
- 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](#).
- Si vous installez Horizon 7 en mode FIPS, vous devez désélectionner le paramètre global **Utiliser IPSec pour les connexions du serveur de sécurité** dans Horizon Administrator, car il est nécessaire de configurer IPsec manuellement en mode FIPS après avoir installé un serveur de sécurité.

Procédure

- 1 Téléchargez le fichier du programme d'installation du Serveur de connexion sur le site de téléchargement de VMware à l'adresse <https://my.vmware.com/web/vmware/downloads>.

Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut le Serveur de connexion.

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_TCP_PORT=4172
VDM_SERVER_SS_PCOIP_UDP_PORT=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 d'Horizon 7*.

Le serveur de sécurité s'affiche dans le volet Serveurs de sécurité dans Horizon 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.

Note 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 [Supprimer des règles IPsec pour le serveur de sécurité](#).

Étape suivante

Configurez un certificat de serveur SSL pour le serveur de sécurité. Reportez-vous à la section [Chapitre 8 Configuration de certificats TLS pour des serveurs Horizon 7](#).

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](#) et [Dimensionnement de paramètres de Windows Server pour prendre en charge votre déploiement](#).

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 le format *PROPERTY=value* de manière que Microsoft Windows Installer (MSI) puisse interpréter les propriétés et les valeurs.

Tableau 7-3. Propriétés MSI pour installer un serveur de sécurité en silence

Propriété MSI	Description	Valeur par défaut
INSTALLDIR	<p>Chemin d'accès et dossier dans lequel le logiciel Serveur de connexion est installé.</p> <p>Par exemple : <code>INSTALLDIR=""D:\abc\my folder""</code></p> <p>Les guillemets délimitant le chemin permettent au programme d'installation MSI d'interpréter l'espace comme étant une partie valide du chemin.</p> <p>Cette propriété MSI est facultative.</p>	<p>%ProgramFiles</p> <p>%\VMware\VMware View\Server</p>
VDM_SERVER_INSTANCE_TYPE	<p>Type d'installation du Serveur de connexion :</p> <ul style="list-style-type: none"> ■ 1. Installation standard ■ 2. Installation de réplica ■ 3. Installation de serveur de sécurité <p>Pour installer un serveur de sécurité, définissez <code>VDM_SERVER_INSTANCE_TYPE=3</code></p> <p>Cette propriété MSI est requise lors de l'installation d'un serveur de sécurité.</p>	1
VDM_SERVER_NAME	<p>Nom d'hôte ou adresse IP de l'instance du Serveur de connexion existante à coupler avec le serveur de sécurité.</p> <p>Par exemple : <code>VDM_SERVER_NAME=cs1.internaldomain.com</code></p> <p>Cette propriété MSI est requise.</p>	aucune
VDM_SERVER_SS_EXTURL	<p>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.</p> <p>Par exemple : <code>VDM_SERVER_SS_EXTURL=https://view.companydomain.com:443</code></p> <p>Cette propriété MSI est requise.</p>	aucune
VDM_SERVER_SS_PWD	<p>Mot de passe de couplage de serveur de sécurité.</p> <p>Par exemple : <code>VDM_SERVER_SS_PWD=secret</code></p> <p>Cette propriété MSI est requise.</p>	aucune
FWCHOICE	<p>Propriété MSI qui détermine s'il faut configurer un pare-feu pour l'instance du Serveur de connexion.</p> <p>Une valeur de 1 configure un pare-feu. Une valeur de 2 ne configure pas un pare-feu.</p> <p>Par exemple : <code>FWCHOICE=1</code></p> <p>Cette propriété MSI est facultative.</p>	1

Tableau 7-3. Propriétés MSI pour installer un serveur de sécurité en silence (Suite)

Propriété MSI	Description	Valeur par défaut
VDM_SERVER_SS_PCOIP_IPADDR	Adresse IP externe de PCoIP Secure Gateway. Dans un environnement IPv6, cette propriété peut également être définie sur le nom de domaine complet 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
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 aux postes de travail Horizon 7.	aucune
VDM_SERVER_SS_FORCE_IPSEC	Force l'utilisation d'IPsec entre le serveur de sécurité et son instance du Serveur de connexion couplée. Par défaut, l'installation et le couplage sans assistance du serveur de sécurité sur une instance du Serveur de connexion 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
VDM_IP_PROTOCOL_USAGE	Spécifie la version IP que les composants d'Horizon 7 utilisent pour la communication. Les valeurs possibles sont IPv4 et IPv6 .	IPv4
VDM_FIPS_ENABLED	Indiquez si le mode FIPS doit être activé ou désactivé. Une valeur de 1 active le mode FIPS. Une valeur de 0 désactive le mode FIPS. Si cette propriété est définie sur 1 et que Windows n'est pas en mode FIPS, le programme d'installation échouera.	0

Supprimer des règles IPsec pour le 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 du Serveur de connexion couplée. Si vous n'effectuez pas cette étape, la mise à niveau ou la réinstallation échoue.

Par défaut, la communication entre un serveur de sécurité et son instance du Serveur de connexion couplée est régie par des règles IPsec. Lorsque vous mettez à niveau ou réinstallez le serveur de sécurité et le coupez de nouveau avec l'instance du Serveur de connexion, 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 le Serveur de connexion.

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 Horizon 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.

Note Vous n'avez pas à supprimer un serveur de sécurité d'Horizon Administrator avant de mettre à niveau ou de réinstaller le serveur de sécurité. Supprimez un serveur de sécurité d'Horizon Administrator uniquement si vous prévoyez de le supprimer définitivement de l'environnement Horizon 7.

Avec View 5.0.x et versions antérieures, vous pouviez supprimer un serveur de sécurité depuis l'interface utilisateur d'Horizon Administrator ou à l'aide de la commande `vdmaadmin -S`. Dans View 5.1 et versions supérieures, vous devez utiliser `vdmaadmin -S`. Consultez la section « Suppression de l'entrée pour une instance du Serveur de connexion Horizon ou un serveur de sécurité à l'aide de l'option -S » dans le document *Administration d'Horizon 7*.



Attention 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. Par conséquent, si vous utilisez un équilibrage de charge pour gérer un groupe de serveurs de sécurité, exécutez cette procédure sur un serveur, puis mettez ce serveur à niveau avant de supprimer des règles IPsec pour le serveur suivant. Vous pouvez supprimer des serveurs de la production et les ajouter de nouveau un par un de cette manière afin d'éviter toute interruption de service pour vos utilisateurs finaux.

Procédure

- 1 Dans Horizon Administrator, cliquez sur **Configuration de View > Serveurs**.

- 2 Dans 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.

Étape suivante

Mettez à niveau ou réinstallez le serveur de sécurité.

Avantages du dispositif Unified Access Gateway sur VPN

Un dispositif Unified Access Gateway est une passerelle par défaut qui permet d'accéder en toute sécurité à des applications et des postes de travail distants depuis l'extérieur du pare-feu d'entreprise.

Pour obtenir la dernière version de la documentation d'Unified Access Gateway, reportez-vous au document *Déploiement et configuration de VMware Unified Access Gateway* dans <https://docs.vmware.com/fr/Unified-Access-Gateway/index.html>.

Un dispositif Unified Access Gateway réside dans une zone démilitarisée (DMZ) et agit comme un hôte proxy pour les connexions à l'intérieur d'un réseau approuvé, ce qui offre une couche supplémentaire de sécurité en protégeant les postes de travail virtuels, les hôtes d'application et les serveurs contre l'Internet public.

Configurer un dispositif Unified Access Gateway

Unified Access Gateway et les solutions VPN génériques sont similaires, car ils s'assurent que le trafic est transmis à un réseau interne uniquement pour le compte d'utilisateurs à authentification élevée.

Avantages d'Unified Access Gateway par rapport aux solutions VPN génériques :

- **Access Control Manager.** Unified Access Gateway applique automatiquement des règles d'accès. Unified Access Gateway reconnaît les droits des utilisateurs et l'adressage requis pour se connecter en interne. Un VPN fait la même chose, car la plupart des VPN autorisent un administrateur à configurer des règles de connexion réseau pour chaque utilisateur ou groupe d'utilisateurs individuellement. Au début, cela fonctionne bien avec un VPN, mais exige un travail administratif important pour appliquer les règles requises.
- **Interface utilisateur.** Unified Access Gateway ne modifie pas l'interface utilisateur simple d'Horizon Client. Avec Unified Access Gateway, lorsqu'Horizon Client est lancé, les utilisateurs authentifiés sont dans leur environnement View et disposent d'un accès contrôlé à leurs postes de travail et applications. Un VPN exige que vous configuriez le logiciel VPN, puis que vous vous authentifiiez séparément avant de lancer Horizon Client.

- Performances. Unified Access Gateway est conçu pour maximiser la sécurité et les performances. Avec Unified Access Gateway, les protocoles PCoIP, HTML Access et WebSocket sont sécurisés sans qu'une encapsulation supplémentaire soit nécessaire. Des VPN sont implémentés en tant que VPN SSL. Cette implémentation répond aux exigences de sécurité et, avec TLS (Transport Layer Security) activé, elle est considérée comme sûre, mais le protocole sous-jacent avec SSL/TLS est simplement basé sur TCP. Avec des protocoles modernes de vidéo à distance exploitant des transports UDP sans connexion, les avantages de performance peuvent être considérablement réduits lorsque l'on force le transport TCP. Cela ne s'applique pas à toutes les technologies de VPN, car celles qui peuvent également fonctionner avec DTLS ou IPsec au lieu de SSL/TLS peuvent fonctionner correctement avec View, un composant des protocoles de poste de travail Horizon 7.

Améliorer la sécurité d'Horizon avec Unified Access Gateway

Un dispositif Unified Access Gateway renforce la sécurité en superposant l'authentification de certification des terminaux au-dessus de l'authentification des utilisateurs afin que l'accès puisse être limité uniquement à partir des terminaux bien connus et en ajoutant une autre couche de sécurité sur l'infrastructure de postes de travail virtuels.

Note Cette fonctionnalité est prise en charge uniquement dans Windows Horizon Client.

- Reportez-vous à la section Configuration de l'authentification par certificat ou carte à puce sur le dispositif Unified Access Gateway dans le document *Déploiement et configuration de VMware Unified Access Gateway* dans <https://docs.vmware.com/fr/Unified-Access-Gateway/index.html>.
- La fonctionnalité Vérifications de la conformité du point de terminaison fournit une couche supplémentaire de sécurité pour accéder à des postes de travail Horizon, en plus des autres services d'authentification utilisateur qui sont disponibles sur Unified Access Gateway. Reportez-vous à la section Vérifications de la conformité du point de terminaison pour Horizon dans le document *Déploiement et configuration de VMware Unified Access Gateway* dans <https://docs.vmware.com/fr/Unified-Access-Gateway/index.html>.

Zone DMZ à deux tronçons

Pour les situations où une zone DMZ à deux tronçons entre Internet et le réseau interne est requise, vous pouvez déployer un dispositif Unified Access Gateway dans la zone DMZ externe en tant que proxy inverse Web avec Unified Access Gateway dans la zone DMZ interne afin de créer une configuration de zone DMZ à deux tronçons. Le trafic transite par un proxy inverse spécifique dans chaque couche de zone DMZ et ne peut pas contourner une couche de zone DMZ. Pour plus d'informations sur la configuration, consultez le document *Déploiement et configuration de VMware Unified Access Gateway*.

Règles de pare-feu pour le Serveur de connexion Horizon

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

Lorsque vous installez le Serveur de connexion, 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 Horizon 7 via les ports mis à jour.

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

Tableau 7-4. Ports ouverts lors de l'installation du Serveur de connexion Horizon

Protocole	Ports	Type d'instance du Serveur de connexion Horizon
JMS	TCP 4001	Standard et réplica
JMS	TCP 4002	Standard et réplica
JMSIR	TCP 4100	Standard et réplica
JMSIR	TCP 4101	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 UDP 8443	Standard, réplica et serveur de sécurité. Une fois la première connexion à Horizon 7 établie, le navigateur Web ou le 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 une instance du Serveur de connexion View pour autoriser cette seconde connexion.
HTTPS	TCP 8472	Standard et réplica Pour la fonctionnalité Architecture Cloud Pod : utilisée pour la communication entre les espaces.
HTTP	TCP 22389	Standard et réplica Pour la fonctionnalité Architecture Cloud Pod : utilisée pour la réplication LDAP globale.
HTTPS	TCP 22636	Standard et réplica Pour la fonctionnalité Architecture Cloud Pod : utilisée pour la réplication LDAP globale sécurisée.

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

Si la topologie réseau contient un pare-feu principal entre les serveurs de sécurité et les instances du Serveur de connexion, 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 du Serveur de connexion ne pourront pas traverser le pare-feu.

Par défaut, les règles IPsec régissent les connexions entre les serveurs de sécurité et les instances du Serveur de connexion. Pour prendre en charge IPsec, le programme d'installation du Serveur de connexion peut définir les règles de pare-feu Windows sur les hôtes Windows Server où les serveurs Horizon 7 sont installés. Pour un pare-feu principal, vous devez définir les règles vous-même.

Note Il est vivement recommandé d'utiliser IPsec. Vous pouvez également désactiver le paramètre global d'Horizon 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 7-5. 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 Horizon	Les serveurs de sécurité utilisent le port UDP 500 pour négocier la sécurité IPsec.
Serveur de sécurité	ESP	S/O	Serveur de connexion Horizon	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 7-6. 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 Horizon	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 Horizon	Les serveurs de sécurité utilisent le port UDP 4500 pour traverser les NAT et négocier la sécurité IPsec.

Réinstaller le Serveur de connexion Horizon avec une configuration de sauvegarde

Dans certaines situations, vous pouvez avoir à réinstaller la version actuelle d'une instance du Serveur de connexion et à restaurer la configuration d'Horizon 7 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 le Serveur de connexion 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 centre de données avec la configuration d'Horizon 7 existante. Vous pouvez aussi l'utiliser si votre déploiement d'Horizon 7 contient une seule instance du Serveur de connexion et qu'un problème se produit avec ce serveur.

Vous n'avez pas à suivre cette procédure si vous avez plusieurs instances du Serveur de connexion dans un groupe répliqué et qu'une seule instance tombe en panne. Vous pouvez simplement réinstaller le Serveur de connexion en tant qu'instance répliquée. Lors de l'installation, vous fournissez des informations de connexion à une autre instance du Serveur de connexion et Horizon 7 restaure la configuration de View LDAP à partir de l'autre instance.

Conditions préalables

- 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 d'Horizon 7 » dans le document *Administration d'Horizon 7*.

- Familiarisez-vous avec les étapes d'installation d'une nouvelle instance du Serveur de connexion. Reportez-vous à la section [Installer le Serveur de connexion Horizon avec une nouvelle configuration](#).

Procédure

- 1 Installez le Serveur de connexion avec une nouvelle configuration.
- 2 Décryptez le fichier LDIF crypté.

Par exemple :

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

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

Par exemple :

```
vdmimport -f MyDecryptedexport.LDF
```

Note À ce stade, la configuration d'Horizon 7 n'est pas encore accessible. Les clients ne peuvent pas accéder au Serveur de connexion ou se connecter à leurs postes de travail.

- 4 Désinstallez le Serveur de connexion 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 le Serveur de connexion.

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

Étape suivante

Configurez le Serveur de connexion et votre environnement Horizon 7 comme vous le feriez après avoir installé une instance du Serveur de connexion avec une nouvelle configuration.

Options de la ligne de commande Microsoft Windows Installer

Pour installer des composants d'Horizon 7 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 d'Horizon 7 sont des programmes MSI et utilisent des fonctionnalités 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 des composants Horizon 7 et saisir `msiexec /?`.

Pour exécuter un programme d'installation de composant d'Horizon 7 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 7-7. Options de ligne de commande du programme de démarrage d'un composant d' Horizon 7

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 d'Horizon 7 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 d'Horizon 7. 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 d'Horizon 7.

Tableau 7-8. 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 Horizon Agent en silence et n'utiliser que des options et des fonctionnalités d'installation par défaut : VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn" Vous pouvez également utiliser l'option /qb pour afficher une boîte de dialogue de progression de base dans une installation non interactive et automatisée. L'option /qn ou /qb est obligatoire pour que l'installation soit silencieuse. Pour plus d'informations sur les autres paramètres /q, consultez le site Web Microsoft Dev Center.
INSTALLDIR	Spécifie un autre chemin d'installation pour le composant d'Horizon 7. Utilisez le format <code>INSTALLDIR=path</code> pour spécifier un chemin d'installation. Vous pouvez ignorer cette propriété MSI si vous voulez installer le composant d'Horizon 7 dans le chemin par défaut. Cette propriété MSI est facultative.

Tableau 7-8. Options de la ligne de commande et propriétés MSI (Suite)

Option ou propriété MSI	Description
ADDLOCAL	<p>Détermine les options spécifiques du composant à installer.</p> <p>Dans une installation interactive, le programme d'installation d'Horizon 7 affiche des options d'installation personnalisée que vous pouvez cocher ou décocher. Dans une installation silencieuse, vous pouvez utiliser la propriété ADDLOCAL pour installer sélectivement des options de configuration en spécifiant les options sur la ligne de commande. Les options que vous ne spécifiez pas explicitement ne sont pas installées.</p> <p>Dans les installations interactives et silencieuses, le programme d'installation d'Horizon 7 installe automatiquement certaines fonctionnalités. Vous ne pouvez pas utiliser ADDLOCAL pour choisir d'installer ou non ces fonctionnalités non facultatives.</p> <p>Tapez ADDLOCAL=ALL pour installer toutes les options de configuration personnalisées pouvant être installées au cours d'une installation interactive, notamment celles installées par défaut et celles que vous devez sélectionner, sauf NGVC. NGVC et SVIAgent s'excluent mutuellement.</p> <p>L'exemple suivant installe Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG et toutes les fonctionnalités prises en charge sur le système d'exploitation invité : VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=ALL"</p> <p>Si vous n'utilisez pas la propriété ADDLOCAL, les options d'installation personnalisée qui sont installées par défaut et les fonctions installées automatiquement sont installées. Les options d'installation personnalisée qui sont désactivées (non sélectionnées) par défaut ne sont pas installées.</p> <p>L'exemple suivant installe Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG et les options d'installation personnalisée activées par défaut qui sont prises en charge sur le système d'exploitation invité : VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn"</p> <p>Pour spécifier des options 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=value,value,value...</p> <p>Vous devez inclure Core lorsque vous utilisez la propriété ADDLOCAL=value,value,value...</p> <p>L'exemple suivant installe Horizon Agent avec les fonctionnalités Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG, Instant Clone Agent et Impression virtuelle :</p> <p>VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,NGVC,ThinPrint"</p> <p>L'exemple précédent n'installe pas d'autres composants, même ceux qui sont installés par défaut de façon interactive.</p> <p>La propriété MSI ADDLOCAL est facultative.</p>
REBOOT	<p>Vous pouvez utiliser l'option REBOOT=ReallySuppress pour autoriser l'exécution de tâches de configuration système avant le redémarrage du système.</p> <p>Cette propriété MSI est facultative.</p>
/l*v log_file	<p>Écrit des informations de journalisation dans le fichier journal spécifié avec une sortie détaillée.</p> <p>Par exemple : /l*v ""%TEMP%\vmmsi.log""</p> <p>Cet exemple génère un fichier journal détaillé semblable à celui généré lors d'une installation interactive.</p> <p>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.</p> <p>L'option /l*v est facultative.</p>

Désinstallation de composants d' Horizon 7 en silence à l'aide d'options de ligne de commande MSI

Vous pouvez désinstaller des composants d'Horizon 7 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 d'Horizon 7.

La chaîne `product_code` identifie les fichiers de produit du composant d'Horizon 7 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 trouver la chaîne `product_code` qui s'applique aux anciennes versions de composants d'Horizon 7, consultez l'article de la base de connaissances de VMware à l'adresse <http://kb.vmware.com/kb/2064845>.

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](#)

Exemple de désinstallation d'Horizon Agent

Pour désinstaller Horizon Agent version 7.0.2 32 bits, entrez la commande suivante :

```
msiexec.exe /qb /x {B23352D8-AD44-4379-A56E-0E337F9C4036}
```

Pour désinstaller Horizon Agent version 7.0.2 64 bits, entrez la commande suivante :

```
msiexec.exe /qb /x {53D6EE37-6B10-4963-81B1-8E2972A1DA4D}
```

Ajoutez un journal détaillé à la commande.

```
/l*v "%TEMP%\vmmsi_uninstall.log"
```

Si vous ne transmettez pas explicitement l'option `/l`, le fichier journal détaillé par défaut est `%TEMP%\MSInnnn.log`, où `nnnn` est un GUID à quatre caractères.

Le processus de désinstallation d'Horizon Agent conserve certaines clés de Registre. Ces clés sont requises pour conserver les informations de configuration du Serveur de connexion qui permet au poste de travail distant de toujours être couplé avec le Serveur de connexion même si l'agent est désinstallé puis réinstallé. La suppression de ces clés de Registre rompra ce couplage.

Les clés de Registre suivantes sont conservées :

- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMware Horizon View Certificates*
- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\Certificates*
- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\CRLs
- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\CTLs
- HKLM\SOFTWARE\Policies\VMware, Inc.\VMware VDM*
- HKLM\SOFTWARE\Policies\VMware, Inc.\vRealize Operations for Horizon*
- HKLM\SOFTWARE\VMware, Inc.\VMware VDM*
- HKLM\SOFTWARE\Wow6432Node\Microsoft\SystemCertificates\VMware Horizon View Certificates*
- HKLM\SOFTWARE\Wow6432Node\Microsoft\SystemCertificates\VMwareView*
- HKLM\SOFTWARE\Wow6432Node\Policies\VMware, Inc.\VMware VDM*
- HKLM\SOFTWARE\Wow6432Node\Policies\VMware, Inc.\vRealize Operations for Horizon*
- HKLM\SOFTWARE\Wow6432Node\VMware, Inc.
- HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM

Configuration de certificats TLS pour des serveurs Horizon 7

8

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

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

Les certificats utilisés pour la communication entre des Serveurs de connexion, et entre des instances d'Horizon Agent et du Serveur de connexion, sont remplacés à l'aide d'un mécanisme automatique et ne peuvent pas être remplacés manuellement. Pour plus d'informations, reportez-vous au document *Sécurité d'Horizon 7*.

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 contient les rubriques suivantes :

- [Comprendre les certificats TLS pour les serveurs Horizon 7](#)
- [Présentation des tâches de configuration des certificats TLS](#)
- [Obtention d'un certificat TLS signé auprès d'une autorité de certification](#)
- [Configurer le Serveur de connexion Horizon, le serveur de sécurité ou View Composer pour utiliser un nouveau certificat TLS](#)
- [Configurer des points de terminaison clients pour approuver des certificats racine et intermédiaires](#)
- [Configuration de la vérification de la révocation des certificats sur des certificats de serveur](#)
- [Configurer PCoIP Secure Gateway pour utiliser un nouveau certificat TLS](#)
- [Configuration d'Horizon Administrator pour approuver un certificat de vCenter Server ou View Composer](#)
- [Avantages à utiliser des certificats TLS signés par une autorité de certification](#)
- [Problèmes de certificat de dépannage sur le Serveur de connexion Horizon et le serveur de sécurité](#)

Comprendre les certificats TLS pour les serveurs Horizon 7

Vous devez suivre certaines recommandations pour la configuration de certificats TLS pour les serveurs Horizon 7 et les composants associés.

Serveur de connexion Horizon et serveur de sécurité

TLS est requis pour les connexions clientes à un serveur. Les instances client du Serveur de connexion, les serveurs de sécurité et les serveurs intermédiaires qui terminent des connexions TLS requièrent des certificats de serveur TLS.

Par défaut, lorsque vous installez le Serveur de connexion 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 une mise à niveau vers Horizon 7 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 Horizon 7 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 de 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 TLS, 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 TLS 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 TLS](#).

Blast Secure Gateway

Par défaut, Blast Secure Gateway (BSG) utilise le certificat TLS configuré pour l'instance du Serveur de connexion 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 Identity Manager 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 Horizon 7 délègue l'authentification à VMware Identity Manager, vous pouvez configurer Horizon 7 pour accepter les sessions authentifiées de SAML 2.0 depuis VMware Identity Manager. Lorsque VMware Identity Manager est configuré pour prendre en charge Horizon 7, les utilisateurs de VMware Identity Manager peuvent se connecter à des postes de travail distants en sélectionnant des icônes de poste de travail sur le portail utilisateur d'Horizon.

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

Avant d'ajouter un authentificateur SAML 2.0 dans Horizon 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 TLS signés par une autorité de certification, reportez-vous à la section [Avantages à utiliser des certificats TLS signés par une autorité de certification](#).

Lorsque des points de terminaison clients se connectent à une instance du Serveur de connexion ou à un serveur de sécurité, ils se voient présenter le certificat de serveur TLS 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 le Serveur de connexion communique avec vCenter Server et View Composer, le Serveur de connexion se voit présenter des certificats de serveur TLS et des certificats intermédiaires de ces serveurs. Pour approuver les serveurs vCenter Server et View Composer Server, l'ordinateur Serveur de connexion 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 le Serveur de connexion, l'ordinateur Serveur de connexion 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 TLS

Pour configurer des certificats de serveur TLS pour des serveurs Horizon 7, vous devez effectuer plusieurs tâches de haut niveau.

Dans un espace d'instances du Serveur de connexion 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 TLS signé auprès d'une autorité de certification.

Si votre entreprise possède déjà un certificat de serveur TLS valide, vous pouvez l'utiliser pour remplacer le certificat de serveur TLS par défaut fourni avec le Serveur de connexion, 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 TLS valide.	Passez directement à l'étape 2.
Vous n'avez pas de certificat de serveur TLS.	Obtenez un certificat de serveur TLS signé auprès d'une autorité de certification.

- 2 Importez le certificat TLS dans le magasin de certificats de l'ordinateur local Windows sur l'hôte du serveur Horizon 7.
- 3 Pour les instances du Serveur de connexion et les serveurs de sécurité, remplacez le nom convivial du certificat en le renommant **vdm**.

Attribuez le nom convivial **vdm** à un seul certificat sur chaque hôte du serveur Horizon 7.

- 4 Sur les ordinateurs Serveur de connexion, 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 du Serveur de connexion n'approuvent pas les certificats racines des certificats de serveur TLS configurés pour les hôtes du serveur de sécurité, de View Composer et de vCenter Server, vous devez également importer ces certificats racines. Effectuez ces étapes uniquement pour les instances du Serveur de connexion. 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 Horizon 7, ils doivent être configurés pour les clients et les ordinateurs qui lancent Horizon 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 Horizon Administrator approuvent les certificats racines et intermédiaires.

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

Le Serveur de connexion effectue la vérification de la révocation des certificats sur les serveurs Horizon 7, 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 du Serveur de connexion, celui-ci effectue également la vérification de la révocation de certificat sur le certificat du serveur SAML.

Obtention d'un certificat TLS signé auprès d'une autorité de certification

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

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

Consultez le document *Scénarios de configuration des certificats TLS pour Horizon 7* 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.

Important Vous devez suivre certaines règles et directives lorsque vous obtenez des certificats TLS signés d'une autorité 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 TLS 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.
- Pour vous conformer aux recommandations de sécurité VMware, utilisez le nom de domaine complet que les périphériques clients utilisent pour se connecter à l'hôte. N'utilisez pas un nom de serveur simple ou une adresse IP, même pour les communications effectuées à l'intérieur de votre domaine interne.
- 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.
- 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 le Serveur de connexion échoueront également ; les serveurs affectés s'afficheront alors en rouge dans le tableau de bord d'Horizon 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](#).

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 Horizon 7 à partir d'un réseau externe, demandez des certificats de serveur TLS qui sont signés par une autorité de certification tierce approuvée.

Conditions préalables

- Déterminez le nom de domaine complet (FQDN) que les périphériques clients utilisent pour se connecter à l'hôte.

Pour se conformer aux recommandations de sécurité de VMware, utilisez le nom de domaine complet plutôt qu'un nom de serveur simple ou une adresse IP, même pour les communications effectuées à l'intérieur de votre domaine interne.

- 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](#).
- 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.

Étape suivante

- 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 ou un serveur de sécurité, remplacez le nom convivial du certificat par **vdm**. Reportez-vous à la section [Modifier le nom convivial du certificat](#).
- 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 TLS au port utilisé par View Composer](#).

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

Pour configurer une instance du Serveur de connexion, un serveur de sécurité ou une instance de View Composer afin qu'ils utilisent un certificat TLS, 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 du Serveur de connexion, du serveur de sécurité ou de View Composer.

Dans un espace d'instances répliquées du Serveur de connexion, 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 TLS configuré pour l'instance du Serveur de connexion 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 le Serveur de connexion ou le serveur de sécurité pour qu'ils utilisent un certificat, vous devez remplacer 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

Pour pouvoir ajouter des certificats au magasin de certificats Windows, vous devez ajouter le composant logiciel enfichable Certificat à la console de gestion Microsoft (MMC) sur l'hôte Windows Server sur lequel le serveur Horizon 7 est installé.

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

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

3 Modifier le nom convivial du certificat

Pour configurer une instance du Serveur de connexion ou un serveur de sécurité pour qu'ils reconnaissent et utilisent un certificat TLS, 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

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

5 Lier un nouveau certificat TLS au port utilisé par View Composer

Si vous configurez un nouveau certificat TLS 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 de certificats Windows, vous devez ajouter le composant logiciel enfichable Certificat à la console de gestion Microsoft (MMC) sur l'hôte Windows Server sur lequel le serveur Horizon 7 est installé.

Conditions préalables

Vérifiez que MMC et le composant logiciel enfichable Certificat sont disponibles sur l'ordinateur Windows Server sur lequel le serveur Horizon 7 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**.

Étape suivante

Importez le certificat de serveur TLS 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 TLS dans le magasin de certificats de l'ordinateur local Windows sur l'hôte Windows Server sur lequel l'instance du Serveur de connexion 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.

Note Si vous déchargez des connexions TLS vers un serveur intermédiaire, vous devez importer le même certificat de serveur TLS sur le serveur intermédiaire et le serveur Horizon 7 déchargé. Pour plus d'informations, reportez-vous à la section « Décharger des connexions TLS sur des serveurs intermédiaires » dans le document *Administration d'Horizon 7*.

Conditions préalables

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](#).

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 **Plus d'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 Dans l'onglet Général de la boîte de dialogue Informations sur le certificat, vérifiez que la déclaration suivante apparaît : Vous avez une clé privée qui correspond à ce certificat.

Étape suivante

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

Modifier le nom convivial du certificat

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

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

Conditions préalables

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](#).

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 du serveur Horizon 7, 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**.

Étape suivante

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

Si les certificats du Serveur de connexion, 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 du Serveur de connexion, 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 racines non approuvés dans toutes les instances du Serveur de connexion répliquées d'un espace.

Note 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 du Serveur de connexion. S'il manque des certificats intermédiaires sur un hôte du Serveur de connexion ou du serveur de sécurité, ils doivent être configurés pour les clients et les ordinateurs qui lancent Horizon Administrator. S'il manque des certificats intermédiaires sur un hôte de View Composer ou vCenter Server, ils doivent être configurés pour chaque instance du Serveur de connexion.

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.

Note Si un authentificateur SAML est configuré pour être utilisé par une instance du Serveur de connexion, les mêmes recommandations s'appliquent à l'authentificateur SAML 2.0. Si l'hôte du Serveur de connexion 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 de gestion Microsoft (MMC) sur l'hôte Windows Server, développez le nœud **Certificats (Ordinateur local)**, puis 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, 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 TLS au port utilisé par View Composer

Si vous configurez un nouveau certificat TLS 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 délègue 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`.

Conditions préalables

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 Arrêtez le service View Composer.
- 2 Ouvrez une invite de commande sur l'hôte Windows Server sur lequel est installé View Composer.
- 3 Accédez au fichier exécutable `SviConfig`.

Le fichier est situé avec l'application View Composer. Le chemin d'accès par défaut est `C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe`.

- 4 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 TLS disponibles dans le magasin des certificats de l'ordinateur local Windows.

- 5 Pour sélectionner un certificat, tapez le numéro du certificat et appuyez sur Entrée.
- 6 Redémarrez le service View Composer pour que vos modifications prennent effet.

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 de serveur Horizon 7 est signé par une autorité de certification qui n'est pas approuvée par des ordinateurs clients et que des ordinateurs clients accèdent à Horizon Administrator, vous pouvez configurer tous les systèmes clients Windows d'un domaine afin qu'ils approuvent les certificats racines 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 NTAAuth.

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, consultez [Configurer Horizon Client pour Mac pour approuver des certificats racine et intermédiaires](#).
- Pour Horizon Client pour iOS, consultez [Configurer Horizon Client pour qu'iOS approuve les certificats d'approbation racine et intermédiaires](#).
- 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

Conditions préalables

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 NTAAuth.

Par exemple : `certutil -dspublish -f path_to_root_CA_cert NTAAuthCA`

- 2 Sur le serveur Active Directory, accédez au plug-in de gestion de stratégie de groupe.

Version d'AD	Chemin de navigation
Windows 2003	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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.
Windows 2012 R2	<ol style="list-style-type: none"> 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.
Windows 2016	<ol style="list-style-type: none"> 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 accédez à **Paramètres Windows > Paramètres de sécurité > Stratégies de clé publique**.
- 4 Importez le certificat.

Option	Description
Certificat racine	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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 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, 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 Transmettez le certificat racine et les certificats intermédiaires à l'ordinateur qui exécute Horizon Client pour Mac.
- 2 Ouvrez le certificat racine sur l'ordinateur Mac.

Le certificat affiche le message suivant : Voulez-vous que votre ordinateur autorise les certificats signés par *nom de l'autorité de certification* 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 des iPads et des iPhones qui exécutent Horizon Client pour iOS, vous pouvez configurer le terminal pour qu'il approuve les certificats racine et intermédiaires. Vous devez distribuer le certificat racine et tous les certificats intermédiaires dans la chaîne d'approbation vers les terminaux.

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. Il n'est pas possible de vérifier l'authenticité du *Nom du certificat*.
L'installation de ce profil modifiera les paramètres de votre iPad. Certificat racine.
L'installation du certificat *Nom du certificat* l'ajoute 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 du Serveur de connexion 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 du Serveur de connexion, le Serveur de connexion effectue également la vérification de la révocation des certificats sur le certificat du serveur SAML 2.0.

Horizon 7 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.

Valeur	Description
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.

Note Si votre entreprise utilise des paramètres proxy pour l'accès Internet, vous devrez peut-être configurer vos ordinateurs Serveur de connexion 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 du Serveur de connexion qui sont utilisées pour des connexions clientes sécurisées. Si une instance du Serveur de connexion ne peut pas accéder à Internet, la vérification de la révocation des certificats peut échouer et l'instance du Serveur de connexion ou les serveurs de sécurité couplés peuvent apparaître en rouge sur le tableau de bord d'Horizon Administrator. Pour résoudre ce problème, reportez-vous à la section « Résolution de la vérification de la révocation des certificats du serveur de sécurité » dans le document *Administration d'Horizon 7*.

Configurer PCoIP Secure Gateway pour utiliser un nouveau certificat TLS

Pour respecter les réglementations de sécurité du secteur ou de la juridiction, vous pouvez remplacer le certificat TLS par défaut généré par le service PCoIP Secure Gateway (PSG) par un certificat signé par une autorité de certification.

Dans Horizon 7, 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 TLS 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 clients et PSG et ne requièrent pas de configuration supplémentaire dans Horizon 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 TLS 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.

Note 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

Lorsqu'une instance du Serveur de connexion 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 à un autre nom de sujet du certificat TLS que vous prévoyez d'utiliser pour PSG.

2 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 ou du serveur de sécurité sur lequel est exécuté PSG.

3 Définir le nom convivial du certificat PSG dans le registre Windows

PSG identifie le certificat TLS 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 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

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'Horizon 7.

Vérifier que le nom du serveur correspond au nom de sujet du certificat PSG

Lorsqu'une instance du Serveur de connexion 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 à un autre nom de sujet du certificat TLS 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 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 du Serveur de connexion 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 à un autre nom de sujet du certificat TLS 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.

Étape suivante

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 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**.

Conditions préalables

- Vérifiez que la longueur de clé est d'au moins 1 024 bits.
- Vérifiez que le certificat TLS 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](#).
- 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](#).
- 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](#).
- Familiarisez-vous avec la modification du nom convivial du certificat. Reportez-vous à la section [Modifier le nom convivial du certificat](#).

Procédure

- 1 Dans la fenêtre MMC sur l'hôte Windows Server, ouvrez le dossier **Certificats (ordinateur local) > Personnel**.

- 2 Importez le certificat TLS 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 l'instruction suivante s'affiche 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.

Note 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.

Étape suivante

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 TLS 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 ou du serveur de sécurité sur lequel est exécuté PSG.

Le nom convivial du certificat **vdm** est utilisé par toutes les instances du Serveur de connexion 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 TLS 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.

Conditions préalables

- 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](#).
- 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](#).

Procédure

- 1 Démarrez l'éditeur de Registre Windows sur l'ordinateur Serveur de connexion 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.

Étape suivante

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'Horizon 7.

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.

Conditions préalables

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 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 d'Horizon Administrator pour approuver un certificat de vCenter Server ou View Composer

Dans le tableau de bord d'Horizon Administrator, vous pouvez configurer Horizon 7 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 TLS 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 TLS signés par une autorité de certification. Dans le tableau de bord d'Horizon Administrator, vous pouvez également configurer Horizon 7 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 TLS 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 TLS spécifique à un domaine Web comme `www.mycorp.com` ou demander un certificat de serveur TLS 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 Horizon 7 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 Horizon et le serveur de sécurité

Des problèmes de certificat sur un serveur Horizon 7 vous empêchent de vous connecter à Horizon Administrator ou provoquent l'affichage d'un indicateur de santé rouge pour un serveur.

Problème

Vous ne pouvez pas vous connecter à Horizon Administrator sur l'instance du Serveur de connexion concernée par le problème. Lorsque vous vous connectez à Horizon Administrator sur une autre instance du Serveur de connexion 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.

Dans l'autre instance du Serveur de connexion, cliquer sur l'indicateur de santé rouge affiche **Certificat SSL : non valide** et **État : (vide)**, ce qui indique qu'aucun certificat valide n'a été trouvé. Le fichier journal d'Horizon 7 contient une entrée de journal de type **ERREUR** avec le texte d'erreur suivant : **Aucun certificat correspondant dans le magasin de clés.**

Les données du journal d'Horizon 7 sont situées dans `C:\ProgramData\VMware\VDM\logs\log-*.txt` sur l'instance du Serveur de connexion.

Cause

Il se peut qu'un certificat ne se soit pas correctement installé sur un serveur Horizon 7 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. Horizon 7 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](#).

- 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](#).

- Vérifiez que le certificat dispose d'un nom convivial de **vdm**.

Reportez-vous à la section [Modifier le nom convivial du certificat](#).

- 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 TLS signé auprès d'une autorité de certification](#).

Activation d' Horizon 7 pour les licences d'abonnement

9

Vous pouvez déployer des licences d'abonnement d'Horizon 7 pour les utiliser avec votre déploiement d'Horizon 7 sur site ou sur VMware Cloud on AWS.

La licence d'abonnement d'Horizon 7 fournit le même produit avec une meilleure flexibilité du déploiement. Les licences d'abonnement d'Horizon 7 activent le déploiement d'Horizon 7 dans le centre de données, le cloud privé et sur VMware Horizon Cloud Service.

Ce chapitre contient les rubriques suivantes :

- [VMware Horizon 7 Cloud Connector](#)
- [Déployer le dispositif virtuel Horizon 7 Cloud Connector avec Horizon 7](#)
- [Configurer un certificat signé par une autorité de certification pour le dispositif virtuel Horizon 7 Cloud Connector](#)

VMware Horizon 7 Cloud Connector

Horizon 7 Cloud Connector est un dispositif virtuel qui connecte un espace Horizon 7 avec VMware Horizon Cloud Service. Horizon 7 Cloud Connector est un composant obligatoire qui pont vos espaces Horizon 7 avec VMware Horizon Cloud Service. Horizon 7 Cloud Connector est requis pour les services de cloud hébergés, notamment les licences d'abonnement Horizon 7, le tableau de bord d'état de santé et Horizon Help Desk Tool.

Vous devez disposer d'un compte My VMware actif pour acheter une licence Horizon 7 sur <https://my.vmware.com>. Vous recevez ensuite un e-mail d'abonnement avec le lien de téléchargement d'Horizon 7 Cloud Connector en tant que fichier OVA.

Lorsque vous déployez le dispositif virtuel Horizon 7 Cloud Connector à partir de vSphere Web Client, vous coupez Cloud Connector avec l'espace de Serveur de connexion que vous voulez connecter à Horizon Cloud Service. Dans le cadre du processus de couplage, le dispositif virtuel Horizon 7 Cloud Connector connecte le Serveur de connexion à Horizon Cloud Service pour gérer la licence d'abonnement Horizon 7 et d'autres services. Avec une licence d'abonnement Horizon 7, il n'est pas nécessaire d'entrer manuellement une clé de licence Horizon 7 pour l'activation du produit VMware Horizon 7. Toutefois, vous n'avez pas besoin d'utiliser les clés de licence pour activer la prise en charge des composants, tels que vSphere, App Volumes, etc.

Note Le dispositif virtuel Horizon 7 Cloud Connector ne prend pas en charge un environnement IPv6.

Déployer le dispositif virtuel Horizon 7 Cloud Connector avec Horizon 7

Après avoir acheté une licence d'abonnement, vous recevrez un e-mail d'abonnement de licence, qui contient le lien de téléchargement du dispositif virtuel Horizon 7 Cloud Connector. Vous pouvez installer et coupler le dispositif virtuel Horizon 7 Cloud Connector avec un Serveur de connexion dans un espace.

Conditions préalables

- Horizon 7 version 7.6 ou version ultérieure.
- Vous devez posséder un compte My VMware sur <https://my.vmware.com> pour acheter une licence d'abonnement d'Horizon 7.
- Téléchargez le dispositif virtuel Horizon 7 Cloud Connector à partir de l'e-mail de licence d'abonnement que vous avez reçu de my.vmware.com.
- Vérifiez le serveur de connexion que vous souhaitez coupler au dispositif virtuel Horizon 7 Cloud Connector. Vous pouvez coupler le dispositif virtuel Horizon 7 Cloud Connector à un seul serveur de connexion installé dans un espace sur site à la fois.
- Si le dispositif virtuel Horizon 7 Cloud Connector ne fait pas partie du domaine Active Directory auquel le Serveur de connexion est joint, ajoutez le nom de domaine complet du Serveur de connexion à coupler avec Horizon 7 Cloud Connector au fichier `/etc/hosts` sur le dispositif virtuel Horizon 7 Cloud Connector.
- Si vous utilisez le navigateur Web Microsoft Internet Explorer, vérifiez que le mode de compatibilité est désactivé pour afficher l'interface utilisateur du dispositif Horizon 7 Cloud Connector.
- Déployez et joignez le dispositif virtuel Horizon 7 Cloud Connector avec l'adresse IP statique à Active Directory. Ajoutez l'entrée de recherche directe et inversée du dispositif virtuel Horizon 7 Cloud Connector dans le DNS de votre domaine Active Directory avant de commencer le déploiement.

Procédure

- 1 Téléchargez le dispositif Horizon 7 Cloud Connector à partir du lien fourni dans l'e-mail de l'abonnement de votre compte. Le dispositif Horizon 7 Cloud Connector est téléchargeable en tant que fichier OVA.
- 2 Utilisez vSphere Web Client pour déployer le dispositif Horizon 7 Cloud Connector en tant que modèle OVF. Pour plus d'informations sur le déploiement des modèles OVF, consultez la documentation *Administration d'une machine virtuelle vSphere*.

Note Lorsque vous entrez un mot de passe racine pour le modèle OVF, vous devez vérifier que le mot de passe contient au minimum huit caractères, avec une majuscule, un chiffre et un caractère spécial.

- 3 Dans vSphere Web Client, mettez sous tension le dispositif Horizon 7 Cloud Connector.
L'adresse IP de l'interface utilisateur du dispositif Horizon 7 Cloud Connector s'affiche.
- 4 Dans un navigateur Web, entrez l'adresse IP du dispositif Horizon 7 Cloud Connector pour vous connecter à l'interface utilisateur d'Horizon 7 Cloud Connector.
Utilisez vos informations d'identification du compte My VMware pour vous connecter.
- 5 Connectez le dispositif Horizon 7 Cloud Connector avec l'instance du Serveur de connexion sur site. Dans la zone **Se connecter au Serveur de connexion Horizon 7**, entrez le nom de domaine complet du Serveur de connexion qui est hébergé sur site et cliquez sur **Se connecter**.
- 6 Cochez la case pour vérifier l'empreinte numérique du certificat du Serveur de connexion.

Note Cette vérification est ignorée si le Serveur de connexion dispose d'un certificat d'autorité de certification racine valide.

- 7 Entrez le nom de domaine, le nom d'utilisateur et le mot de passe du Serveur de connexion et cliquez sur **Se connecter**.

Note Pour optimiser l'audit des actions d'Horizon 7 Cloud Connector, utilisez un nom d'utilisateur et un mot de passe uniques pour le Serveur de connexion.

- 8 Éventuellement, si le Serveur de connexion est déjà couplé avec un autre dispositif Horizon 7 Cloud Connector, cliquez sur **Accepter** pour supprimer le couplage existant et le coupler avec le dispositif Horizon 7 Cloud Connector que vous avez téléchargé.
- 9 Pour configurer l'espace Horizon 7 sur Horizon Cloud Service, entrez un nom pour le nœud, sélectionnez emplacement du centre de données et entrez une description facultative.
L'espace Horizon 7 est correctement couplé avec VMware Horizon Cloud Service.
- 10 Pour reconfigurer éventuellement les détails du Serveur de connexion dans le même espace, cliquez sur **Reconfigurer** et suivez les étapes pour terminer l'assistant.
- 11 Pour supprimer éventuellement la connexion entre le Serveur de connexion sur site et Horizon Cloud Service, cliquez sur **Débrancher**.

Note Ne supprimez pas le dispositif virtuel Horizon 7 Cloud Connector de vCenter Server avant de cliquer sur **Déconnecter**.

Étape suivante

- Affichez les détails de la licence d'abonnement dans Horizon Administrator. Pour plus d'informations, reportez-vous au document *Administration d'Horizon 7*.
- Si vous devez mettre à niveau vers la dernière version du dispositif virtuel Horizon 7 Cloud Connector, reportez-vous au document *Mises à niveau d'Horizon 7*.
- Pour vous connecter à la console d'administration d'Horizon Cloud, reportez-vous au *Guide d'administration de VMware Horizon Cloud Service on Microsoft Azure* disponible à l'adresse <https://docs.vmware.com/fr/VMware-Horizon-Cloud-Service/index.html>.

Configurer un certificat signé par une autorité de certification pour le dispositif virtuel Horizon 7 Cloud Connector

Pour renforcer la sécurité, vous pouvez configurer un certificat personnalisé signé par une autorité de certification pour le dispositif virtuel Horizon 7 Cloud Connector.

Conditions préalables

- Vérifiez que la chaîne de certificats complète est au format PEM.
- Vérifiez que la clé privée est disponible au format PEM.
- Vérifiez que le nom de domaine complet et l'autre nom du sujet sont inclus dans le certificat émis.

Procédure

- 1 Ouvrez une session SSH vers le dispositif virtuel Horizon 7 Cloud Connector.
- 2 Copiez le certificat signé par une autorité de certification dans le répertoire `/root/server.crt`.
- 3 Copiez la clé signée par une autorité de certification dans le répertoire `/root/server.key`.
- 4 Sauvegardez le certificat existant.

Utilisez la commande suivante :

```
cp /etc/nginx/ssl/server.crt /etc/nginx/ssl/server.crt.orig
```

- 5 Sauvegardez la clé existante.

Utilisez la commande suivante :

```
cp /etc/nginx/ssl/server.key /etc/nginx/ssl/server.key.orig
```

- 6 Copiez le fichier `nginx.conf` existant.

Utilisez la commande suivante :

```
cp /etc/nginx/nginx.conf /etc/nginx/nginx.conf.orig
```

- 7 Copiez le certificat de l'autorité de certification dans le répertoire `/etc/nginx/ssl`.

Utilisez la commande suivante :

```
cp /root/server.crt /etc/nginx/ssl/server.crt
```

- 8 Copiez le fichier de clé du certificat de l'autorité de certification dans le répertoire `/etc/nginx/ssl`.

Utilisez la commande suivante :

```
cp /root/server.key /etc/nginx/ssl/server.key
```

9 Vérifiez le propriétaire et l'autorisation du fichier de certificat et de clé.

Utilisez les commandes suivantes :

```
chown -R root:root /etc/nginx/ssl
```

```
chmod -R 600 /etc/nginx/ssl
```

10 Vérifiez que le nom de domaine complet émis dans le certificat correspond à la directive du nom de serveur dans le bloc 443 d'écoute du serveur dans le fichier de configuration nginx sur /etc/nginx/nginx.conf.**11** Vérifiez et redémarrez nginx.

Utilisez les commandes suivantes :

```
nginx -t
```

```
systemctl restart nginx
```

12 Testez le nouveau certificat en rechargeant l'URL de l'interface utilisateur d'Horizon 7 Cloud Connector dans un navigateur Web.**13** (Facultatif) Si le certificat fonctionne correctement, supprimez les fichiers sauvegardés.

Utilisez les commandes suivantes :

```
rm /etc/nginx/ssl/server.crt.orig
```

```
rm /etc/nginx/ssl/server.key.orig
```

```
rm /etc/nginx/nginx.conf.orig
```

14 Supprimez les certificats copiés de l'autorité de certification et les fichiers de clés dans le répertoire racine.

Utilisez les commandes suivantes :

```
rm /root/server.crt
```

```
rm /root/server.key
```

Configuration d' Horizon 7 pour la première fois

10

Après l'installation du logiciel du serveur Horizon 7 et la configuration de certificats SSL pour les serveurs, vous devez prendre des mesures supplémentaires pour configurer un environnement Horizon 7 fonctionnel.

Vous configurez des comptes d'utilisateurs pour vCenter Server et View Composer, installez une clé de licence Horizon 7, ajoutez vCenter Server et View Composer à votre environnement Horizon 7, configurez PCoIP Secure Gateway et un tunnel sécurisé et, éventuellement, dimensionnez les paramètres Windows Server pour prendre en charge votre environnement Horizon 7.

Ce chapitre contient les rubriques suivantes :

- [Configuration de comptes utilisateur pour vCenter Server, View Composer et les clones instantanés](#)
- [Configuration du Serveur de connexion Horizon pour la première fois](#)
- [Configuration des connexions Horizon Client](#)
- [Remplacement des ports par défaut pour les services Horizon 7](#)
- [Dimensionnement de paramètres de Windows Server pour prendre en charge votre déploiement](#)

Configuration de comptes utilisateur pour vCenter Server, View Composer et les clones instantanés

Pour utiliser vCenter Server avec Horizon 7, vous devez configurer un compte d'utilisateur avec des privilèges vCenter Server appropriés. Vous pouvez créer un rôle vCenter Server avec des privilèges appropriés et attribuer ce rôle au compte d'utilisateur vCenter Server.

Si vous n'installez pas View Composer sur la même machine que vCenter Server, vous devez également créer un compte d'utilisateur dans Active Directory que Horizon 7 peut utiliser pour s'authentifier sur le service View Composer de la machine autonome.

Si vous utilisez View Composer, vous devez créer un troisième compte d'utilisateur dans Active Directory qui permet à View Composer d'effectuer certaines opérations dans Active Directory. View Composer requiert que ce compte joigne les machines virtuelles de clone lié à votre domaine Active Directory. Reportez-vous à la section [Créer un compte d'utilisateur pour les opérations AD de View Composer](#).

Si vous utilisez des clones instantanés, vous devez créer un compte utilisateur dans Active Directory qui permet au Serveur de connexion d'effectuer certaines opérations dans Active Directory. Le Serveur de connexion requiert que ce compte joigne les machines virtuelles de clone instantané à votre domaine Active Directory. Reportez-vous à la section [Créer un compte d'utilisateur pour les opérations Instant Clone](#).

Pour résumer, lorsque vous configurez Horizon 7 pour la première fois, vous fournissez ces comptes d'utilisateur dans Horizon Administrator :

- L'utilisateur vCenter Server permet à Horizon 7 et à View Composer d'effectuer des opérations dans vCenter Server.
- L'utilisateur du serveur View Composer Server autonome permet à Horizon 7 de s'authentifier sur le service View Composer d'une machine autonome.

Si vous installez View Composer sur la même machine que vCenter Server, l'utilisateur de vCenter Server effectue les deux fonctions précédentes, et vous n'utilisez pas un utilisateur de serveur View Composer Server autonome.

- L'utilisateur de View Composer pour les opérations AD permet à View Composer d'effectuer certaines opérations dans Active Directory.
- L'utilisateur du clone instantané pour les opérations AD permet au Serveur de connexion d'effectuer certaines opérations dans Active Directory.

Où utiliser l'utilisateur de vCenter Server et les utilisateurs de View Composer

Après la création et la configuration de ces comptes d'utilisateurs, vous spécifiez les noms d'utilisateur dans Horizon Administrator.

- Vous spécifiez un utilisateur de vCenter Server lorsque vous ajoutez vCenter Server à Horizon 7.
- Vous spécifiez un utilisateur de serveur View Composer Server autonome lorsque vous configurez les paramètres de View Composer et sélectionnez **Serveur View Composer autonome**.
- Vous spécifiez un utilisateur de View Composer pour les opérations AD lorsque vous configurez des domaines View Composer.
- Vous spécifiez l'utilisateur de View Composer pour les opérations AD lorsque vous créez des pools de clones liés.

Configurer un utilisateur de vCenter Server pour Horizon 7 et View Composer

Pour configurer un compte d'utilisateur qui permet à Horizon 7 d'effectuer des opérations sur vCenter Server, vous devez attribuer un rôle vCenter Server avec des privilèges appropriés à cet utilisateur.

La liste de privilèges que vous devez ajouter au rôle de vCenter Server varie, selon que vous utilisiez Horizon 7 avec ou sans View Composer. Le service View Composer effectue des opérations dans vCenter Server qui nécessitent des privilèges en complément des privilèges de base.

Si vous installez View Composer sur la même machine que vCenter Server, vous devez définir l'utilisateur de vCenter Server comme administrateur système local sur la machine vCenter Server. Cette exigence permet à Horizon 7 de s'authentifier sur le service View Composer.

Si vous installez View Composer sur une autre machine que vCenter Server, vous n'avez pas besoin de définir l'utilisateur de vCenter Server comme un administrateur local sur la machine vCenter Server. Cependant, vous devez créer un compte d'utilisateur de serveur View Composer Server autonome qui doit être un administrateur local sur la machine View Composer.

Conditions préalables

- Dans Active Directory, créez un utilisateur dans le domaine du Serveur de connexion ou un domaine approuvé. Reportez-vous à la section [Création d'un compte d'utilisateur pour vCenter Server](#).
- 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](#).
- Si vous utilisez View Composer, familiarisez-vous avec les privilèges requis supplémentaires. Reportez-vous à la section [Privilèges de View Composer et d'Instant Clone requis pour l'utilisateur de vCenter Server](#).

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 minimaux dont le Serveur de connexion 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**, puis sélectionnez des privilèges pour ce rôle.

Ce rôle doit posséder tous les privilèges dont le Serveur de connexion et View Composer ont besoin pour fonctionner dans vCenter Server.

- Si vous utilisez Horizon 7 sans View Composer, vous pouvez créer un rôle encore plus limité avec les privilèges minimum dont le Serveur de connexion 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**, puis sélectionnez des privilèges pour le rôle.

- Si vous utilisez des clones instantanés, vous pouvez créer un rôle limité avec les privilèges minimaux requis par le serveur de connexion 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 Instant Clone**, et sélectionnez des privilèges pour le rôle. Pour les privilèges Instant Clone, reportez-vous à la section [Privilèges de View Composer et d'Instant Clone requis pour l'utilisateur de vCenter Server](#).

- 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.

Note 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 installez View Composer sur la même machine que vCenter Server, ajoutez le compte d'utilisateur de vCenter Server comme membre du groupe Administrateurs local sur la machine vCenter Server.

Cette étape n'est pas requise si vous n'installez pas View Composer sur la même machine que vCenter Server.

Étape suivante

Dans Horizon Administrator, lorsque vous ajoutez vCenter Server à Horizon 7, spécifiez l'utilisateur de vCenter Server. Reportez-vous à la section [Ajouter des instances de vCenter Server à Horizon 7](#).

Privilèges requis pour l'utilisateur de vCenter Server

L'utilisateur de vCenter Server doit disposer de privilèges vCenter Server suffisants pour permettre à Horizon 7 d'effectuer des opérations dans vCenter Server. Créez un rôle View Manager pour l'utilisateur de vCenter Server avec les privilèges requis.

Tableau 10-1. Privilège requis pour le rôle View Manager

Groupe de privilèges	Privilèges à activer
Dossier	Créer le dossier Supprimer le dossier
Banque de données	Allouer de l'espace

Tableau 10-1. Privilège requis pour le rôle View Manager (Suite)

Groupe de privilèges	Privilèges à activer
Machine virtuelle	<p>Dans Configuration :</p> <ul style="list-style-type: none"> ■ Ajouter ou supprimer un périphérique ■ Avancé ■ Modifier les paramètres de périphérique <p>Dans Interaction :</p> <ul style="list-style-type: none"> ■ Mettre hors tension ■ Mettre sous tension ■ Réinitialiser ■ Interrompre ■ Exécuter des opérations d'effacement ou de réduction <p>Dans Inventaire :</p> <ul style="list-style-type: none"> ■ Créer un nouveau ■ Créer à partir de l'existant ■ Supprimer <p>Dans Provisionnement :</p> <ul style="list-style-type: none"> ■ Personnaliser ■ Déployer un modèle ■ Lire des spécifications de personnalisation ■ Modèle de clone ■ Cloner la machine virtuelle
Ressource	Attribuer une machine virtuelle au pool de ressources
Global	<p>Agir en tant que vCenter Server</p> <p>L'utilisateur de vCenter Server requiert ce privilège même si vous n'utilisez pas View Storage Accelerator.</p>
Hôte	<p>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.</p> <p>Dans Configuration :</p> <ul style="list-style-type: none"> ■ Paramètres avancés
Stockage basé sur le profil (si vous utilisez des banques de données vSAN ou Virtual Volumes)	(tous)

Privilèges de View Composer et d'Instant Clone requis pour l'utilisateur de vCenter Server

Pour prendre en charge View Composer ou les Instant Clones, l'utilisateur de vCenter Server doit disposer de privilèges supplémentaires à ceux requis pour prendre en charge Horizon 7.

Privilèges de View Composer et d'Instant Clone répertorie l'ensemble des privilèges requis pour View Composer, View Manager et les Instant Clones.

Tableau 10-2. Privilèges de View Composer et d'Instant Clone

Groupe de privilèges sur vCenter Server	Privilèges à activer
Dossier	Créer un dossier Supprimer le dossier
Banque de données Tableau 10-2	Allouer de l'espace Parcourir la banque de données Opérations de fichier de niveau inférieur
Hôte	Dans Inventaire <ul style="list-style-type: none"> ■ Modifier le cluster
Machine virtuelle	Dans Configuration (tous) Dans Interaction : <ul style="list-style-type: none"> ■ Mettre hors tension ■ Mettre sous tension ■ Réinitialiser ■ Interrompre ■ Exécuter des opérations d'effacement ou de réduction ■ Connexion périphérique Dans Inventaire (tous) Dans Gestion des snapshots (tous) Dans Provisionnement : <ul style="list-style-type: none"> ■ Personnaliser ■ Déployer un modèle ■ Lire des spécifications de personnalisation ■ Modèle de clone ■ Cloner la machine virtuelle ■ Autoriser l'accès au disque
Ressource	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 hors tension
Global	Activer des méthodes Désactiver des méthodes Balise système Gérer des attributs personnalisés Définir un attribut personnalisé Le privilège suivant est requis pour mettre en œuvre View Storage Accelerator, qui active la mise en cache de l'hôte ESXi. L'utilisateur de vCenter Server requiert ce privilège même si vous n'utilisez pas View Storage Accelerator. Agir en tant que vCenter Server
Réseau	(tous)
Stockage basé sur le profil	(tous : si vous utilisez des banques de données vSAN ou Virtual Volumes)

Tableau 10-2. Privilèges de View Composer et d'Instant Clone (Suite)

Groupe de privilèges sur vCenter Server	Privilèges à activer
Vues de stockage	Vue
Opérations cryptographiques	<p>Les privilèges suivants sont requis si vous utilisez des machines virtuelles Instant Clone équipées d'un vTPM (Virtual Trusted Platform Module).</p> <ul style="list-style-type: none"> ■ Cloner ■ Déchiffrer ■ Accès direct ■ Chiffrer ■ Gérer KMS ■ Migrer

Configuration du Serveur de connexion Horizon pour la première fois

Une fois vous avez installé le Serveur de connexion, vous devez installer une licence produit et ajouter des serveurs vCenter Server et des services View Composer à Horizon 7. 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 Horizon 7 et s'affichent automatiquement dans Horizon Administrator.

Horizon Administrator et Serveur de connexion Horizon

Horizon Administrator fournit une interface de gestion Web pour Horizon 7.

Le Serveur de connexion Horizon peut disposer de plusieurs instances qui servent de serveurs réplica ou de serveurs de sécurité. En fonction de votre déploiement d'Horizon 7, vous pouvez obtenir une interface d'Horizon Administrator avec chaque instance d'un Serveur de connexion.

Utilisez les meilleures pratiques suivantes pour utiliser Horizon Administrator avec un Serveur de connexion :

- Utilisez le nom d'hôte et l'adresse IP du Serveur de connexion pour vous connecter à Horizon Administrator. Utilisez l'interface d'Horizon Administrator pour gérer le Serveur de connexion et des serveurs de sécurité ou des serveurs réplica associés.
- Dans un environnement d'espace, vérifiez que tous les administrateurs utilisent le nom d'hôte et l'adresse IP du même serveur de connexion pour vous connecter à Horizon Administrator. N'utilisez pas le nom d'hôte et l'adresse IP de l'équilibrage de charge pour accéder à une page Web d'Horizon Administrator.

- Pour identifier l'espace du Serveur de connexion que vous utilisez, vous pouvez voir le nom de l'espace dans l'en-tête d'Horizon Administrator et dans l'onglet du navigateur Web.

Note Si vous utilisez des dispositifs Unified Access Gateway plutôt que des serveurs de sécurité, vous devez utiliser l'API REST Unified Access Gateway pour gérer les dispositifs Unified Access Gateway. Les versions antérieures de Unified Access Gateway sont nommées Access Point. Pour plus d'informations, consultez le document *Déploiement et configuration d'Unified Access Gateway*.

Ouvrir une session sur Horizon Administrator

Pour effectuer des tâches de configuration initiale, vous devez ouvrir une session sur Horizon Administrator.

Conditions préalables

Vérifiez que vous utilisez un navigateur Web pris en charge par Horizon Administrator. Reportez-vous à la section [Exigences d'Horizon Administrator](#).

Procédure

- 1 Ouvrez votre navigateur Web et saisissez l'URL suivante, où *server* est le nom d'hôte de l'instance du serveur de connexion.

https://server/admin

Note Vous pouvez utiliser l'adresse IP si vous avez accès à une instance du Serveur de connexion lorsque le nom de l'hôte ne peut être résolu. Toutefois, dans ce cas, l'hôte que vous contactez ne correspond pas au certificat TLS configuré pour l'instance du Serveur de connexion, ce qui bloque l'accès ou autorise l'accès avec une sécurité limitée.

Votre accès à Horizon Administrator dépend du type de certificat configuré sur l'ordinateur Serveur de connexion.

Si vous ouvrez votre navigateur sur l'hôte du Serveur de connexion, 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 Horizon 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 TLS actuel.

2 Connectez-vous à l'aide d'un compte qui dispose du rôle Administrateurs.

Vous établissez une attribution initiale au rôle Administrateurs lorsque vous installez une instance autonome du Serveur de connexion ou la première instance du Serveur de connexion dans un groupe répliqué. Par défaut, le compte que vous utilisez pour installer le Serveur de connexion est sélectionné, mais vous pouvez modifier ce compte en groupe local Administrateurs ou en groupe global de domaine.

Si vous choisissez le groupe local Administrateurs, vous pouvez utiliser n'importe quel utilisateur de domaine ajouté à ce groupe directement ou via l'appartenance au groupe global. Vous ne pouvez pas utiliser des utilisateurs locaux ajoutés à ce groupe.

Après avoir ouvert une session sur Horizon Administrator, vous pouvez utiliser **Configuration de View > Administrateurs** afin de modifier la liste des utilisateurs et des groupes ayant le rôle Administrateurs.

Installer la clé de licence produit

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

Note La clé de licence produit n'est pas requise si vous avez une licence d'abonnement Horizon 7. Pour plus d'informations sur les licences d'abonnement, reportez-vous à la section [Chapitre 9 Activation d'Horizon 7 pour les licences d'abonnement](#).

Lors de votre première ouverture de session, Horizon Administrator affiche la page Licence produit et utilisation.

Une fois la clé de licence installée, Horizon 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 du Serveur de connexion 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.

Note Le Serveur de connexion nécessite une clé de licence valide. La clé de licence de produit est une clé de 25 caractères.

Procédure

- 1 Dans Horizon 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 7 que la licence produit vous autorise à utiliser.

Les fonctionnalités et capacités de VMware Horizon 7 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 Horizon 7

Vous devez configurer Horizon 7 pour qu'il se connecte aux instances de vCenter Server dans votre déploiement Horizon 7. vCenter Server crée et gère les machines virtuelles que Horizon 7 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 Horizon 7.

Horizon 7 se connecte à l'instance de vCenter Server via un canal sécurisé (SSL).

Conditions préalables

- Installez la clé de licence produit du Serveur de connexion.
- Configurez un utilisateur de vCenter Server autorisé à effectuer dans vCenter Server les opérations nécessaires à la prise en charge de Horizon 7. 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 Horizon 7 et View Composer](#).

- Vérifiez qu'un certificat de serveur TLS/SSL est installé sur l'hôte de vCenter Server. Dans un environnement de production, installez un certificat 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 Horizon 7.

- Vérifiez que toutes les instances du Serveur de connexion 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 du Serveur de connexion. 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](#).

- 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 Horizon 7.
- 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.
- Si vous prévoyez d'utiliser Horizon 7 en mode FIPS, vérifiez que vous disposez de vCenter Server 6.0 ou version ultérieure et d'hôtes ESXi 6.0 ou version ultérieure.

Pour plus d'informations, reportez-vous à la section [Chapitre 4 Installation d'Horizon 7 en mode FIPS](#).

- 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](#) 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](#).

Procédure

- 1 Dans Horizon 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.

Note Si vous entrez un serveur à l'aide d'un nom DNS ou d'une URL, Horizon 7 n'effectue pas de recherche DNS pour vérifier si un administrateur a précédemment ajouté ce serveur à Horizon 7 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.

Étape suivante

Configurez les paramètres de View Composer.

- Si l'instance de vCenter Server est configurée avec un certificat SSL signé et si le Serveur de connexion 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 TLS par défaut](#).

Si Horizon 7 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 au Serveur de connexion de se connecter au service View Composer. View Composer peut être installé sur sa propre machine autonome ou sur la même machine que vCenter Server.

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

Conditions préalables

- Vérifiez que vous avez configuré le Serveur de connexion 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 Horizon 7](#).
- Vérifiez que ce service View Composer n'est pas déjà configuré pour se connecter à une instance de vCenter Server différente.
- Si vous avez installé View Composer sur une machine autonome, vérifiez que vous avez créé un compte d'utilisateur de serveur View Composer Server autonome. Ce compte d'utilisateur de domaine doit être membre du groupe Administrateurs local sur la machine View Composer.

Procédure

- 1 Dans Horizon 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 la machine View Composer.

Option	Description
View Composer est installé sur la même machine que vCenter Server.	<p>a Sélectionnez View Composer est co-installé avec vCenter Server.</p> <p>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.</p>
View Composer est installé sur sa propre machine séparée.	<p>a Sélectionnez Serveur View Composer Server autonome.</p> <p>b Dans la zone de texte de l'adresse du serveur View Composer Server, tapez le nom de domaine complet (FQDN) de la machine View Composer.</p> <p>c Tapez le nom d'un compte d'utilisateur de domaine qui peut s'authentifier sur le service View Composer.</p> <p>Ce compte doit être membre du groupe Administrateurs local sur la machine View Composer autonome.</p> <p>Par exemple : domain.com\user ou user@domain.com</p> <p>d Tapez le mot de passe de ce compte d'utilisateur de domaine.</p> <p>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.</p>

- 4 Cliquez sur **Suivant** pour afficher la page Domaines View Composer.

Étape suivante

Configurez les domaines de View Composer.

- Si l'instance de View Composer est configurée avec un certificat SSL signé et si le Serveur de connexion 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 TLS par défaut](#).

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 Horizon Administrator.

Conditions préalables

- Votre administrateur Active Directory doit créer un utilisateur View Composer pour les opérations AD. Cet utilisateur de domaine doit avoir l'autorisation d'ajouter et de supprimer des machines virtuelles dans le domaine Active Directory qui contient vos clones liés. Pour plus d'informations sur les autorisations requises pour cet utilisateur, reportez-vous à [Créer un compte d'utilisateur pour les opérations AD de View Composer](#).
- Dans Horizon Administrator, vérifiez que vous avez rempli les pages Informations sur vCenter Server et Paramètres de View Composer dans l'assistant Ajouter un serveur vCenter Server.

Procédure

- 1 Dans la page Domaines View Composer, cliquez sur **Ajouter** pour ajouter l'utilisateur de View Composer aux informations du compte des opérations AD.
- 2 Saisissez le nom de domaine du domaine Active Directory.
Par exemple : **domain.com**
- 3 Tapez le nom d'utilisateur de domaine, notamment le nom de domaine, de l'utilisateur de View Composer.
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.

Étape suivante

Activez la récupération d'espace disque de machine virtuelle et configurez View Storage Accelerator pour Horizon 7.

Ajouter un administrateur de domaine Instant Clone

Avant de créer un pool de postes de travail Instant Clone, vous devez ajouter un administrateur de domaine Instant Clone à Horizon 7.

L'administrateur de domaine Instant Clone doit disposer de certains privilèges de domaine Active Directory.

Procédure

- 1 Dans Horizon Administrator, sélectionnez **Configuration de View > Administrateurs de domaine Instant Clone**.
- 2 Cliquez sur **Ajouter**.
- 3 Entrez le nom de connexion et le mot de passe de l'administrateur de domaine Instant Clone.

Autoriser vSphere à récupérer de l'espace disque dans des machines virtuelles de clone lié

Dans vSphere 5.1 et versions ultérieures, vous pouvez activer la fonctionnalité de récupération d'espace disque pour Horizon 7. À partir de vSphere 5.1, Horizon 7 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, Horizon 7 peut conserver les clones liés proches de la taille réduite avec laquelle ils démarrent lors de leur premier provisionnement.

La fonctionnalité 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, Horizon 7 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 Horizon 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.

View Composer Array Integration (VCAI) n'est pas pris en charge dans les pools contenant des machines virtuelles intégrant des disques à optimisation d'espace. VCAI utilise la technologie de snapshot NFS natif VAAI (vStorage APIs for Array Integration) pour cloner des machines virtuelles.

Conditions préalables

- 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 Horizon Administrator, fournissez les renseignements dans 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 Horizon 7 5.2 ou version ultérieure. Vous devez sélectionner **Activer la récupération d'espace** si vous effectuez une mise à niveau vers Horizon 7 5.2 ou version ultérieure depuis Horizon 7 5.1 ou version antérieure.

Étape suivante

Sur la page Paramètres de stockage, configurez View Storage Accelerator.

Pour terminer la configuration de la récupération d'espace disque dans Horizon 7, configurez la récupération d'espace pour les pools de postes de travail.

Configurer View Storage Accelerator pour vCenter Server

Dans vSphere 5.1 et versions ultérieures, 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 Horizon 7 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 Horizon 7.

Vous activez la mise en cache sur vos hôtes ESXi en sélectionnant le paramètre View Storage Accelerator dans l'assistant vCenter Server dans Horizon Administrator, comme décrit dans cette procédure.

Vérifiez que View Storage Accelerator est également configuré pour des pools de postes de travail individuels. 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.

View Storage Accelerator est activé pour un pool de postes de travail par défaut. Vous pouvez activer ou désactiver cette fonctionnalité lors de la création ou de la modification d'un pool. La meilleure approche consiste à activer cette fonctionnalité lorsque vous créez un pool de postes de travail pour la première fois. Si vous activez cette fonctionnalité en modifiant un pool existant, vous devez vous assurer qu'un nouveau réplica et ses disques digest soient créés avant que des clones liés soient provisionnés. Vous pouvez créer un nouveau réplica en recomposant le pool sur un nouveau snapshot ou en rééquilibrant le pool sur une nouvelle banque de données. Les fichiers digest peuvent être configurés uniquement pour des machines virtuelles dans un pool de postes de travail où elles sont désactivées.

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.

La technologie de snapshot NFS natif (VAAI) n'est pas prise en charge dans les pools activés pour View Storage Accelerator.

View Storage Accelerator est maintenant conçu pour fonctionner dans des configurations qui utilisent la hiérarchisation de réplica Horizon 7, 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 Horizon 7 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.

Important Si vous prévoyez d'utiliser cette fonctionnalité et que vous utilisez plusieurs espaces View qui partagent des hôtes ESXi, vous devez activer la fonction View Storage Accelerator pour tous les pools qui se trouvent sur les hôtes ESXi partagés. Si les paramètres ne sont pas les mêmes sur tous les espaces, cela peut entraîner l'instabilité des machines virtuelles des hôtes ESXi partagés.

Conditions préalables

- Vérifiez que la version de vos hôtes vCenter Server et ESXi est la version 5.1 ou ultérieure.

Dans un cluster ESXi, vérifiez que la version de tous les hôtes est la version 5.1 ou ultérieure.

- Vérifiez que l'utilisateur de vCenter Server a reçu le privilège **Hôte > Configuration > Paramètres avancés** dans vCenter Server.

Reportez-vous à la section [Configuration de comptes utilisateur pour vCenter Server, View Composer et les clones instantanés](#).

Procédure

- 1 Dans Horizon Administrator, fournissez les renseignements dans 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 Horizon 7.

Étape suivante

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](#).

Pour régler les paramètres de View Storage Accelerator dans Horizon 7, configurez View Storage Accelerator pour des pools de postes de travail. Reportez-vous à la section « Configurer View Storage Accelerator pour des pools de postes de travail » dans le document *Configuration des postes de travail virtuels dans Horizon 7*.

Limites d'opérations simultanées pour vCenter Server et View Composer

Lorsque vous ajoutez vCenter Server à Horizon 7 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 10-3. Limites d'opérations simultanées pour vCenter Server et View Composer

Paramètre	Description
Opérations d'approvisionnement de vCenter simultanées max.	Détermine le nombre maximal de demandes simultanées que le Serveur de connexion peut créer pour provisionner 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 le Serveur de connexion 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 . Ce paramètre s'applique à des machines virtuelles complètes et à des clones liés.
Nombre max. d'opérations de maintenance View Composer simultanées	Détermine le nombre maximal d'opérations d'actualisation, de recomposition et de rééquilibrage View Composer pouvant se dérouler simultanément sur 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 max. d'opérations d'approvisionnement 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 Horizon 7*.

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 TLS par défaut

Lorsque vous ajoutez des instances de vCenter Server et de View Composer à Horizon 7, vous devez vérifier que les certificats TLS utilisés pour les instances de vCenter Server et de View Composer sont valides et approuvés par le Serveur de connexion. 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, vous n'avez pas à accepter l'empreinte numérique 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 le Serveur de connexion 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.

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

Pour plus d'informations sur la configuration de certificats TLS, reportez-vous au [Chapitre 8 Configuration de certificats TLS pour des serveurs Horizon 7](#).

Vous ajoutez d'abord vCenter Server et View Composer dans Horizon 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.

Note 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 d'Horizon Administrator, l'icône de vCenter Server ou de View Composer devient rouge et la boîte de dialogue Certificat non valide détecté s'affiche. Dans Horizon Administrator, cliquez sur **Configuration de View > Serveurs** et modifiez l'entrée de vCenter Server associée au service View Composer. Cliquez ensuite sur **Modifier** dans les paramètres de vCenter Server et suivez les invites pour vérifier et accepter le certificat autosigné.

De la même façon, dans Horizon Administrator, vous pouvez configurer un authentificateur SAML qu'utilisera une instance du Serveur de connexion. Si le certificat de serveur SAML n'est pas approuvé par le Serveur de connexion, vous devez déterminer s'il convient ou non d'accepter l'empreinte numérique de certificat. Si vous n'acceptez pas l'empreinte, vous ne pouvez pas configurer l'authentificateur SAML dans Horizon 7. Une fois l'authentificateur SAML configuré, vous pouvez le reconfigurer dans la boîte de dialogue Modifier le Serveur de connexion.

Procédure

- 1 Lorsque Horizon 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 du Serveur de connexion ou du 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 du Serveur de connexion 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 du Serveur de connexion 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 du Serveur de connexion 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 qui se connectent à des applications et des postes de travail distants avec le protocole d'affichage VMware Blast et 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.

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, en contournant l'hôte du Serveur de connexion 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 le Serveur de connexion 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 du Serveur de connexion sur un réseau WAN, vous activez le tunnel sécurisé, PCoIP Secure Gateway et 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 du Serveur de connexion ou du serveur de sécurité, selon le type de client utilisé.

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

Configurer PCoIP Secure Gateway et les connexions par tunnel sécurisé

Vous utilisez Horizon 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 Blast Secure Gateway](#).

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 du Serveur de connexion couplée avec le serveur de sécurité.

Dans une configuration de réseau dans laquelle des clients externes se connectent directement à un hôte du Serveur de connexion, vous activez ou désactivez le tunnel sécurisé et PCoIP Secure Gateway en modifiant cette instance du Serveur de connexion dans Horizon Administrator.

Conditions préalables

- Si vous prévoyez d'activer le composant PCoIP Secure Gateway, vérifiez que l'instance du Serveur de connexion et que le serveur de sécurité couplé sont View 4.6 ou version ultérieure.
- Si vous coupez un serveur de sécurité avec une instance du Serveur de connexion sur laquelle vous avez déjà activé le composant PCoIP Secure Gateway, vérifiez que le serveur de sécurité est View 4.6 ou version ultérieure.

Procédure

- 1 Dans Horizon Administrator, sélectionnez **Configuration de View > Serveurs**.
- 2 Dans le panneau Serveurs de connexion, sélectionnez une instance du Serveur de connexion 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	Cochez la case 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 Blast Secure Gateway

Dans Horizon Administrator, vous pouvez configurer l'utilisation de Blast Secure Gateway pour offrir un accès sécurisé à des applications et des postes de travail distants, via HTML Access ou via des connexions clientes qui utilisent le protocole d'affichage VMware Blast.

Blast Secure Gateway inclut la mise en réseau Blast Extreme Adaptive Transport (BEAT), qui s'ajuste dynamiquement aux conditions du réseau, comme les vitesses variables et les pertes de paquets.

- Blast Secure Gateway prend en charge la mise en réseau BEAT uniquement lors de l'exécution sur un dispositif Unified Access Gateway.
- Les instances d'Horizon Client utilisant IPv4 et celles d'Horizon Client utilisant IPv6 peuvent être traitées simultanément sur le port TCP 8443 et sur le port UDP 8443 (pour BEAT) lorsque vous vous connectez à un dispositif Unified Access Gateway version 3.3 ou version ultérieure.
- Les instances d'Horizon Client qui utilisent une condition de réseau normale doivent se connecter à un Serveur de connexion (BSG désactivé), un serveur de sécurité (BSG désactivé) ou à des versions ultérieures à la version 2.8 d'un dispositif Unified Access Gateway. Si Horizon Client utilise une condition de réseau normale pour se connecter à un Serveur de connexion (BSG activé), à un serveur de sécurité (BSG activé) ou à des versions antérieures à la version 2.8 d'un dispositif Unified Access Gateway, le client détecte automatiquement la condition de réseau et revient à la mise en réseau TCP.
- Les instances d'Horizon Client qui utilisent une condition de réseau faible doivent se connecter à la version 2.9 ou ultérieure d'un dispositif Unified Access Gateway (avec le serveur tunnel UDP activé). Si Horizon Client utilise une condition de réseau faible pour se connecter à un Serveur de connexion (BSG activé), à un serveur de sécurité (BSG activé) ou à des versions antérieures à la version 2.8 d'un dispositif Unified Access Gateway, le client détecte automatiquement la condition de réseau et revient à la mise en réseau TCP.
- Pour les instances d'Horizon Client qui utilisent une condition de réseau faible pour se connecter à un Serveur de connexion (BSG désactivé), un serveur de sécurité (BSG désactivé), à la version 2.9 ou ultérieure d'un dispositif Unified Access Gateway (sans serveur de tunnel UDP activé) ou à la version 2.8 d'un dispositif Unified Access Gateway, le client détecte automatiquement la condition de réseau et revient à la condition de réseau normale.

Pour plus d'informations, consultez la documentation d'Horizon Client à l'adresse <https://docs.vmware.com/fr/VMware-Horizon-Client/index.html>.

Note Vous pouvez également utiliser des dispositifs Unified Access Gateway, plutôt que des serveurs de sécurité, pour un accès externe sécurisé à des serveurs et des postes de travail Horizon 7. Si vous utilisez des dispositifs Unified Access Gateway, vous devez désactiver les passerelles sécurisées sur les instances du Serveur de connexion et activer ces passerelles sur les dispositifs Unified Access Gateway. Pour plus d'informations, consultez le document *Déploiement et configuration d'Unified Access Gateway*.

Lorsque Blast Secure Gateway n'est pas activé, les périphériques clients et les navigateurs Web clients utilisent le protocole VMware Blast Extreme pour établir des connexions directes à des machines virtuelles de poste de travail distant et à des applications, en contournant 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 du Serveur de connexion couplée avec le serveur de sécurité. Si des utilisateurs externes se connectent directement à un hôte du Serveur de connexion, vous activez ou désactivez Blast Secure Gateway en modifiant cette instance du Serveur de connexion.

Conditions préalables

Si des utilisateurs sélectionnent des postes de travail distants à l'aide de VMware Identity Manager, vérifiez que VMware Identity Manager est installé et configuré pour être utilisé avec le Serveur de connexion et que ce dernier est couplé avec un serveur d'authentification SAML 2.0.

Procédure

- 1 Dans Horizon Administrator, sélectionnez **Configuration de View > Serveurs**.
- 2 Dans l'onglet **Serveurs de connexion**, sélectionnez une instance du Serveur de connexion 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 les connexions Blast à la machine
Activer Blast Secure Gateway pour HTML Access	Sélectionner Utiliser Blast Secure Gateway pour les connexions HTML Access à la machine uniquement
Désactiver Blast Secure Gateway	Sélectionner Ne pas utiliser Blast Secure Gateway

Blast Secure Gateway est activé par défaut.

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

Configuration d'URL externes pour 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 qu'il peut résoudre en adresse IP) qui permet au client d'atteindre un hôte du Serveur de connexion ou du serveur de sécurité.

Pour utiliser PCoIP Secure Gateway, un client se connecte à un hôte du Serveur de connexion ou du serveur de sécurité en utilisant une URL. Dans un environnement IPv4, l'URL doit identifier un hôte par son adresse IP. Dans un environnement IPv6, l'URL peut identifier un hôte par son adresse IP ou son nom de domaine complet.

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 ou à l'ordinateur de l'utilisateur d'atteindre un hôte du Serveur de connexion ou du serveur de sécurité.

Utilisation de connexions par tunnel à partir de sites externes

Par défaut, un hôte du Serveur de connexion 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 du Serveur de connexion 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 Horizon 7, vous devez configurer l'hôte du Serveur de connexion 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 clients qui utilisent PCoIP de réaliser des connexions sécurisées via PCoIP Secure Gateway. Dans un environnement IPv4, l'URL doit identifier un hôte par son adresse IP. Dans un environnement IPv6, l'URL peut identifier un hôte par son adresse IP ou son nom de domaine complet. L'URL permet aux clients de se connecter à partir d'un emplacement externe.

Une troisième URL permet aux utilisateurs de faire des connexions sécurisées depuis leurs périphériques clients ou 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 du Serveur de connexion couplées avec les serveurs de sécurité.

Le processus de configuration des URL externes est différent pour des instances du Serveur de connexion et des serveurs de sécurité.

- Pour une instance du Serveur de connexion, vous définissez les URL externes en modifiant des paramètres du Serveur de connexion dans Horizon Administrator.
- Pour un serveur de sécurité, vous définissez les URL externes lorsque vous exécutez le programme d'installation du Serveur de connexion. Vous pouvez utiliser Horizon Administrator pour modifier une URL externe d'un serveur de sécurité.

Définir les URL externes d'une instance du Serveur de connexion

Vous utilisez Horizon Administrator pour configurer les URL externes d'une instance du Serveur de connexion.

L'URL externe de tunnel sécurisé, l'URL externe PCoIP et l'URL externe Blast doivent être les adresses que les systèmes clients utilisent pour atteindre cette instance du Serveur de connexion.

Conditions préalables

- Vérifiez que les connexions par tunnel sécurisé et PCoIP Secure Gateway sont activés sur l'instance du Serveur de connexion. Reportez-vous à la section [Configurer PCoIP Secure Gateway et les connexions par tunnel sécurisé](#).
- Pour définir l'URL externe Blast, vérifiez que Blast Secure Gateway est activé sur l'instance du Serveur de connexion. Reportez-vous à la section [Configurer Blast Secure Gateway](#).

Procédure

- 1 Dans Horizon Administrator, cliquez sur **Configuration de View > Serveurs**.
- 2 Dans l'onglet Serveurs de connexion, sélectionnez une instance du Serveur de connexion 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**

Note Vous pouvez utiliser l'adresse IP si vous avez accès à une instance du Serveur de connexion lorsque le nom de l'hôte ne peut être résolu. Toutefois, dans ce cas, l'hôte que vous contactez ne correspond pas au certificat TLS configuré pour l'instance du Serveur de connexion, ce qui bloque l'accès ou autorise l'accès avec une sécurité limitée.

- 4 Saisissez l'URL externe de PCoIP Secure Gateway dans la zone de texte **URL externe PCoIP**.

Dans un environnement IPv4, spécifiez l'URL externe PCoIP sous la forme d'une adresse IP avec le numéro de port 4172. Dans un environnement IPv6, vous pouvez spécifier une adresse IP ou un nom de domaine complet, et le numéro de port 4172. Dans les deux cas, n'incluez pas de nom de protocole.

Par exemple, dans un environnement IPv4 : **10.20.30.40:4172**

Les clients doivent pouvoir utiliser l'URL pour accéder au 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 cet hôte du Serveur de connexion.

- 6 Vérifiez que toutes les adresses de cette boîte de dialogue permettent aux systèmes clients d'atteindre cette instance du Serveur de connexion.
- 7 Cliquez sur **OK**.

Modifier les URL externes d'un serveur de sécurité

Vous utilisez Horizon 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 du Serveur de connexion.

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.

Conditions préalables

- Vérifiez que les connexions par tunnel sécurisé et PCoIP Secure Gateway sont activés sur l'instance du Serveur de connexion qui est couplée avec ce serveur de sécurité. Reportez-vous à la section [Configurer PCoIP Secure Gateway et les connexions par tunnel sécurisé](#).
- Pour définir l'URL externe Blast, vérifiez que Blast Secure Gateway est activé sur l'instance du Serveur de connexion qui est couplée avec ce serveur de sécurité. Reportez-vous à la section [Configurer Blast Secure Gateway](#).

Procédure

- 1 Dans Horizon 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`

Note 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 TLS 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**.

Dans un environnement IPv4, spécifiez l'URL externe PCoIP sous la forme d'une adresse IP avec le numéro de port 4172. Dans un environnement IPv6, vous pouvez spécifier une adresse IP ou un nom de domaine, et le numéro de port 4172. Dans les deux cas, n'incluez pas de nom de protocole.

Par exemple, dans un environnement IPv4 : 10.20.30.40:4172

Les clients doivent pouvoir utiliser l'URL pour accéder au 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.

- 6 Vérifiez que toutes les adresses de cette boîte de dialogue permettent aux systèmes clients d'atteindre cet hôte du serveur de sécurité.

- 7 Cliquez sur **OK** pour enregistrer vos modifications.

Horizon 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.

Donner préférence aux noms DNS lorsque le Serveur de connexion Horizon renvoie des informations d'adresses

Par défaut, lors de l'envoi des adresses de machines de postes de travail et d'hôtes RDS à des clients et à des passerelles, le Serveur de connexion Horizon donne préférence aux adresses IP. Vous pouvez changer ce comportement par défaut avec un attribut LDAP Horizon 7 qui demande au Serveur de connexion Horizon de donner préférence aux noms DNS. Dans certains environnements, le renvoi de noms DNS à des clients et à des passerelles par le Serveur de connexion peut offrir une flexibilité supplémentaire dans la conception d'une infrastructure réseau.

Note Cet attribut LDAP Horizon 7 remplace la fonctionnalité par poste de travail qui est fournie par le paramètre de stratégie de groupe, `Connect using DNS Name`, dans Horizon 6.0.x et versions antérieures.

L'attribut LDAP Horizon 7 affecte les clients qui exécutent Horizon Client 3.3 pour Windows ou version ultérieure, HTML Access 3.5 ou version ultérieure et les passerelles sécurisées sur les instances du Serveur de connexion (pas les serveurs de sécurité).

Conditions préalables

Pour plus d'informations sur l'utilisation de l'utilitaire ADSI Edit sur votre version du système d'exploitation Windows Server, consultez le site Web Microsoft TechNet.

Procédure

- 1 Démarrez l'utilitaire ADSI Edit sur votre ordinateur Serveur de connexion.
- 2 Dans l'arborescence de la console, sélectionnez **Se connecter à**.
- 3 Dans la zone de texte **Sélectionnez ou entrez un nom unique ou un contexte d'attribution de noms**, tapez le nom unique **DC=vdi**, **DC=vmware**, **DC=int**.
- 4 Dans la zone de texte **Sélectionnez ou entrez un domaine ou un serveur**, sélectionnez ou tapez **localhost:389** ou le nom de domaine complet de l'ordinateur Serveur de connexion suivi du port 389.

Par exemple : `localhost:389` ou `mycomputer.mydomain.com:389`

- 5 Sur l'objet **CN=Common**, **OU=Global**, **OU=Properties**, définissez la valeur d'attribut **pae-PreferDNS** sur 1.

Lorsque cet attribut est défini sur 1, le Serveur de connexion renvoie un nom DNS, si un nom DNS est disponible et si le destinataire prend en charge la résolution de noms. Sinon, le Serveur de connexion renvoie une adresse IP, si une adresse IP de type approprié pour votre environnement (IPv4 ou IPv6) est disponible.

Lorsque cet attribut n'est pas défini ou est défini sur 0, le Serveur de connexion renvoie une adresse IP, si une adresse IP du type approprié est disponible. Sinon, une erreur de compatibilité d'adresse IP est renvoyée.

Autoriser HTML Access via un équilibrage de charge

Des instances du Serveur de connexion et des serveurs de sécurité qui se trouvent directement derrière un équilibrage de charge ou une passerelle à équilibrage de charge doivent connaître l'adresse avec laquelle les navigateurs se connectent à l'équilibrage de charge lorsque des utilisateurs utilisent HTML Access.

Pour les instances du Serveur de connexion et les serveurs de sécurité qui se trouvent directement derrière une passerelle, exécutez la procédure décrite dans la section [Autoriser HTML Access via une passerelle](#).

Vous devez exécuter cette procédure pour chaque serveur Horizon 7 se trouvant derrière l'équilibrage de charge ou la passerelle à équilibrage de charge.

Procédure

- 1 Créez ou modifiez le fichier `locked.properties` dans le dossier de configuration de la passerelle SSL sur l'hôte du Serveur de connexion ou du serveur de sécurité.

Par exemple : `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`

- 2 Ajoutez la propriété `balancedHost` et définissez-la sur l'adresse de l'équilibrage de charge.

Par exemple, si des utilisateurs tapent **`https://view.example.com`** dans un navigateur pour atteindre l'un des serveurs Horizon 7 à équilibrage de charge, ajoutez `balancedHost=view.example.com` au fichier `locked.properties`.

- 3 Enregistrez le fichier `locked.properties`.
- 4 Redémarrez le service Serveur de connexion ou le service du serveur de sécurité pour que vos modifications prennent effet.

Autoriser HTML Access via une passerelle

Des instances du Serveur de connexion et des serveurs de sécurité qui se trouvent directement derrière une passerelle, telle qu'Access Point, doivent connaître l'adresse avec laquelle les navigateurs se connectent à la passerelle lorsque des utilisateurs utilisent HTML Access.

Pour les instances du Serveur de connexion et les serveurs de sécurité qui se trouvent derrière un équilibrage de charge ou une passerelle à équilibrage de charge, exécutez la procédure décrite dans la section [Autoriser HTML Access via un équilibrage de charge](#).

Vous devez exécuter cette procédure pour chaque serveur Horizon 7 se trouvant derrière la passerelle.

Procédure

- 1 Créez ou modifiez le fichier `locked.properties` dans le dossier de configuration de la passerelle SSL sur l'hôte du Serveur de connexion ou du serveur de sécurité.

Par exemple : `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`

- 2 Ajoutez la propriété `portalHost` et définissez-la sur l'adresse de la passerelle.

Par exemple, si `https://view-gateway.example.com` est l'adresse que les navigateurs utilisent pour accéder à Horizon 7 via la passerelle, ajoutez `portalHost=view-gateway.example.com` au fichier `locked.properties`.

Si l'instance du Serveur de connexion ou le serveur de sécurité se trouve derrière plusieurs passerelles, vous pouvez spécifier chaque passerelle en ajoutant un numéro à la propriété `portalHost`, par exemple :

```
portalHost.1=view-gateway-1.example.com
portalHost.2=view-gateway-2.example.com
```

Vous devez également spécifier plusieurs propriétés `portalHost` si une machine unique de passerelle est connue sous plusieurs noms.

- 3 Enregistrez le fichier `locked.properties`.
- 4 Redémarrez le service Serveur de connexion ou le service du serveur de sécurité pour que vos modifications prennent effet.

Remplacement des ports par défaut pour les services Horizon 7

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 du Serveur de connexion, du 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 obtenir la liste des ports TCP et UDP par défaut qui sont utilisés par les serveurs Horizon 7, consultez le document *Sécurité d'Horizon 7*.

Remplacer les ports HTTP ou les cartes réseau par défaut pour des instances du Serveur de connexion Horizon et des serveurs de sécurité

Vous pouvez remplacer les ports HTTP ou les cartes réseau par défaut pour une instance du Serveur de connexion 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, Horizon 7 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](#).

Conditions préalables

Vérifiez que le port spécifié dans l'URL externe pour cette instance du Serveur de connexion 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 du Serveur de connexion 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 télécharger 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 Horizon 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 ou le service du serveur de sécurité pour que vos modifications prennent effet.

Étape suivante

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 du Serveur de connexion Horizon 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 du Serveur de connexion 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.

Conditions préalables

Vérifiez que le port spécifié dans l'URL externe PCoIP sur l'instance du Serveur de connexion 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 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 de contrôle par défaut pour PCoIP Secure Gateway sur des instances du Serveur de connexion et des serveurs de sécurité

Vous pouvez remplacer le port par défaut qui contrôle le service PCoIP Secure Gateway (PSG) exécuté sur une instance du Serveur de connexion ou sur un serveur de sécurité. Vous pouvez avoir besoin d'effectuer cette tâche pour éviter la contention du port.

PCoIP Secure Gateway écoute les connexions de contrôle sur le port TCP 50060 local par défaut.

Procédure

- 1 Créez ou modifiez le fichier `locked.properties` dans le dossier de configuration de la passerelle SSL sur l'ordinateur du Serveur de connexion ou du serveur de sécurité sur lequel est exécuté PCoIP Secure Gateway.

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 `psgControlPort` au fichier `locked.properties`.

Par exemple :

```
psgControlPort=52060
```

- 3 Démarrez l'éditeur du Registre Windows sur la même machine.
- 4 Allez à la clé de Registre `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway`.
- 5 Sous cette clé de registre, ajoutez la valeur de chaîne suivante (REG_SZ) avec votre numéro de port mis à jour.

Par exemple :

```
TCPControlPort "52060"
```

Note Le numéro de port de `TCPControlPort` est le même que celui de `psgControlPort`.

- 6 Redémarrez le service Serveur de connexion ou le service du serveur de sécurité 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.

Conditions préalables

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 Accédez au fichier exécutable SviConfig.

Le fichier est situé avec l'application View Composer. Le chemin d'accès par défaut est C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe.

- 4 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.

- 5 Redémarrez le service View Composer pour que vos modifications prennent effet.

Étape suivante

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 un serveur Horizon 7, et que vous voulez autoriser la redirection HTTP pour les clients Horizon Client qui tentent de se connecter au port 80, vous devez configurer le fichier `locked.properties` sur le serveur Horizon 7.

Note Cette procédure n'a aucun effet si vous déchargez SSL sur un périphérique intermédiaire. Avec le déchargement SSL en place, le port HTTP sur le serveur Horizon 7 fournit le service aux clients.

Conditions préalables

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 du Serveur de connexion 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 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 Horizon Client de se connecter à des serveurs Horizon 7 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 Horizon Client, vous devez configurer le fichier `locked.properties` sur le serveur Horizon 7.

Note Cette procédure n'a aucun effet si vous déchargez SSL sur un périphérique intermédiaire. Avec le déchargement SSL en place, le port HTTP sur le serveur Horizon 7 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 du Serveur de connexion 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 ou le service du serveur de sécurité pour que vos modifications prennent effet.

Activer l'accès à distance pour afficher les compteurs de performances Horizon 7 sur les serveurs de connexion

Les compteurs de performances Horizon 7 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 Horizon 7 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 le Serveur de connexion. 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 du Serveur de connexion Horizon

Sur un ordinateur Serveur de connexion, 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 le Serveur de connexion.

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 mesure 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 le Serveur de connexion avec une mémoire inférieure à 10 Go, Horizon 7 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 du Serveur de connexion 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 le Serveur de connexion pour vous assurer que la taille de segment JVM augmente automatiquement à la valeur recommandée. Vous n'avez pas besoin de réinstaller le Serveur de connexion.

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

Pour connaître la configuration matérielle et de mémoire du Serveur de connexion, reportez-vous à la section [Configuration matérielle requise du Serveur de connexion Horizon](#).

Pour obtenir des recommandations matérielles et de mémoire pour utiliser le Serveur de connexion dans un déploiement important, reportez-vous à la section « Configuration de machine virtuelle et nombre maximal dans le Serveur de connexion » du document *Planification de l'architecture Horizon 7*.

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 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 le Serveur de connexion 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

11

Vous pouvez créer une base de données des événements pour enregistrer des informations sur des événements d'Horizon 7. En outre, si vous utilisez un serveur Syslog, vous pouvez configurer le Serveur de connexion pour qu'il envoie des événements à un serveur Syslog ou créer un fichier plat d'événements écrit au format SysLog.

Ce chapitre contient les rubriques suivantes :

- [Ajouter une base de données et un utilisateur de base de données pour des événements Horizon 7](#)
- [Préparer une base de données SQL Server pour le reporting d'événements](#)
- [Configurer la base de données des événements](#)
- [Configurer la journalisation des événements pour des serveurs Syslog](#)

Ajouter une base de données et un utilisateur de base de données pour des événements Horizon 7

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.

Déployez le serveur de base de données pour la base de données d'événements sur un serveur dédié, afin que l'activité de journalisation d'événements n'ait pas d'incidence sur le provisionnement et les autres activités critiques pour les déploiements de Horizon 7.

Note Vous n'avez pas à créer une source de données ODBC pour cette base de données.

Conditions préalables

- 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 a accès. Pour voir une liste des versions de base de données prises en charge, reportez-vous à la section [Exigences de base de données pour View Composer et la base de données d'événements](#).
- 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](#)
- 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 12c ou 11g](#)

Procédure

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

Pour une base de données Oracle 12c ou 11g, fournissez également un préfixe d'Identificateur système Oracle (SID) que vous utiliserez lorsque vous configurerez la base de données des événements dans Horizon 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'incrimer 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 Horizon Administrator.

Étape suivante

Suivez les instructions de la section [Configurer la base de données des événements](#).

Préparer une base de données SQL Server pour le reporting d'événements

Avant de pouvoir utiliser Horizon 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.

Conditions préalables

- 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 Horizon 7](#).
- 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.

Étape suivante

Utilisez Horizon Administrator pour connecter la base de données au Serveur de connexion. Suivez les instructions de la section [Configurer la base de données des événements](#).

Configurer la base de données des événements

La base de données des événements stocke des informations sur des événements Horizon 7 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 du Serveur de connexion. Vous devez configurer uniquement un hôte dans un groupe du Serveur de connexion. Les hôtes restant dans le groupe sont configurés automatiquement.

Note La sécurité de la connexion de la base de données entre l'instance du Serveur de connexion 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 Horizon 7. 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.

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 d'Horizon 7*.

Vous pouvez également générer des événements Horizon 7 au format SysLog pour qu'un logiciel d'analyse tiers puisse accéder aux données d'événement. Vous utilisez la commande `vdmin` avec l'option `-I` pour enregistrer les messages d'événements d'Horizon 7 au format SysLog dans les fichiers journaux des événements. Reportez-vous à la section « Génération de messages de journal des événements Horizon 7 au format Syslog à l'aide de l'option I » dans le document *Administration d'Horizon 7*.

Conditions préalables

Vous avez besoin des informations suivantes pour configurer une base de données des événements :

- Le nom DNS ou l'adresse IP du serveur de base de données.
- Le type de serveur de base de données : Microsoft SQL Server ou Oracle.
- Le numéro de port utilisé pour accéder au serveur de base de données. Le port par défaut est 1521 pour Oracle et 1433 pour SQL Server. Pour SQL Server, si le serveur de base de données est une instance nommée, ou si vous utilisez SQL Server Express, vous devez déterminer le numéro de port. Pour plus d'informations sur la connexion à une instance nommée de SQL Server, consultez l'article de la Base de connaissances Microsoft à l'adresse <http://support.microsoft.com/kb/265808>.
- Le nom de la base de données des événements que vous avez créé sur le serveur de base de données. Reportez-vous à la section [Ajouter une base de données et un utilisateur de base de données pour des événements Horizon 7](#).

Pour une base de données Oracle 12c ou 11g, vous devez utiliser l'Identificateur du système Oracle (SID) comme nom de base de données lorsque vous configurez la base de données des événements dans Horizon 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 Horizon 7](#).

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 d'Horizon 7.

Note 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 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 Horizon 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 d'Horizon 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 d'Horizon 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 Horizon 7 au format Sys Log pour qu'un logiciel d'analyse puisse accéder aux données d'événement.

Vous devez configurer uniquement un hôte dans un groupe du Serveur de connexion. 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 Horizon 7 au format Syslog à l'aide de l'option `-I` de la commande `vdmadmin`, dans le document *Administration d'Horizon 7*.

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.

Conditions préalables

Vous avez besoin des informations suivantes pour configurer le Serveur de connexion 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 Horizon 7 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 Horizon Administrator, sélectionnez **Configuration de View > Configuration d'événements**.
- 2 (Facultatif) Dans la zone **Syslog**, pour configurer le Serveur de connexion 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 Horizon 7 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 Horizon 7 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
```