

Mises à niveau 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 © 2009–2018 VMware, Inc. Tous droits réservés. [Informations sur le copyright et les marques commerciales.](#)

Table des matières

Mises à niveau de Horizon 7	5	
1	Présentation de la mise à niveau d' Horizon 7	6
2	Application d'une branche de maintenance étendue	9
3	Mettre à niveau l'application cliente	10
4	Configuration système requise pour les mises à niveau du serveur Horizon 7	12
	Matrice de compatibilité des différentes versions des composants d' Horizon 7	12
	Exigences de View Composer	13
	Systèmes d'exploitation pris en charge pour View Composer	13
	Exigences matérielles de View Composer autonome	14
	Exigences de base de données pour View Composer et la base de données d'événements	15
	Exigences de mise à niveau pour View Composer	15
	Exigences du Serveur de connexion Horizon	16
	Configuration matérielle requise du Serveur de connexion Horizon	16
	Systèmes d'exploitation pris en charge pour le Serveur de connexion Horizon	17
	Exigences de mise à niveau du Serveur de connexion Horizon	18
	Systèmes d'exploitation pris en charge pour Horizon Agent	19
5	Mise à niveau des composants d' Horizon 7 Server	21
	Mise à niveau de View Composer	21
	Préparation de vCenter Server et de View Composer pour une mise à niveau	22
	Mise à niveau de View Composer	24
	Activer TLSv1.0 sur des connexions vCenter et ESXi depuis View Composer	25
	Activer l'authentification Digest Access pour View Composer	26
	Mise à niveau manuelle de la base de données View Composer	27
	Migrer View Composer vers une autre machine	30
	Mise à niveau du Serveur de connexion VMware Horizon	37
	Préparation du Serveur de connexion pour une mise à niveau	37
	Mise à niveau de Serveurs de connexion dans un groupe répliqué	38
	Activer TLSv1.0 sur des connexions vCenter depuis un Serveur de connexion	42
	Mise à niveau vers la version la plus récente du Serveur de connexion sur une machine différente	43
	Créer un groupe répliqué après avoir rétabli un snapshot du Serveur de connexion	44
	Mise à niveau des serveurs de sécurité	45
	Préparation du serveur de sécurité pour une mise à niveau	46

Mettre à niveau les serveurs de sécurité et leurs Serveurs de connexion couplés	46
Remplacement d'un serveur de sécurité par un dispositif Unified Access Gateway	50
Mise à niveau d'un environnement Architecture Cloud Pod	51
Mise à niveau de serveurs Horizon 7 pour autoriser HTML Access	51
Mettre à niveau vCenter Server	52
Accepter l'empreinte numérique d'un certificat TLS par défaut	53
Utilisation des fichiers de modèle d'administration de stratégie de groupe Horizon 7	55

6 Mettre à niveau des hôtes ESXi et leurs machines virtuelles 57

7 Mise à niveau des postes de travail publiés et virtuels 60

Exigences liées à la sécurité pour la mise à niveau de postes de travail	60
Mettre à niveau les hôtes RDS qui fournissent des postes de travail basés sur une session	60
Mettre à niveau View Agent ou Horizon Agent	62
Mise à niveau de pools de postes de travail View Composer	65
Mettre à niveau des pools de postes de travail d'Instant Clone	67

8 Mettre à niveau le dispositif virtuel Horizon 7 Cloud Connector 69

Dépanner la mise à niveau du dispositif virtuel Horizon 7 Cloud Connector	70
---	----

9 Tâches postérieures à la mise à niveau pour activer de nouvelles fonctionnalités dans votre configuration d'Horizon 72

Passer le mode de sécurité des messages JMS sur Amélioré	72
Tâches de mise à niveau de pools de postes de travail pour utiliser la récupération d'espace	74
Tâches de mise à niveau si vous utilisez les banques de données VMware vSAN	75
Mettre à niveau une banque de données non-vSAN vers une banque de données vSAN	75
Mettre à niveau à partir de la version 1 du format de disque vSAN	77
Mise à niveau d'Horizon View 5.3.x sur une banque de données vSAN	79
Configurer la page du portail Web de VMware Horizon pour les utilisateurs finaux	80

10 Mise à niveau séparée de composants vSphere dans un environnement Horizon 7 85

Mises à niveau de Horizon 7

Mises à niveau de Horizon 7 fournit des instructions sur la mise à niveau depuis les dernières versions de maintenance d'Horizon View 5.3, VMware Horizon™ 6 (avec View) ou VMware Horizon 6 version 6.1 ou 6.2 vers VMware Horizon 7. Vous pouvez également utiliser ce guide lorsque vous effectuez la mise à niveau vers des versions de maintenance d'Horizon 7.

Si vous effectuez également la mise à niveau de votre version de VMware vSphere®, ce guide vous indique les étapes à suivre à différents stades de la mise à niveau d'Horizon 7.

Public cible

Ce guide est destiné à toute personne devant effectuer une mise à niveau vers cette dernière version de ce produit. Les informations contenues dans ce guide sont destinées aux administrateurs Microsoft Windows ou Linux expérimentés qui connaissent bien le fonctionnement des datacenters et de la technologie des machines virtuelles.

Présentation de la mise à niveau d' Horizon 7

1

La mise à niveau du déploiement d'Horizon 7 d'entreprise implique plusieurs tâches de haut niveau. La mise à niveau est un processus à plusieurs étapes dans lequel des procédures doivent être effectuées dans un ordre particulier. Vous effectuez la mise à niveau de View Composer avant celle du Horizon Connection Server et des autres serveurs Horizon 7.

Important Avec Horizon 6 version 6.2 et ultérieures, il est possible d'installer des composants d'Horizon 7 pour qu'ils s'exécutent en mode FIPS. Horizon 7 ne prend pas en charge la mise à niveau depuis une installation non-FIPS vers une installation FIPS. Horizon ne prend pas en charge la mise à niveau depuis Horizon 6 version 6.2 en mode FIPS vers Horizon 7 en mode FIPS. Si vous devez effectuer une nouvelle installation, consultez « Installation d'Horizon 7 en mode FIPS », dans le document *Installation d'Horizon 7*.

Pendant une mise à niveau, Horizon 7 ne prend pas en charge les opérations d'approvisionnement et de maintenance de View Composer. Les opérations, telles que l'approvisionnement et la recomposition de postes de travail de clone lié, ne sont pas prises en charge pendant la période de transition lorsque des serveurs Horizon 7 continuent d'exécuter la version précédente. Vous pouvez exécuter ces opérations uniquement lorsque toutes les instances du Serveur de connexion et de View Composer ont été mises à niveau.

Vous devez effectuer le processus de mise à niveau dans un ordre spécifique. L'ordre est également important au cours de chaque étape de la mise à niveau.

Note Cette présentation concerne les mises à niveau pour des versions majeures, mineures et de maintenance.

Le nombre des tâches suivantes que vous devez effectuer dépend des composants d'Horizon 7 que vous utilisez dans votre déploiement.

- 1 Mettez à niveau le logiciel Horizon Client qui s'exécute sur des périphériques clients d'utilisateurs finaux. Reportez-vous à la section [Chapitre 3Mettre à niveau l'application cliente](#).
- 2 Sur les machines physiques ou virtuelles qui hébergent View Composer et VMware® vCenter Server™, faites des sauvegardes et arrêtez temporairement certaines tâches programmées. Reportez-vous à la section [Préparation de vCenter Server et de View Composer pour une mise à niveau](#).

Si vous disposez d'un View Composer autonome installé sur une autre machine que vCenter Server, vous devrez uniquement effectuer une sauvegarde de la base de données de View Composer et du certificat TLS/SSL de View Composer. Vous pouvez planifier une mise à niveau de vCenter Server séparément si vous souhaitez également mettre à niveau 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.

- 3 Mettez View Composer à niveau sur l'hôte existant ou migrez vers une nouvelle machine. Reportez-vous à la section [Mise à niveau de View Composer](#).
- 4 Sur les machines physiques ou virtuelles qui hébergent des instances du Serveur de connexion, faites des sauvegardes et enregistrez divers paramètres de configuration et système. Reportez-vous à la section [Préparation du Serveur de connexion pour une mise à niveau](#).

Si vous disposez de plusieurs instances du Serveur de connexion dans un groupe répliqué, effectuez des sauvegardes et notez les paramètres de configuration d'une seule instance du groupe. Pour d'autres tâches de préparation, vous pouvez effectuer les tâches pour une seule instance à la fois, juste avant d'effectuer la mise à niveau de cette instance du serveur.

- 5 Mettez à niveau des instances du Serveur de connexion qui ne sont pas couplées à des serveurs de sécurité. Reportez-vous à la section [Mise à niveau de Serveurs de connexion dans un groupe répliqué](#).

Dans un environnement de production typique composé d'au moins deux instances du Serveur de connexion renforcées par un équilibrage de charge, si vous devez limiter la durée des interruptions, vous pouvez supprimer des instances du Serveur de connexion une par une du cluster à équilibrage de charge lors de leur mise à niveau.

Important Dès qu'une instance du Serveur de connexion est mise à niveau vers la version la plus récente, vous ne pouvez plus la déclasser vers une version antérieure. Dès que toutes les instances du Serveur de connexion d'un groupe répliqué sont mises à niveau, vous ne pouvez plus ajouter une autre instance qui exécute une version antérieure.

- 6 Si vous utilisez des serveurs de sécurité, effectuez des sauvegardes et enregistrez les différentes configurations et les paramètres du système. Reportez-vous à la section [Préparation du serveur de sécurité pour une mise à niveau](#).

Pour limiter l'interruption du service, vous pouvez effectuer ces tâches pour un serveur de sécurité à la fois, juste avant d'effectuer la mise à niveau de ce serveur.

- 7 Si vous utilisez des serveurs de sécurité, mettez à niveau chaque serveur de sécurité et son instance du Serveur de connexion couplée. Si vous mettez à jour ces couples un par un, le fait de supprimer chaque serveur de sécurité du groupe équilibré en charge, de mettre à niveau le couple et d'ajouter de nouveau le serveur de sécurité au groupe permet d'éviter les interruptions de service. Reportez-vous à la section [Mettre à niveau les serveurs de sécurité et leurs Serveurs de connexion couplés](#).
- 8 Mettez à niveau les stratégies de groupe utilisées dans Active Directory. Reportez-vous à la section [Utilisation des fichiers de modèle d'administration de stratégie de groupe Horizon 7](#).

- 9 Si vous mettez également à niveau des composants VMware vSphere, mettez à niveau vCenter Server. Reportez-vous à la section [Mettre à niveau vCenter Server](#).

Durant la mise à niveau de vCenter Server, les postes de travail à distance et les sessions d'applications ne seront pas déconnectés. Les postes de travail à distance en état de provisionnement ne seront pas activés durant la mise à niveau de vCenter Server et les nouveaux postes de travail ne pourront pas être lancés. Les opérations de View Composer ne sont pas autorisées durant la mise à niveau de vCenter Server.

- 10 Si vous mettez également à niveau vSphere, mettez à niveau les hôtes VMware® ESXi™ et les machines virtuelles. Reportez-vous à la section [Chapitre 6 Mettre à niveau des hôtes ESXi et leurs machines virtuelles](#).

Les hôtes ESXi peuvent être mis à niveau sans interruption en utilisant vMotion pour déplacer les machines virtuelles vers un autre hôte du cluster, si les hôtes sont configurés dans un environnement en cluster.

- 11 Si vous utilisez actuellement des serveurs de services Terminal Server Windows comme sources de postes de travail, procédez à une mise à niveau vers Windows Server 2008 R2 ou version ultérieure et vérifiez que le rôle Hôte RDS est installé. Reportez-vous à la section [Mettre à niveau les hôtes RDS qui fournissent des postes de travail basés sur une session](#).
- 12 Mettez à niveau le logiciel Horizon™ Agent ou View Agent™ qui s'exécute sur les machines physiques ou virtuelles utilisées en tant que sources de postes de travail, en tant que postes de travail de clone complet dans un pool et en tant que postes de travail individuels dans un pool manuel. Reportez-vous à la section [Mettre à niveau View Agent ou Horizon Agent](#).
- 13 Utilisez les sources de postes de travail de machine virtuelle qui viennent d'être mises à niveau pour créer des pools de postes de travail mis à niveau. Reportez-vous à la section [Mise à niveau de pools de postes de travail View Composer](#).
- 14 Si vous utilisez la fonction Architecture Cloud Pod, consultez [Mise à niveau d'un environnement Architecture Cloud Pod](#).

Comme certaines commandes peuvent mettre à niveau plusieurs étapes simultanément, VMware vous recommande de bien comprendre les modifications irréversibles à chaque étape avant de mettre à niveau vos environnements de production.

Important VMware View® Client avec la fonctionnalité Mode local, pour l'utilisation de postes de travail hors connexion, a été supprimé et cette présentation n'inclut donc pas d'étapes de mise à niveau d'instances de Serveur de transfert View et de View Client avec Mode local. À la place de la fonctionnalité Mode local, VMware recommande d'utiliser VMware® Mirage™, qui est inclus avec VMware Horizon 6.0 et versions ultérieures. Pour plus d'informations, reportez-vous aux notes de mise à jour d'Horizon 7, accessibles à l'adresse <https://docs.vmware.com/fr/VMware-Horizon-7/index.html>.

Application d'une branche de maintenance étendue

2

Une branche de maintenance étendue (ESB) est une option disponible à partir d'Horizon 7.5, VMware App Volumes 2.14 et VMware User Environment Manager 9.4.0. Elle contient des mises à jour périodiques de Service Pack (SP), qui incluent des correctifs de bogues cumulatifs et critiques, ainsi que des correctifs de sécurité.

Si vous décidez de ne pas effectuer la mise à niveau vers la dernière version d'Horizon et de conserver la même version, vous pouvez déployer une ESB et continuer à recevoir des correctifs de bogues et de sécurité en temps voulu. Les mises à jour de SP n'incluent pas les nouvelles fonctionnalités, vous pouvez donc vous reposer sur une plate-forme Horizon stable pour vos déploiements critiques.

Des ESB distinctes sont disponibles une fois par an pour la plate-forme Horizon principale, VMware App Volumes et VMware User Environment Manager. Les ESB sont prises en charge pendant 24 mois avec trois mises à jour de SP planifiées : SP1 sera publié six mois après la version initiale, SP2 trois mois après SP1 et SP3 six mois après SP2.

Pour plus d'informations, reportez-vous à la section FAQ : Horizon 7, App Volumes, branche de maintenance étendue (ESB) UEM <https://kb.vmware.com/s/article/52845>.

Mettre à niveau l'application cliente

3

Effectuez la mise à niveau vers la dernière version d'Horizon Client et mettez à niveau le microprogramme sur les périphériques de client léger si vous les utilisez.

La fonctionnalité Mode local d'Horizon Client a été supprimée. À la place, VMware recommande d'utiliser Mirage, qui est inclus avec VMware Horizon 7. Pour plus d'informations, reportez-vous à Horizon 7 Notes de mise à jour, accessible à l'adresse <https://docs.vmware.com/fr/VMware-Horizon-7/index.html>.

Important La mise à niveau implique l'exécution de la nouvelle version du programme d'installation d'Horizon Client sans supprimer au préalable l'ancienne version de l'application cliente. Si vos utilisateurs finaux possèdent View Client 4.6.0 pour Windows ou une version antérieure, demandez-leur de supprimer le logiciel client avant de télécharger et d'exécuter le dernier programme d'installation d'Horizon Client.

Conditions préalables

- Vérifiez que vous possédez un compte d'utilisateur de domaine avec des privilèges d'administration sur les hôtes que vous allez utiliser pour exécuter le programme d'installation et réaliser la mise à niveau.
- Vérifiez que le poste de travail client, l'ordinateur portable, la tablette ou le téléphone respecte la configuration système et matérielle d'Horizon Client. Consultez le document « Utilisation d'Horizon Client » pour connaître le type spécifique de poste de travail ou de périphérique client mobile. Allez sur <https://docs.vmware.com/fr/VMware-Horizon-Client/index.html>.

Procédure

- 1 Demandez aux utilisateurs finaux d'effectuer la mise à niveau vers la version la plus récente d'Horizon Client.

Option	Action
Horizon Client	<p>Téléchargez et envoyez les programmes d'installation d'Horizon Client à vos utilisateurs finaux ou publiez-les sur un site Web et demandez aux utilisateurs finaux de télécharger le programme d'installation et de l'exécuter. Vous pouvez télécharger les programmes d'installation ou demander à vos utilisateurs de les télécharger sur le site Web VMware à l'adresse https://www.vmware.com/go/viewclients.</p> <p>Pour les clients mobiles, vous pouvez également demander aux utilisateurs finaux d'obtenir la version la plus récente d'Horizon Client sur d'autres sites Web qui vendent des applications, y compris l'App Store d'Apple, Google Play, Amazon et Windows Store.</p>
Portail Web utilisateur VMware Horizon	<p>Les utilisateurs peuvent ouvrir un navigateur et rechercher une instance du Serveur de connexion. La page Web qui s'affiche est appelée portail Web utilisateur de VMware Horizon. Elle contient des liens pour télécharger le fichier du programme d'installation d'Horizon Client.</p> <p>Note Les liens par défaut de la page Web pointent vers le site de téléchargement d'Horizon Client. Vous pouvez modifier les liens par défaut pour qu'ils pointent ailleurs. Reportez-vous à la section Configurer la page du portail Web de VMware Horizon pour les utilisateurs finaux.</p>
Client léger	<p>Mettez à niveau le microprogramme de client léger et installez le nouveau logiciel Horizon Client sur les périphériques client des utilisateurs finaux. Les clients légers et les clients zéro sont fournis par des partenaires VMware.</p>

- 2 Demandez aux utilisateurs finaux de vérifier s'ils peuvent ouvrir une session et se connecter à leurs postes de travail distants.

Configuration système requise pour les mises à niveau du serveur Horizon 7

4

Les hôtes et les machines virtuelles dans un déploiement Horizon 7 doivent répondre aux exigences matérielles et de système d'exploitation spécifiques.

Ce chapitre contient les rubriques suivantes :

- [Matrice de compatibilité des différentes versions des composants d'Horizon 7](#)
- [Exigences de View Composer](#)
- [Exigences du Serveur de connexion Horizon](#)
- [Systèmes d'exploitation pris en charge pour Horizon Agent](#)

Matrice de compatibilité des différentes versions des composants d' Horizon 7

Comme les grandes entreprises doivent souvent effectuer des mises à niveau graduelles, les composants sont conçus pour être plutôt à compatibilité ascendante et descendante, au moins lors des mises à niveau.

Les versions suivantes sont prises en charge pour la mise à niveau vers Horizon 7 :

- Dernière version de maintenance d'Horizon View 5.3
- Dernière version de maintenance de VMware Horizon 6.0 (avec View)
- Dernière version de maintenance de VMware Horizon 6 version 6.1
- Dernière version de maintenance de VMware Horizon 6 version 6.2

Pour déterminer la dernière version de maintenance d'un composant particulier, consultez les notes de mise à jour de cette version, disponibles à l'adresse <https://docs.vmware.com/en/VMware-Horizon-7/index.html>

La compatibilité du Serveur de connexion Horizon avec Horizon Agent est limitée à l'interopérabilité lors d'une mise à niveau du Serveur de connexion. Vous devez mettre les instances de View Agent ou de Horizon Agent à niveau dès que possible pour qu'elles correspondent à la version du Serveur de connexion qui les gère.

Le tableau suivant répertorie les composants et indique s'ils sont compatibles avec d'autres composants dont la version est différente.

Tableau 4-1. Matrice de compatibilité pour VMware Horizon 7 et les versions antérieures des composants View

	Serveur de connexion : version antérieure	Serveur de sécurité : version antérieure	View Composer : version antérieure	View Agent : version antérieure	Horizon Client (Windows) : version antérieure
Serveur de connexion 7.0	Uniquement lors des mises à niveau	Uniquement si couplé avant la mise à niveau	Non	Uniquement lors des mises à niveau	Oui
Serveur de sécurité 7.0 (PCoIP et RDP)	Non	S/O	Non	Uniquement lors des mises à niveau	Oui
View Composer 7.0	Uniquement lors des mises à niveau	Uniquement lors des mises à niveau	S/O	Uniquement lors des mises à niveau	S/O
Horizon Agent 7.0	Uniquement pendant la mise à niveau (reportez-vous à l'exception de la note figurant après ce tableau)	Non	Non	S/O	Uniquement lors des mises à niveau
Horizon Client 4.0	Oui	Oui	Oui	Oui	S/O



Attention Pendant une mise à niveau, les opérations de provisionnement et de maintenance de View Composer ne sont pas prises en charge. Les opérations, telles que l'approvisionnement et la recomposition de postes de travail de clone lié, ne sont pas prises en charge pendant la période de transition lorsque des serveurs Horizon 7 continuent d'exécuter la version précédente. Vous pouvez exécuter ces opérations uniquement lorsque toutes les instances du Serveur de connexion et de View Composer ont été mises à niveau vers la dernière version.

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 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.

Tableau 4-2. 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 4-3. 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**.

Exigences de mise à niveau pour View Composer

Le processus de mise à niveau de View Composer a des exigences et des limitations spécifiques.

Pour exécuter le programme d'installation de View Composer, vous devez être un utilisateur de domaine avec des privilèges d'administrateur sur le système.

Exigences liées à la sécurité

- View Composer requiert un certificat TLS signé par une autorité de certification. 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.

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

Pour plus d'informations sur les exigences des certificats de sécurité, consultez la section « Configuration de certificats SSL pour View Server » dans le document *Installation de Horizon 7*.

- Les certificats pour les serveurs vCenter Server, View Composer et Horizon 7 doivent inclure des listes de révocation de certificat (CRL). Pour plus d'informations, consultez la section « Configuration de la vérification de révocation de certificat sur des certificats de serveur » dans le document *Installation de Horizon 7*.
- Vérifiez qu'aucune application exécutée sur l'ordinateur View Composer n'utilise de bibliothèques Windows SSL qui requièrent SSLv2 fourni 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. SSLv3, TLSv1.0 et RC4 sont également désactivés par défaut. Pour plus d'informations, consultez la section « Protocoles et chiffrements anciens désactivés dans View » dans le document *Sécurité d'Horizon 7*.
- Pour améliorer la sécurité de View Composer, désactivez les suites de chiffrement faible sur l'ordinateur Windows Server sur lequel le service View Composer est installé. Reportez-vous à la section « Désactiver des chiffrements faibles dans les protocoles SSL/TLS » dans le document *Installation d'Horizon 7*.
- Vous devrez peut-être apporter des modifications à la configuration du protocole de sécurité pour qu'il continue à être compatible avec vSphere. Si possible, appliquez des correctifs à ESXi et à vCenter Server pour prendre en charge TLSv1.1 et TLSv1.2 avant la mise à niveau de View Composer. Si vous ne pouvez pas appliquer de correctifs, réactivez TLSv1.0 sur View Composer avant la mise à niveau. Pour plus d'informations, reportez-vous à la section [Activer TLSv1.0 sur des connexions vCenter et ESXi depuis View Composer](#).
- À partir d'Horizon 7 version 7.0.3, vous pouvez activer l'authentification Digest Access pour View Composer afin d'améliorer la sécurité. Pour plus d'informations, reportez-vous à la section [Activer l'authentification Digest Access pour 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.

Tableau 4-4. 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 4-5. 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 de mise à niveau du Serveur de connexion Horizon

Le processus de mise à niveau du Serveur de connexion Horizon a des exigences et des limites spécifiques.

- Le Serveur de connexion nécessite une clé de licence valide pour cette version la plus récente.
- Le compte d'utilisateur de domaine que vous utilisez pour installer la nouvelle version du Serveur de connexion doit disposer de privilèges administratifs sur l'hôte du Serveur de connexion.
L'administrateur du Serveur de connexion doit disposer d'informations d'identification administratives pour vCenter Server.
- Lorsque vous exécutez le programme d'installation, vous autorisez un compte d'administrateur. 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 Horizon 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.
- 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.

Exigences liées à la sécurité

- Le Serveur de connexion requiert un certificat TLS signé par une autorité de certification et que vos clients peuvent valider. Bien qu'un certificat auto-signé par défaut soit généré en l'absence de certificat signé par une autorité de certification lorsque vous installez le Serveur de connexion, vous devez remplacer le certificat auto-signé par défaut dès que possible. Les certificats auto-signés sont affichés comme étant non valides dans Horizon Administrator.

En outre, les clients mis à jour attendent des informations sur le certificat du serveur à communiquer dans le cadre de négociation TLS entre client et serveur. Souvent, les clients mis à jour n'approuvent pas les certificats auto-signés.

Pour plus d'informations sur les exigences des certificats de sécurité, consultez la section « Configuration de certificats TLS pour les serveurs Horizon 7 » dans le guide *Installation d'Horizon 7*. Consultez également le document *Scénarios de configuration des certificats TLS pour Horizon 7* qui décrit la configuration des serveurs intermédiaires qui effectuent des tâches telles que l'équilibrage de charge et le déchargement des connexions SSL.

Note Si vos serveurs d'origine disposent déjà de certificats TLS signés par une autorité de certification, lors de la mise à niveau, Horizon 7 importe votre certificat signé par une autorité de certification existant dans le magasin de certificats Windows Server.

- Les certificats de vCenter Server, View Composer et Horizon 7 doivent inclure des listes de révocation de certificat (CRL). Pour plus d'informations, consultez « Configuration de la vérification de révocation de certificat sur des certificats de serveur » dans le document *Installation d'Horizon 7*.

Important Si votre entreprise utilise des paramètres proxy pour l'accès Internet, vous devrez peut-être configurer vos hôtes du Serveur de connexion pour qu'ils utilisent le proxy. Cette étape garantit que les serveurs peuvent accéder à des sites de vérification de la révocation des certificats sur Internet. Vous pouvez utiliser les commandes Netshell de Microsoft pour importer les paramètres proxy dans le Serveur de connexion. Pour plus d'informations, reportez-vous à la section « Troubleshooting Horizon 7 Server Certificate Revocation Checking (Dépannage de la vérification de la révocation des certificats du serveur Horizon 7) » dans le document *Administration d'Horizon 7*.

- 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 de réseau inclut un pare-feu entre un serveur de sécurité et une instance du Serveur de connexion, vous devez configurer le pare-feu pour qu'il prenne en charge IPsec. Reportez-vous au document *Installation d'Horizon 7*.
- Vous devrez peut-être apporter des modifications à la configuration du protocole de sécurité pour qu'il continue à être compatible avec vSphere. Si possible, appliquez des correctifs à ESXi et à vCenter Server pour prendre en charge TLSv1.1 et TLSv1.2 avant la mise à niveau du Serveur de connexion. Si vous ne pouvez pas appliquer de correctifs, réactivez TLSv1.0 sur le Serveur de connexion avant la mise à niveau. Pour plus d'informations, reportez-vous à la section [Activer TLSv1.0 sur des connexions vCenter depuis un Serveur de connexion](#).
- Si vous utilisez des serveurs Horizon 7 avec une version de View Agent antérieure à 6.2, vous devrez activer TLSv1.0 pour les connexions PCoIP. Les versions de View Agent antérieures à 6.2 ne prennent en charge le protocole de sécurité TLSv1.0 que pour PCoIP. TLSv1.0 est désactivé par défaut sur les serveurs Horizon 7, y compris les Serveurs de connexion et les serveurs de sécurité. Vous pouvez activer TLSv1.0 pour les connexions PCoIP sur ces serveurs en suivant les instructions dans la base de connaissances de VMware, à l'adresse <http://kb.vmware.com/kb/2130798>.

Si vous prévoyez d'exécuter de nouvelles installations d'instances du Serveur de connexion sur des machines physiques ou virtuelles supplémentaires, consultez la liste complète des exigences d'installation dans le document *Installation d'Horizon 7*.

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 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, consultez la rubrique sur la désactivation des chiffrements faibles pour View Composer ou Horizon Agent dans le document *Installation d'Horizon 7*.

Mise à niveau des composants d' Horizon 7 Server

5

Les composants de serveur que vous devez mettre à niveau comprennent le Horizon Connection Server, des serveurs répliqués et des serveurs de sécurité. En fonction des composants facultatifs que vous utilisez, vous devez également mettre à niveau View Composer.

Si vous diffusez les tâches de mise à niveau sur plusieurs périodes de maintenance, vous pouvez vérifier si chaque phase du processus a réussi ou a rencontré des problèmes. VMware vous recommande de mettre à niveau tous les composants de serveur lors de la première fenêtre de maintenance.

Ce chapitre contient les rubriques suivantes :

- [Mise à niveau de View Composer](#)
- [Mise à niveau du Serveur de connexion VMware Horizon](#)
- [Mise à niveau des serveurs de sécurité](#)
- [Mise à niveau d'un environnement Architecture Cloud Pod](#)
- [Mise à niveau de serveurs Horizon 7 pour autoriser HTML Access](#)
- [Mettre à niveau vCenter Server](#)
- [Accepter l'empreinte numérique d'un certificat TLS par défaut](#)
- [Utilisation des fichiers de modèle d'administration de stratégie de groupe Horizon 7](#)

Mise à niveau de View Composer

Pendant une mise à niveau, Horizon 7 ne prend pas en charge les opérations d'approvisionnement et de maintenance de View Composer. Les opérations, telles que l'approvisionnement et la recomposition de postes de travail de clone lié, ne sont pas prises en charge pendant la période de transition lorsque des serveurs Horizon 7 continuent d'exécuter la version précédente. Vous pouvez exécuter ces opérations uniquement lorsque toutes les instances du Horizon Connection Server et de View Composer ont été mises à niveau.

Note Avant de pouvoir utiliser la fonctionnalité de View Composer 6.2 pour créer des batteries automatisées d'hôtes RDS de clone lié, vous devez mettre à niveau tous les composants d'Horizon vers Horizon 6 version 6.2 ou ultérieure.

Préparation de vCenter Server et de View Composer pour une mise à niveau

Étant donné que vCenter Server et View Composer sont souvent installés sur une même machine virtuelle ou physique, certaines tâches de préparation s'appliquent aux deux.

Préparation de mises à niveau incluant vSphere

Si vous mettez à niveau vCenter Server et procédez à une mise à niveau vers la version d'Horizon 7 la plus récente, consultez le *Guide de mise à niveau de VMware vSphere* et effectuez les tâches ci-dessous dans l'ordre suivant :

- 1 Vérifiez que la machine virtuelle ou physique satisfait les exigences système de la version de vCenter Server vers laquelle vous voulez effectuer la mise à niveau.
- 2 Vérifiez que la machine virtuelle ou physique sur laquelle l'instance actuelle de View Composer est installée satisfait les exigences de sécurité de la nouvelle version.

Reportez-vous à la section [Exigences de mise à niveau pour View Composer](#).
- 3 Si vCenter Server est installé sur une machine virtuelle, prenez un snapshot de la machine virtuelle.

Pour obtenir des instructions sur la prise de snapshots, reportez-vous à l'aide en ligne de vSphere Client™.
- 4 Si le nom de l'ordinateur comporte plus de 15 caractères, raccourcissez-le à 15 caractères ou moins.
- 5 Sauvegardez les bases de données vCenter Server et View Composer.

Pour plus d'instructions sur l'exécution d'une sauvegarde de base de données, consultez la documentation de votre fournisseur de base de données.
- 6 Vérifiez que le serveur de base de données est compatible avec la version de vCenter Server que vous prévoyez d'utiliser.

Par exemple, si le serveur de base de données est Oracle 9i, vous devez effectuer la mise à niveau.
- 7 Vérifiez que la base de données est compatible avec la nouvelle version de View Composer.

View Composer prend en charge un sous-ensemble des serveurs de base de données compatibles avec vCenter Server. Si vous utilisez déjà vCenter Server avec un serveur de base de données qui n'est pas pris en charge par View Composer, continuez à utiliser ce serveur de base de données pour vCenter Server et installez un serveur de base de données distinct à utiliser pour les événements des bases de données View Composer et Horizon 7.
- 8 Faites une copie du dossier qui contient des certificats TLS.

Ce dossier est situé dans %ALLUSERSPROFILE%\Application Data\VMware\VMware VirtualCenter.
- 9 Renseignez l'adresse IP et le nom du système de la machine sur laquelle vCenter Server est installé.
- 10 Pour tous les pools de postes de travail de clone lié et d'Instant Clone, utilisez Horizon Administrator pour désactiver le provisionnement des nouvelles machines virtuelles.

Pour les clones liés, comme View Composer peut être mis à niveau au cours d'une période de maintenance différente de celle de ses pools de postes de travail, le provisionnement doit être reporté jusqu'à ce que les deux composants soient mis à niveau.

- 11 Si des pools de postes de travail de clone lié ou d'Instant Clone sont définis pour actualiser le disque du système d'exploitation à la fermeture de session, utilisez Horizon Administrator pour modifier le paramètre **Postes de travail/Pools** pour ce pool et définissez **Supprimer ou actualiser la machine à la fermeture de session** sur **Jamais**.

Pour les clones liés, ce paramètre évite qu'une erreur se produise lorsque View Composer récemment mis à jour tente d'actualiser un poste de travail sur lequel Horizon Agent n'a pas encore été mis à niveau.

- 12 Si des pools de postes de travail de clone lié ou d'Instant Clone sont programmés pour une opération d'actualisation, de recomposition ou de transfert d'image, Horizon Administrator permet d'annuler ces tâches.

Préparation de mises à niveau de View Composer uniquement

Si vous mettez à niveau uniquement View Composer, et non vCenter Server, vous devez exécuter les tâches suivantes :

- 1 Vérifiez que la machine virtuelle ou physique sur laquelle l'instance actuelle de View Composer est installée satisfait les exigences de sécurité de la nouvelle version.

Reportez-vous à la section [Exigences de mise à niveau pour View Composer](#).

- 2 Si View Composer est installé sur une machine virtuelle, prenez un snapshot de la machine virtuelle. Pour plus d'instructions sur la prise de snapshots, consultez l'aide en ligne de vSphere Client.

- 3 Sauvegardez la base de données View Composer.

Pour plus d'instructions sur l'exécution d'une sauvegarde de base de données, consultez la documentation de votre fournisseur de base de données.

- 4 Vérifiez que la base de données est compatible avec la nouvelle version de View Composer.

View Composer prend en charge un sous-ensemble des serveurs de base de données compatibles avec vCenter Server. Si vous utilisez déjà vCenter Server avec un serveur de base de données qui n'est pas pris en charge par View Composer, continuez à utiliser ce serveur de base de données pour vCenter Server et installez un serveur de base de données distinct à utiliser pour les événements des bases de données View Composer et Horizon 7.

- 5 Renseignez l'adresse IP et le nom du système de la machine sur laquelle vCenter Server est installé.
- 6 Pour tous les pools de postes de travail de clone lié, utilisez Horizon Administrator pour désactiver le provisionnement des nouvelles machines virtuelles.

Comme View Composer peut être mis à niveau au cours d'une période de maintenance différente de celle de ses pools de postes de travail, le provisionnement doit être reporté jusqu'à ce que les deux composants soient mis à niveau.

- 7 Si des pools de poste de travail sont définis pour actualiser le disque du système d'exploitation à la fermeture de session, utilisez Horizon Administrator pour modifier les paramètres de **Postes de travail/Pools** pour ce pool et définissez **Supprimer ou actualiser la machine à la fermeture de session** sur **Jamais**.

Ce paramètre évite qu'une erreur se produise lorsque View Composer récemment mis à jour tente d'actualiser un poste de travail sur lequel View Agent n'a pas encore été mis à niveau.

- 8 Si un pool de postes de travail est programmé pour une opération d'actualisation ou de recomposition, utilisez Horizon Administrator pour annuler ces tâches.

Mise à niveau de View Composer

Au cours de la première fenêtre de maintenance, vous allez mettre à niveau View Composer. Des opérations, telles que l'approvisionnement et la recomposition de postes de travail de clone lié, ne sont pas prises en charge tant que tous les serveurs Horizon 7 ne sont pas mis à niveau.

Conditions préalables

- Déterminez quand effectuer cette procédure. Choisissez une période de maintenance de poste de travail disponible. Prévoyez 15 à 30 minutes.
- Effectuez les tâches répertoriées dans la section [Préparation de mises à niveau de View Composer uniquement](#)
- Vérifiez que le serveur sur lequel View Composer est installé possède un certificat de serveur TLS/SSL signé par une autorité de certification installé et configuré. Après la mise à niveau du Horizon Connection Server, si View Composer n'utilise pas de certificat signé par une autorité de certification, le certificat autosigné par défaut est affiché comme étant non valide dans Horizon Administrator.
- Vérifiez que vous possédez un compte d'utilisateur de domaine avec des privilèges d'administration sur les hôtes que vous allez utiliser pour exécuter le programme d'installation et réaliser la mise à niveau.
- Déterminez si vous souhaitez laisser l'assistant du programme d'installation mettre à niveau la base de données View Composer si une mise à niveau du schéma est requise. Vous pouvez choisir d'exécuter l'utilitaire de ligne de commande SviConfig lorsque l'assistant a terminé la mise à niveau manuelle du schéma de la base de données et la création d'un journal de la mise à niveau.

Procédure

- 1 Sur les machines virtuelles ou physiques sur lesquelles View Composer est installé, téléchargez et exécutez le programme d'installation de View Composer.

Vous pouvez télécharger le programme d'installation sur le site Web de VMware.

Des instructions pas à pas d'exécution du programme d'installation figurent dans le document *Installation de Horizon 7*.

- 2 Spécifiez si vous souhaitez que l'assistant mette à niveau le schéma de la base de données si une mise à niveau de schéma est requise.

Si une boîte de dialogue apparaît avec le message "Database upgrade completed with warnings" ("Mise à niveau de la base de données terminée avec des avertissements"), vous pouvez cliquer sur **OK** et ignorer le message en toute sécurité.

- 3 Lorsque l'assistant vous invite à fournir le numéro de port de View Composer, vérifiez que le numéro de port est défini sur 18443.

Étape suivante

Si vous devez effectuer une mise à niveau manuelle du schéma de la base de données, reportez-vous à [Exécution de SviConfig pour mettre à niveau manuellement la base de données](#).

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](#).

Lors de la fenêtre de maintenance suivante, continuez la mise à niveau d'Horizon 7. Reportez-vous à la section [Mise à niveau de Serveurs de connexion dans un groupe répliqué](#).

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.

Activer l'authentification Digest Access pour View Composer

À partir d'Horizon 7 version 7.0.3, la méthode d'authentification d'accès de base pour la sécurité Web est activée par défaut dans View Composer. Pour une sécurité améliorée, vous pouvez activer la méthode d'authentification Digest Access pour View Composer.

Conditions préalables

- Vérifiez que View Composer 7.0.3 ou une version ultérieure est installé.
- Vérifiez que vous pouvez ouvrir une session sur la machine View Composer en tant qu'administrateur.
- Vérifiez que le Serveur de connexion 7.0.3 ou une version ultérieure est installé.

Procédure

- 1 Accédez au répertoire dans lequel View Composer est installé.
- 2 Modifiez le fichier SviWebService.exe.config.
- 3 Pour l'option de configuration SslPoxBinding, définissez authenticationScheme="Digest".
- 4 Pour l'option de configuration SslBasicAuth, définissez clientCredentialType="Digest".
- 5 Enregistrez et fermez le fichier SviWebService.exe.config.
- 6 Modifiez le fichier SviConfig.exe.config.
- 7 Pour l'option de configuration SslSviBinding, définissez clientCredentialType="Digest".

- 8 Enregistrez et fermez le fichier SviConfig.exe.config.
- 9 Redémarrez le service View Composer.
 - a Démarrez l'outil Windows Services en saisissant `services.msc` à l'invite de commande.
 - b Dans la liste de services, cliquez avec le bouton droit sur le service que vous voulez redémarrer. Par exemple, cliquez avec le bouton droit sur VMware Horizon Composer 7.0.3.
 - c Cliquez sur **Redémarrer**.

Mise à niveau manuelle de la base de données View Composer

Plutôt que de laisser le programme d'installation de View Composer mettre à niveau la base de données quand une mise à jour de schéma est requise, vous pouvez mettre à niveau manuellement la base de données. Vous pouvez utiliser l'utilitaire SviConfig lorsque vous devez observer le processus de mise à niveau plus attentivement ou lorsque des tâches de mise à niveau doivent être distribuées aux administrateurs informatiques avec différentes responsabilités.

Lorsque vous mettez à niveau View Composer vers une version avec un schéma de base de données mis à niveau, une invite du programme d'installation vous demande si vous souhaitez que l'assistant mette à niveau la base de données. Si vous choisissez de ne pas utiliser l'assistant du programme d'installation, vous devez utiliser l'utilitaire SviConfig pour mettre à niveau la base de données et migrer les données existantes.

L'utilisation de l'utilitaire de ligne de commande SviConfig a les avantages suivants :

- Cet utilitaire renvoie des codes de résultat et crée un journal de la mise à niveau de la base de données pour simplifier le dépannage si la mise à niveau échoue.
- Vous pouvez séparer les tâches de mise à niveau. Un administrateur de vSphere ou de Horizon 7 peut exécuter le programme d'installation de View Composer pour mettre à niveau le logiciel. Un administrateur de base de données peut utiliser SviConfig pour mettre à niveau la base de données View Composer.
- La mise à niveau logicielle et la mise à niveau de base de données peuvent se produire lors de différentes périodes de maintenance. Par exemple, votre site peut exécuter des opérations de maintenance de base de données uniquement les week-ends, alors que des tâches de maintenance logicielle peuvent se produire au cours de la semaine.

Exécution de SviConfig pour mettre à niveau manuellement la base de données

Avec l'utilitaire de ligne de commande SviConfig, vous pouvez mettre à niveau la base de données View Composer séparément à partir du logiciel View Composer. Cet utilitaire crée également un fichier journal pour simplifier le dépannage si la mise à niveau échoue.

Important Seuls les administrateurs View Composer expérimentés doivent utiliser l'utilitaire SviConfig. Cet utilitaire est conçu pour résoudre des problèmes liés au service View Composer.

Conditions préalables

- Sauvegardez la base de données View Composer. Pour plus d'instructions, consultez la documentation pour votre serveur de base de données.
- Vérifiez que vous connaissez le nom de source de base de données (DSN) de la base de données View Composer.
- Vérifiez que vous connaissez le nom d'utilisateur et le mot de passe du compte d'administrateur de base de données pour cette base de données.

Procédure

- 1 Sur la machine virtuelle ou physique vCenter Server, ouvrez une invite de commande Windows et naviguez vers le fichier exécutable SviConfig.

Le fichier est situé avec l'application View Composer. Le chemin d'accès par défaut est C:\Program Files (86)\VMware\VMware View Composer\sviconfig.exe.

- 2 Entrez la commande pour arrêter VMware View Composer.

net stop svid

- 3 Exécutez la commande SviConfig databaseupgrade.

```
sviconfig -operation=databaseupgrade
          -DsnName=target_DSN
          -Username=database_administrator_username
```

Par exemple :

```
sviconfig -operation=databaseupgrade -dsname=LinkedClone
          -username=Admin
```

- 4 Lorsqu'un message vous y invite, fournissez le mot de passe.

Une opération réussie affiche des informations montrant les étapes de mise à niveau.

```
Establishing database connection.
Database connection established successfully.
Upgrading database.
Load data from SVI_VC_CONFIG_ENTRY table.
Update SVI_DEPLOYMENT_GROUP table.
Update SVI_REPLICA table.
Update SVI_SIM_CLONE table.
SviConfig finished successfully.
Database is upgraded successfully.
```

- 5 Entrez la commande de démarrage de View Composer.

net start svid

Un journal complet du processus de mise à niveau est créé et placé dans C:\Users\All Users\VMware\View Composer\vmware-sviconfig.log.

Étape suivante

Si la mise à niveau de la base de données échoue, reportez-vous à [Dépannage d'un échec de mise à niveau de la base de données View Composer](#).

Si le code de résultat est différent de 0, ce qui indique une réussite, reportez-vous à la section [Codes de résultat pour une mise à jour manuelle du schéma de base de données](#)

Codes de résultat pour une mise à jour manuelle du schéma de base de données

Lorsque vous mettez à niveau manuellement la base de données View Composer, la commande `sviconfig databaseupgrade` affiche un code de résultat.

[Tableau 5-1](#) indique les codes de résultat `sviconfig databaseupgrade`.

Tableau 5-1. Codes de résultat pour la commande `databaseupgrade`

Code	Description
0	L'opération s'est terminée avec succès.
1	Le DSN fourni est introuvable.
2	Des informations d'identification d'administrateur de base de données non valides ont été fournies.
3	Le pilote pour la base de données n'est pas pris en charge.
4	Un problème inattendu s'est produit et la commande n'a pas pu se terminer.
14	Une autre application utilise le service View Composer. Arrêtez le service avant d'exécuter la commande.
15	Un problème s'est produit au cours du processus de restauration. Des détails sont fournis dans la sortie du journal à l'écran.
17	Impossible de mettre à niveau les données de la base de données.
18	Impossible de se connecter au serveur de base de données.

Dépannage d'un échec de mise à niveau de la base de données View Composer

Lorsque vous effectuez la mise à niveau du service View Composer avec le programme d'installation de View Composer ou que vous exécutez la commande `SviConfig databaseupgrade`, l'opération peut ne pas réussir à mettre à niveau la base de données View Composer.

Problème

L'opération `SviConfig databaseupgrade` affiche le code d'erreur 17 ou le programme d'installation de View Composer affiche un message d'avertissement.

```
Database upgrade completed with warnings
```

Cause

Le logiciel de mise à niveau de la base de données contacte vCenter Server pour obtenir des données supplémentaires sur les postes de travail. La mise à niveau de la base de données peut échouer si les postes de travail ne sont pas disponibles, si l'hôte ESXi n'est pas en cours d'exécution ou si vCenter Server n'est pas disponible.

Solution

- 1 Pour plus d'informations, consultez le fichier journal SviConfig de View Composer.

L'emplacement par défaut de ce fichier est C:\Users\All Users\VMware\View Composer\vmware-sviconfig.log. Le script de mise à niveau journalise un message pour chaque échec.

- 2 Examinez les enregistrements du journal pour identifier les postes de travail qui n'ont pas pu se mettre à niveau.

Option	Action
Le poste de travail existe mais n'est pas disponible.	Rendez le poste de travail de nouveau disponible. En fonction de la cause de l'échec, vous pouvez avoir à redémarrer l'hôte ESXi ou vCenter Server ou à exécuter une autre action.
Le poste de travail n'existe pas.	Ignorez le message de journal. Note Un poste de travail supprimé peut sembler exister dans Horizon Administrator si un administrateur supprime la machine virtuelle de poste de travail directement dans vSphere.

- 3 Exécutez de nouveau la commande SviConfig databaseupgrade.

Migrer View Composer vers une autre machine

Dans certains cas, il peut être nécessaire de migrer un service VMware Horizon View Composer vers une nouvelle machine virtuelle ou physique Windows Server. Par exemple, vous pouvez migrer View Composer et vCenter Server vers un nouvel hôte ESXi ou un cluster pour développer votre déploiement de Horizon 7. En outre, il est inutile d'installer View Composer et vCenter Server sur la même machine Windows Server.

Vous pouvez migrer View Composer depuis la machine vCenter Server vers une machine autonome ou depuis une machine autonome vers la machine vCenter Server.

Important Ces rubriques concernent la migration de la version la plus récente de View Composer vers une autre machine. Vous devez procéder à une mise à niveau à partir de la version antérieure de View Composer avant d'effectuer ces tâches.

Si votre version actuelle de View Composer est installée sur une machine qui ne répond pas à la configuration système de la nouvelle version de View Composer, vous ne pouvez pas utiliser ces procédures. Après avoir migré View Composer vers un système disposant d'un système d'exploitation Windows Server qui est pris en charge pour cette version, vous pouvez effectuer une mise à niveau sur place vers la dernière version de View Composer.

- **Conseils sur la migration de View Composer**

Les étapes requises pour migrer le service VMware Horizon View Composer varient selon que vous souhaitez ou non conserver les machines virtuelles de clone lié existantes.

- **Migrer View Composer avec une base de données existante**

Lorsque vous migrez View Composer vers une autre machine physique ou virtuelle, si vous prévoyez de conserver vos machines virtuelles de clone lié actuelles, le nouveau service VMware Horizon View Composer doit continuer à utiliser la base de données View Composer existante.

- **Migrer View Composer sans machines virtuelles de clone lié**

Si le service VMware Horizon View Composer actuel ne gère aucune machine virtuelle de clone lié, vous pouvez migrer View Composer vers une nouvelle machine physique ou virtuelle sans migrer les clés RSA vers la nouvelle machine. Le service VMware Horizon View Composer migré peut se connecter à la base de données View Composer d'origine ou vous pouvez préparer une nouvelle base de données pour View Composer.

- **Préparer Microsoft .NET Framework pour la migration de clés RSA**

Pour utiliser une base de données View Composer existante, vous devez migrer le conteneur de clés RSA entre les machines. Vous migrez le conteneur de clés RSA à l'aide de l'outil d'inscription ASP.NET IIS fourni avec Microsoft .NET Framework.

- **Migrer le conteneur de clés RSA vers le nouveau service View Composer**

Pour utiliser une base de données View Composer existante, vous devez migrer le conteneur de clés RSA de la machine physique ou virtuelle source sur laquelle le service VMware Horizon View Composer existant réside vers la machine sur laquelle vous souhaitez installer le nouveau service VMware Horizon View Composer.

Conseils sur la migration de View Composer

Les étapes requises pour migrer le service VMware Horizon View Composer varient selon que vous souhaitez ou non conserver les machines virtuelles de clone lié existantes.

Pour conserver les machines virtuelles de clone lié dans votre déploiement, le service VMware Horizon View Composer que vous installez sur la nouvelle machine virtuelle ou physique doit continuer à utiliser la base de données View Composer existante. La base de données View Composer contient les données requises pour créer, approvisionner, maintenir et supprimer les clones liés.

Lorsque vous migrez le service VMware Horizon View Composer, vous pouvez également migrer la base de données View Composer vers une nouvelle machine.

Que vous procédiez ou non à la migration de la base de données View Composer, la base de donnée doit être configurée sur une machine disponible dans le même domaine que la nouvelle machine sur laquelle vous installez le service VMware Horizon View Composer ou sur un domaine approuvé.

View Composer crée des paires de clés RSA pour crypter et décrypter des informations d'authentification stockées dans la base de données View Composer. Pour rendre cette source de données compatible avec le nouveau service VMware Horizon View Composer, vous devez migrer le conteneur de clés RSA créé par le service VMware Horizon View Composer d'origine. Vous devez importer le conteneur de clés RSA sur la machine sur laquelle vous installez le nouveau service.

Si le service VMware Horizon View Composer actuel ne gère pas de machines virtuelles de clone lié, vous pouvez migrer le service sans utiliser la base de données View Composer existante. Il n'est pas nécessaire de migrer les clés RSA, que vous utilisiez ou non la base de données existante.

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

Migrer View Composer avec une base de données existante

Lorsque vous migrez View Composer vers une autre machine physique ou virtuelle, si vous prévoyez de conserver vos machines virtuelles de clone lié actuelles, le nouveau service VMware Horizon View Composer doit continuer à utiliser la base de données View Composer existante.

Effectuez les étapes de cette procédure lorsque vous migrez View Composer dans les directions suivantes :

- D'une machine vCenter Server vers une machine autonome
- D'une machine autonome vers une machine vCenter Server
- D'une machine autonome vers une autre machine autonome
- D'une machine vCenter Server vers une autre machine vCenter Server

Lorsque vous migrez le service VMware Horizon View Composer, vous pouvez également migrer la base de données View Composer vers un nouvel emplacement. Par exemple, vous devrez peut-être migrer la base de données View Composer si la base de données actuelle se trouve sur une machine vCenter Server que vous migrez également.

Lorsque vous installez le service VMware Horizon View Composer sur la nouvelle machine, vous devez configurer le service pour qu'il se connecte à la base de données View Composer.

Conditions préalables

- Familiarisez-vous avec les exigences de migration de View Composer. Reportez-vous à la section [Conseils sur la migration de View Composer](#).
- Familiarisez-vous avec les étapes de migration du conteneur de clés RSA vers le nouveau service VMware Horizon View Composer. Reportez-vous aux sections [Préparer Microsoft .NET Framework pour la migration de clés RSA](#) et [Migrer le conteneur de clés RSA vers le nouveau service View Composer](#).
- Familiarisez-vous avec l'installation du service VMware Horizon View Composer dans le document *Installation d'Horizon 7*.

- Familiarisez-vous avec la configuration d'un certificat TLS pour View Composer dans le document *Installation d'Horizon 7*.
- Familiarisez-vous avec la configuration de View Composer dans Horizon Administrator. Consultez les rubriques sur la configuration des paramètres de View Composer et des domaines View Composer dans le document *Administration d'Horizon 7*.
- Il est recommandé de vérifier que les machines source et de destination que vous utilisez pour migrer View Composer sont identiques et partagent les mêmes informations d'identification d'administrateur. Lorsque vous migrez View Composer depuis une machine autonome vers une machine vCenter Server sur laquelle View Composer est déjà installé, la configuration de View Composer peut échouer si les informations d'identification utilisées sur les deux machines sont différentes.

Procédure

- 1 Désactivez le provisionnement de machine virtuelle dans l'instance de vCenter Server associée au service VMware Horizon View Composer.
 - a Dans Horizon Administrator, sélectionnez **Configuration de View > Serveurs**.
 - b Dans l'onglet **Serveurs vCenter Server**, sélectionnez l'instance de vCenter Server et cliquez sur **Désactiver l'approvisionnement**.
- 2 (Facultatif) Migrez la base de données View Composer vers un nouvel emplacement.

Si vous devez effectuer cette étape, contactez votre administrateur de base de données pour obtenir des instructions sur la migration.
- 3 Désinstallez le service VMware Horizon View Composer de la machine actuelle.
- 4 (Facultatif) Migrez le conteneur de clés RSA vers la nouvelle machine.
- 5 Installez le service VMware Horizon View Composer sur la nouvelle machine.

Lors de l'installation, spécifiez le nom DSN de la base de données qui était utilisée par le service VMware Horizon View Composer d'origine. Spécifiez également le nom d'utilisateur et le mot de passe d'administrateur de domaine qui étaient fournis pour la source de données ODBC pour cette base de données.

Si vous avez migré la base de données, les informations sur le nom DSN et la source de données doivent pointer vers le nouvel emplacement de la base de données. Que vous ayez migré la base de données ou pas, le nouveau service VMware Horizon View Composer doit avoir accès aux informations de base de données d'origine concernant les clones liés.
- 6 Configurez un certificat de serveur SSL pour View Composer sur la nouvelle machine.

Vous pouvez copier le certificat qui a été installé pour View Composer sur la machine d'origine ou installer un nouveau certificat.
- 7 Dans Horizon Administrator, configurez les nouveaux paramètres de View Composer.
 - a Dans Horizon Administrator, sélectionnez **Configuration de View > Serveurs**.
 - b Dans l'onglet **vCenter Servers**, sélectionnez l'instance de vCenter Server associée à ce service View Composer et cliquez sur **Modifier**.

- c Dans le volet Paramètres de View Composer Server, cliquez sur **Modifier** et fournissez les nouveaux paramètres de View Composer.

Si vous installez View Composer avec vCenter Server sur la nouvelle machine, sélectionnez **View Composer est co-installé avec vCenter Server**.

Si vous installez View Composer sur une machine autonome, sélectionnez **Serveur View Composer Server autonome** et fournissez le FQDN de la machine View Composer, ainsi que le nom d'utilisateur et le mot de passe de l'utilisateur de View Composer.

- d Dans le volet Domaines, cliquez sur **Vérifier les informations sur le serveur** et ajoutez ou modifiez les domaines View Composer si nécessaire.
- e Cliquez sur **OK**.

Migrer View Composer sans machines virtuelles de clone lié

Si le service VMware Horizon View Composer actuel ne gère aucune machine virtuelle de clone lié, vous pouvez migrer View Composer vers une nouvelle machine physique ou virtuelle sans migrer les clés RSA vers la nouvelle machine. Le service VMware Horizon View Composer migré peut se connecter à la base de données View Composer d'origine ou vous pouvez préparer une nouvelle base de données pour View Composer.

Conditions préalables

- Familiarisez-vous avec l'installation du service VMware Horizon View Composer dans le document *Installation d'Horizon 7*.
- Familiarisez-vous avec la configuration d'un certificat TLS pour View Composer dans le document *Installation d'Horizon 7*.
- Familiarisez-vous avec les étapes de suppression de View Composer d'Horizon Administrator. Reportez-vous à la rubrique sur la suppression de View Composer d'Horizon Administrator dans le document *Administration d'Horizon 7*.

Avant de pouvoir supprimer View Composer, vérifiez qu'il ne gère plus aucune machine virtuelle de clone lié. S'il reste des clones liés, vous devez les supprimer.

- Familiarisez-vous avec la configuration de View Composer dans Horizon Administrator. Consultez les rubriques sur la configuration des paramètres de View Composer et des domaines View Composer dans le document *Administration d'Horizon 7*.

Procédure

- 1 Dans Horizon Administrator, supprimez View Composer d'Horizon Administrator.
 - a Sélectionnez **Configuration de View > Serveurs**.
 - b Dans l'onglet **vCenter Servers**, sélectionnez l'instance de vCenter Server associée au service View Composer et cliquez sur **Modifier**.
 - c Dans le volet Paramètres de View Composer Server, cliquez sur **Modifier**.
 - d Sélectionnez **Ne pas utiliser View Composer** et cliquez sur **OK**.

- 2 Désinstallez le service VMware Horizon View Composer de la machine actuelle.

- 3 Installez le service VMware Horizon View Composer sur la nouvelle machine.

Lors de l'installation, configurez View Composer pour qu'il se connecte au nom DSN de la base de données View Composer d'origine ou nouvelle.

- 4 Configurez un certificat de serveur TLS pour View Composer sur la nouvelle machine.

Vous pouvez copier le certificat qui a été installé pour View Composer sur la machine d'origine ou installer un nouveau certificat.

- 5 Dans Horizon Administrator, configurez les nouveaux paramètres de View Composer.

- a Dans Horizon Administrator, sélectionnez **Configuration de View > Serveurs**.
- b Dans l'onglet **vCenter Servers**, sélectionnez l'instance de vCenter Server associée à ce service View Composer et cliquez sur **Modifier**.
- c Dans le volet Paramètres de View Composer Server, cliquez sur **Modifier**.
- d Fournissez les nouveaux paramètres de View Composer.

Si vous installez View Composer avec vCenter Server sur la nouvelle machine, sélectionnez **View Composer est co-installé avec vCenter Server**.

Si vous installez View Composer sur une machine autonome, sélectionnez **Serveur View Composer Server autonome** et fournissez le FQDN de la machine View Composer, ainsi que le nom d'utilisateur et le mot de passe de l'utilisateur de View Composer.

- e Dans le volet Domaines, cliquez sur **Vérifier les informations sur le serveur** et ajoutez ou modifiez les domaines View Composer si nécessaire.
- f Cliquez sur **OK**.

Préparer Microsoft .NET Framework pour la migration de clés RSA

Pour utiliser une base de données View Composer existante, vous devez migrer le conteneur de clés RSA entre les machines. Vous migrez le conteneur de clés RSA à l'aide de l'outil d'inscription ASP.NET IIS fourni avec Microsoft .NET Framework.

Conditions préalables

Téléchargez .NET Framework et lisez les informations sur l'outil d'inscription ASP.NET IIS. Accédez à <http://www.microsoft.com/net>.

Procédure

- 1 Installez .NET Framework sur la machine physique ou virtuelle sur laquelle le service VMware Horizon View Composer associé à la base de données existante est installé.
- 2 Installez .NET Framework sur la machine de destination sur laquelle vous souhaitez installer le nouveau service VMware Horizon View Composer.

Étape suivante

Migrez le conteneur de clés RSA vers la machine de destination. Reportez-vous à la section [Migrer le conteneur de clés RSA vers le nouveau service View Composer](#).

Migrer le conteneur de clés RSA vers le nouveau service View Composer

Pour utiliser une base de données View Composer existante, vous devez migrer le conteneur de clés RSA de la machine physique ou virtuelle source sur laquelle le service VMware Horizon View Composer existant réside vers la machine sur laquelle vous souhaitez installer le nouveau service VMware Horizon View Composer.

Vous devez effectuer cette procédure avant d'installer le nouveau service VMware Horizon View Composer.

Conditions préalables

Vérifiez que les outils d'enregistrement Microsoft .NET Framework et ASP.NET IIS sont installés sur les machines source et de destination. Reportez-vous à la section [Préparer Microsoft .NET Framework pour la migration de clés RSA](#).

Procédure

- 1 Sur la machine source sur laquelle réside le service VMware Horizon View Composer existant, ouvrez une invite de commande et accédez au répertoire %windir%\Microsoft.NET\Framework\v2.0xxxxx.
- 2 Saisissez la commande `aspnet_regiis` pour enregistrer la paire de clés RSA dans un fichier local.

`aspnet_regiis -px "SviKeyContainer" "keys.xml" -pri`

L'outil d'inscription ASP.NET IIS exporte la paire de clés publique/privée RSA du conteneur SviKeyContainer vers le fichier `keys.xml` et enregistre le fichier en local.

- 3 Copiez le fichier `keys.xml` vers la machine de destination sur laquelle vous souhaitez installer le nouveau service VMware Horizon View Composer.

- 4 Sur la machine de destination, ouvrez une invite de commande et accédez au répertoire %windir%\Microsoft.NET\Framework\v2.0xxxxx.

- 5 Saisissez la commande `aspnet_regiis` pour migrer les données de la paire de clés RSA.

`aspnet_regiis -pi "SviKeyContainer" "path\keys.xml" -exp`

où *path* est le chemin vers le fichier exporté.

L'option `-exp` crée une paire de clés exportable. Si une future migration est requise, les clés peuvent être exportées depuis cette machine et importées vers une autre machine. Si vous avez précédemment migré les clés vers cette machine sans utiliser l'option `-exp`, vous pouvez de nouveau importer les clés à l'aide de l'option `-exp` afin de pouvoir exporter les clés ultérieurement.

L'outil d'inscription importe les données de paire de clés dans le conteneur de clés local.

Étape suivante

Installez le nouveau service VMware Horizon View Composer sur la machine de destination. Fournissez les informations sur le nom DSN et la source de données ODBC qui permettent à View Composer de se connecter aux mêmes informations de base de données que celles utilisées par le service VMware Horizon View Composer d'origine. Pour plus d'informations sur l'installation, consultez la section « Installation de View Composer » dans le document *Installation d'Horizon 7*.

Effectuez les étapes pour migrer View Composer vers une nouvelle machine et utiliser la même base de données. Reportez-vous à la section [Migrer View Composer avec une base de données existante](#).

Mise à niveau du Serveur de connexion VMware Horizon

Si votre déploiement utilise des équilibres de charge pour gérer des instances du Serveur de connexion, il est possible d'effectuer une mise à niveau de l'infrastructure du serveur de connexion sans interruption de service.

Note Avant de pouvoir utiliser la fonction d'Horizon 6 version 6.2 pour cloner un pool de postes de travail, vous devez mettre à niveau toutes les instances du Serveur de connexion d'un espace vers Horizon 6 version 6.2 ou supérieure.

Après avoir effectué une nouvelle installation ou une mise à niveau de toutes les instances du Serveur de connexion vers Horizon 7 version 7.2, vous ne pouvez pas rétrograder les instances du Serveur de connexion vers une version antérieure à Horizon 7 version 7.2, car les clés de protection des données LDAP ont été modifiées.

Pour avoir malgré tout la possibilité de rétrograder des instances du Serveur de connexion dont vous planifiez la mise à niveau vers Horizon 7 version 7.2, vous devez sauvegarder les instances du Serveur de connexion avant de commencer la mise à niveau. Si vous avez besoin de rétrograder les instances du Serveur de connexion, vous devez rétrograder toutes les instances du Serveur de connexion, puis appliquer la sauvegarde au dernier Serveur de connexion rétrogradé.

Préparation du Serveur de connexion pour une mise à niveau

Avant d'effectuer la mise à niveau du Serveur de connexion ou de l'un des composants vSphere sur lesquels repose le Serveur de connexion, vous devez effectuer plusieurs tâches afin de garantir la réussite de ces mises à niveau.

Tâches à effectuer sur une seule instance d'un groupe répliqué

Avant de commencer la mise à jour d'une instance du Serveur de connexion, effectuez les tâches suivantes à l'aide d'une seule des instances. Puisque les instances sont répliquées, les paramètres d'une des instances sont appliqués à toutes les autres :

- Si le Serveur de connexion est installé sur une machine virtuelle, prenez un snapshot de la machine virtuelle.

Pour plus d'instructions sur la prise de snapshots, consultez l'aide en ligne de vSphere Client. Si vous devez rétablir ce snapshot et que vous possédez d'autres instances du Serveur de connexion dans un groupe répliqué, vous devez désinstaller ces instances avant de rétablir le snapshot du maître. Après avoir rétabli le snapshot, vous pouvez réinstaller les instances répliquées et pointer vers l'instance rétablie.

Vous pouvez nommer le snapshot Phase de préparation de mise à niveau.

- Ouvrez Horizon Administrator et consignez tous les paramètres et paramètres globaux des postes de travail et des pools : les sections Pools et Postes de travail de l'arborescence de l'inventaire et la section des paramètres globaux dans l'arborescence de configuration de View.

Par exemple, prenez une capture d'écran des paramètres applicables.

- Utilisez l'utilitaire `vdmexport.exe` pour sauvegarder la base de données LDAP.

Pour obtenir des instructions, consultez le guide d'administration de votre version actuelle du document Administration de *Administration d'Horizon 7*.

Tâches à effectuer pour chaque instance avant la mise à niveau

- Vérifiez que la machine virtuelle ou physique sur laquelle l'instance actuelle du Serveur de connexion est installée satisfait les exigences système pour la nouvelle version.

Reportez-vous à la section [Exigences du Serveur de connexion Horizon](#).

- Renseignez l'adresse IP et le nom de système de la machine sur laquelle le Serveur de connexion est installé.
- Déterminez si votre entreprise a écrit des fichiers ou des scripts de commandes qui s'exécutent sur la base de données View sur l'instance du Serveur de connexion, et si c'est le cas, fournissez leurs noms et leurs emplacements.
- Ouvrez Horizon Administrator et consignez tous les paramètres spécifiques à cette instance.

Par exemple, accédez à **Configuration de View > Serveurs > Serveurs de connexion**, sélectionnez l'instance du serveur de connexion dans le tableau et cliquez sur **Modifier**. Vous pouvez enregistrer une copie d'écran de chaque onglet dans la boîte de dialogue **Modifier les paramètres du serveur de connexion**.

Mise à niveau de Serveurs de connexion dans un groupe répliqué

Cette procédure décrit la mise à niveau des instances du Serveur de connexion qui ne sont pas couplées à des serveurs de sécurité. Par exemple, cette procédure s'applique aux Serveurs de connexion configurés pour se connecter à des clients situés dans l'enceinte du pare-feu de la société.

Pour les instances du Serveur de connexion couplées à des serveurs de sécurité, suivez la procédure décrite dans [Mettre à niveau les serveurs de sécurité et leurs Serveurs de connexion couplés](#).

Vous n'avez pas besoin de redémarrer le Serveur de connexion lorsque la mise à niveau est terminée.

Note Cette procédure décrit une mise à niveau sur place. Pour migrer vers une machine différente, reportez-vous à la section [Mise à niveau vers la version la plus récente du Serveur de connexion sur une machine différente](#).

Conditions préalables

- Déterminez quand effectuer cette procédure. Choisissez une période de maintenance de poste de travail disponible. La durée de la mise à niveau dépend du nombre d'instances du Serveur de connexion dans le groupe. Prévoyez 15 à 30 minutes pour chaque instance.
- Si vous utilisez View Composer, vérifiez qu'il a été mis à niveau. Reportez-vous à la section [Mise à niveau de View Composer](#). Après avoir effectué la mise à niveau du Serveur de connexion, vous devez ajouter View Composer à l'aide d'Horizon Administrator.
- Familiarisez-vous avec les exigences liées à la sécurité d'Horizon 7 et vérifiez que ces exigences sont respectées. Reportez-vous à la section [Exigences de mise à niveau du Serveur de connexion Horizon](#). Vous devez obtenir et installer un certificat de serveur SSL signé par une autorité de certification qui inclut des informations de révocation de certificat, vérifier que le Pare-feu Windows avec sécurité avancée est défini sur **on** et configurer des pare-feu principaux pour prendre en charge IPsec.
- Vérifiez que le serveur sur lequel vCenter Server est installé possède un certificat de serveur SSL signé par une autorité de certification installé et configuré. Après la mise à niveau du Serveur de connexion, si vCenter Server n'utilise pas de certificat signé par une autorité de certification, le certificat auto-signé par défaut est affiché comme étant non valide dans Horizon Administrator, et un message indique que vCenter Server n'est pas disponible.
- Effectuez les tâches répertoriées dans la section [Préparation du Serveur de connexion pour une mise à niveau](#)
- Vérifiez que vous possédez une licence valide pour la nouvelle version.

Note Lorsque vous effectuez une mise à niveau de la version 6.0.x ou 6.1.x vers la version 6.2, votre licence précédente fonctionnera toujours et le modèle d'utilisation sera défini sur **Utilisateurs simultanés**. Un nouveau modèle de licence appelé Utilisateur nommé a été ajouté à partir d'Horizon 6 version 6.2. Vous avez la possibilité de passer le modèle de licence sur **Utilisateur nommé**. Pour plus d'informations, consultez le document <http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf>.

- Vérifiez que vous possédez un compte d'utilisateur de domaine avec des privilèges d'administration sur les hôtes que vous allez utiliser pour exécuter le programme d'installation et réaliser la mise à niveau.

- Si vous ne connaissez pas l'utilitaire `vdmexport.exe`, imprimez ses instructions d'utilisation à partir du document Administration de *Administration d'Horizon 7*. Vous utiliserez cet utilitaire pour sauvegarder la base de données View LDAP dans le cadre de la procédure de mise à niveau.

Vous n'avez pas à modifier la configuration des équilibres de charge existants.

Procédure

- 1 Si vous utilisez un équilibrage de charge pour gérer un groupe d'instances du Serveur de connexion, désactivez le serveur qui héberge l'instance du Serveur de connexion que vous êtes sur le point de mettre à niveau.
 - a Ouvrez une session sur Horizon Administrator.
 - b Accédez à **Configuration de View > Serveurs** et cliquez sur l'onglet **Serveurs de connexion**.
 - c Sélectionnez l'instance du Serveur de connexion dans la liste et cliquez sur le bouton **Désactiver** au-dessus du tableau.
 - d Cliquez sur **OK** pour confirmer la désactivation du serveur.

- 2 Sur l'hôte de l'instance du Serveur de connexion, téléchargez et exécutez le programme d'installation de la nouvelle version de 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. Vous n'avez pas besoin d'arrêter des services avant d'effectuer la mise à niveau. Le programme d'installation s'arrête et redémarre des services si nécessaire. En fait, le service VMwareVDMDS doit être en cours d'exécution pour mettre à niveau la base de données View LDAP.

Le programme d'installation détermine qu'une version antérieure est déjà installée et effectue une mise à niveau. Le programme d'installation affiche moins d'options d'installation qu'au cours d'une nouvelle installation.

View LDAP est de nouveau mis à niveau.

Note Avant d'exécuter la mise à niveau, le programme d'installation effectue un contrôle de l'état de réplication pour déterminer si le serveur peut communiquer avec les autres serveurs dans le groupe répliqué et si le serveur peut extraire des mises à jour LDAP depuis les autres serveurs dans le groupe. Si le contrôle de l'état échoue, la mise à niveau n'a pas lieu.

- 3 Vérifiez que le service Serveur de connexion VMware Horizon redémarre lorsque l'assistant du programme d'installation se ferme.
- 4 Ouvrez une session sur Horizon Administrator et activez l'instance du Serveur de connexion que vous venez de mettre à niveau.
 - a Accédez à **Configuration de View > Serveurs** et cliquez sur l'onglet **Serveurs de connexion**.
 - b Sélectionnez l'instance du Serveur de connexion dans la liste et cliquez sur le bouton **Activer** au-dessus du tableau.
 - c Dans la colonne Version, vérifiez que la nouvelle version est affichée.

- 5 Accédez à **Configuration de View > Licence produit et utilisation**, cliquez sur **Modifier la licence**, entrez la clé de licence de et cliquez sur **OK**.
- 6 Si vous utilisez un équilibrage de charge pour gérer cette instance du Serveur de connexion, activez le serveur que vous venez de mettre à niveau.
- 7 Vérifiez que vous pouvez ouvrir une session sur un poste de travail distant.
- 8 Répétez les étapes précédentes pour mettre à niveau chaque instance du Serveur de connexion du groupe.

Important Si vous ne mettez pas à niveau toutes les instances du Serveur de connexion dans un groupe répliqué, les indicateurs d'intégrité dans le tableau de bord Horizon Administrator peuvent indiquer qu'une ou plusieurs instances sont dans un état d'erreur. Cette situation se produit car différentes versions fournissent différents types de données. La solution consiste à mettre à niveau toutes les instances dans le groupe répliqué.

- 9 Utilisez l'utilitaire `vdmexport.exe` pour sauvegarder la base de données View LDAP mise à niveau.
Si vous possédez plusieurs instances du Serveur de connexion dans un groupe répliqué, vous devez exporter les données à partir d'une seule instance.
- 10 Ouvrez une session sur Horizon Administrator et examinez le tableau de bord pour vérifier que les icônes de vCenter Server et View Composer sont vertes.

Si l'une des icônes est rouge et que la boîte de dialogue Certificat non valide détecté apparaît, vous devez cliquer sur **Vérifier** et accepter l'empreinte numérique du certificat non approuvé, comme décrit dans « Étape suivante », ou installer un certificat SSL signé par une autorité de certification valide.

Pour plus d'informations sur le remplacement du certificat par défaut pour vCenter Server, consultez le document *Exemples et scénarios VMware vSphere*.

- 11 Vérifiez que les icônes du tableau de bord des instances du Serveur de connexion sont également vertes.

Si des instances ont des icônes rouges, cliquez sur l'instance pour déterminer l'état de réplication. La réplication peut être affectée pour l'une des raisons suivantes :

- Un pare-feu peut bloquer la communication
- Le service VDMDS de VMware peut être arrêté pour une instance du Serveur de connexion
- Les options VDMS DSA de VMware peuvent bloquer les réplifications
- Un problème de réseau s'est produit

Étape suivante

Pour utiliser un certificat par défaut ou auto-signé à partir de vCenter Server ou View Composer, reportez-vous à la section [Accepter l'empreinte numérique d'un certificat TLS par défaut](#).

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](#).

En cas d'échec de la mise à niveau sur une ou plusieurs instances du Serveur de connexion, reportez-vous à la section [Créer un groupe répliqué après avoir rétabli un snapshot du Serveur de connexion](#)

Important Si vous prévoyez d'utiliser le mode de sécurité des messages amélioré pour les messages JMS, assurez-vous que les pare-feu permettent aux instances du Serveur de connexion de recevoir du trafic JMS entrant sur le port 4002 à partir des postes de travail et des serveurs de sécurité. Ouvrez également le port 4101 pour accepter des connexions d'autres instances du Serveur de connexion.

Si vous réinstallez le Serveur de connexion sur un serveur doté d'un ensemble de collecteur de données configuré pour contrôler les données de performances, arrêtez l'ensemble de collecteur de données et redémarrez-le.

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=vdi**, **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=Propriétés**, 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.

Mise à niveau vers la version la plus récente du Serveur de connexion sur une machine différente

Dans le cadre de votre mise à niveau, vous pouvez migrer le Serveur de connexion vers une nouvelle machine.

Conditions préalables

- Mettez à niveau au moins une instance du Serveur de connexion existante vers la version la plus récente. Reportez-vous à la section [Mise à niveau de Serveurs de connexion dans un groupe répliqué](#). Au cours de cette mise à niveau, votre View LDAP existant sera mis à niveau.
- Vérifiez que la nouvelle machine physique ou virtuelle satisfait aux exigences du système pour l'installation du Serveur de connexion. Reportez-vous aux sections [Systèmes d'exploitation pris en charge pour le Serveur de connexion Horizon](#) et [Configuration matérielle requise du Serveur de connexion Horizon](#).
- Familiarisez-vous avec les exigences liées à la sécurité d'Horizon 7 et vérifiez que ces exigences sont respectées. Reportez-vous à la section [Exigences de mise à niveau du Serveur de connexion Horizon](#).
- Déterminez quand effectuer cette procédure. Choisissez une période de maintenance de poste de travail disponible. Prévoyez 15 à 30 minutes pour chaque instance.
- Vérifiez que vous possédez un compte d'utilisateur de domaine avec des privilèges d'administration sur l'hôte que vous utiliserez pour exécuter le programme d'installation.
- Familiarisez-vous avec la procédure d'installation d'une instance répliquée. Reportez-vous au document *Installation d'Horizon 7*. Vous installez une instance répliquée dans le cadre de cette procédure.

Vous n'avez pas à modifier la configuration des équilibreurs de charge existants.

Procédure

- 1 Vérifiez qu'une instance mise à niveau du Serveur de connexion est exécutée et accessible pour la nouvelle machine sur laquelle vous prévoyez d'installer le Serveur de connexion.

Lorsque vous installez le Serveur de connexion sur le nouvel hôte, vous pointerez vers cette instance existante.
- 2 Sur la nouvelle machine, installez une instance répliquée du Serveur de connexion.

Le View LDAP sur la nouvelle instance répliquera celui de l'instance source mise à niveau.
- 3 Le cas échéant, désinstallez le Serveur de connexion de l'ancien hôte en utilisant l'utilitaire **Ajout/Suppression de programmes** de Windows.
- 4 Dans Horizon Administrator, accédez à l'onglet **Configuration de View > Serveurs > Serveurs de connexion** et déterminez si l'instance du Serveur de connexion qui a été désinstallée figure toujours dans la liste.
- 5 Si l'instance désinstallée du Serveur de connexion apparaît toujours dans la liste, utilisez une commande `vdadmin` pour la supprimer.

`vdadmin.exe -S -s server_name -r`

Dans cet exemple, *server_name* est le nom d'hôte ou l'adresse IP de l'hôte du Serveur de connexion. Pour plus d'informations sur l'outil de ligne de commande `vdadmin`, consultez le document *Administration d'Horizon 7*.

Une nouvelle instance du Serveur de connexion est ajoutée à un groupe et une ancienne instance est supprimée.

Étape suivante

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 mise à niveau des autres composants serveur Horizon 7.

Si vous réinstallez le Serveur de connexion sur un serveur doté d'un ensemble de collecteur de données configuré pour contrôler les données de performances, arrêtez l'ensemble de collecteur de données et redémarrez-le.

Créer un groupe répliqué après avoir rétabli un snapshot du Serveur de connexion

Si une mise à niveau échoue ou si vous devez pour une autre raison rétablir un snapshot d'une machine virtuelle hébergeant un serveur de connexion, vous devez désinstaller les autres instances du serveur de connexion dans le groupe et recréer le groupe répliqué.

Si vous rétablissez le snapshot d'une machine virtuelle du serveur de connexion, les objets View LDAP de la base de données de cette machine virtuelle ne sont plus cohérents avec les objets View LDAP des bases de données des autres instances répliquées. Après le rétablissement d'un snapshot, l'événement suivant est journalisé dans le journal des événements de Windows, dans le journal des événements

VMwareVDMDS (ID de l'événement 2103) : The Active Directory Lightweight Directory Services database has been restored using an unsupported restoration procedure (La base de données Active Directory Lightweight Directory Services a été restaurée à l'aide d'une procédure de restauration non prise en charge). La machine virtuelle rétablie interrompt la réplication de son répertoire View LDAP.

Si vous estimez nécessaire de rétablir un snapshot, vous devez désinstaller les autres instances du Serveur de connexion ainsi que le répertoire View LDAP sur ces machines virtuelles, puis réinstaller les instances de réplica.

Conditions préalables

Déterminez quelle instance du serveur de connexion doit être le nouveau serveur de connexion standard ou maître. Ce serveur de connexion dispose des données de configuration Horizon 7 souhaitées.

Procédure

- 1 Sur toutes les instances du Serveur de connexion hormis celle choisie comme nouvelle instance du Serveur de connexion standard, désinstallez le Serveur de connexion ainsi que l'instance de View LDAP.

L'instance LDAP View est appelée AD LDS Instance VMwareVDMDS.

- 2 Si la machine virtuelle hébergeant l'instance du Serveur de connexion standard ou maître, ouvrez une invite de commande et saisissez la commande suivante afin de vous assurer que la réplication n'est pas désactivée.

```
repadmin /options localhost:389 -DISABLE_OUTBOUND_REPL -DISABLE_INBOUND_REPL
```

- 3 Sur les machines virtuelles devant héberger l'instance de réplica du Serveur de connexion, exécutez le programme d'installation du serveur de connexion, sélectionnez l'option d'installation de **Serveur réplica View**, puis spécifiez le nom d'hôte ou l'adresse IP de l'instance standard du Serveur de connexion.

Le groupe répliqué d'instances du Serveur de connexion est recréé avec des objets View LDAP cohérents.

Mise à niveau des serveurs de sécurité

Si votre déploiement utilise des équilibres de charge pour gérer plusieurs serveurs de sécurité, vous pouvez effectuer une mise à niveau de l'infrastructure du Serveur de connexion sans interruption de service.

Note Pour utiliser des dispositifs Unified Access Gateway au lieu de serveurs de sécurité, vous devez mettre à niveau les instances du Serveur de connexion vers Horizon 6 version 6.2 ou version ultérieure avant d'installer et de configurer les dispositifs Unified Access Gateway pour qu'ils pointent vers les instances du Serveur de connexion ou l'équilibrage de charge associé aux instances. Pour plus d'informations, reportez-vous à la section [Remplacement d'un serveur de sécurité par un dispositif Unified Access Gateway](#).

Préparation du serveur de sécurité pour une mise à niveau

Avant de mettre les serveurs de sécurité à niveau, effectuez ces tâches pour créer des sauvegardes et enregistrer les paramètres de configuration.

- Vérifiez que la machine virtuelle ou physique sur laquelle le serveur de sécurité actuel est installé satisfait les exigences système de la nouvelle version.

Reportez-vous à la section [Exigences du Serveur de connexion Horizon](#).

- Si le serveur de sécurité est installé sur une machine virtuelle, prenez un snapshot de la machine virtuelle.

Pour plus d'instructions sur la prise de snapshots, consultez l'aide en ligne de vSphere Client. Vous pouvez nommer le snapshot Phase de préparation de mise à niveau.

- Ouvrez Horizon Administrator et notez les paramètres de ce serveur de sécurité. Accédez à **Configuration de View > Serveurs** et cliquez sur l'onglet **Serveurs de sécurité**.

Par exemple, sélectionnez le serveur de sécurité, cliquez sur **Edit (Modifier)** et enregistrez une copie d'écran des paramètres.

- Notez l'adresse IP et le nom de système de la machine sur laquelle le serveur de sécurité est installé.
- Si vous utilisez des équilibreurs de charge pour les serveurs de sécurité, notez les paramètres de configuration des équilibreurs de charge.

Note Cette rubrique ne couvre pas la description de la commande d'Horizon Administrator **Préparation pour la mise à niveau ou la réinstallation**, disponible dans l'onglet **Serveurs de sécurité**. Cette commande supprime les règles d'IPsec du serveur de sécurité, ce qui arrête toutes les communications entre le serveur de sécurité et l'instance du Serveur de connexion couplée. En conséquence, la commande devra être utilisée pendant la procédure de mise à niveau, immédiatement après la mise à niveau du serveur de sécurité, comme décrit dans [Mettre à niveau les serveurs de sécurité et leurs Serveurs de connexion couplés](#).

Mettre à niveau les serveurs de sécurité et leurs Serveurs de connexion couplés

Suivez cette procédure si l'instance du Serveur de connexion que vous prévoyez de mettre à jour est couplée à un serveur de sécurité.

Cette procédure est conçue pour mettre à niveau un serveur de sécurité et son instance du Serveur de connexion couplée avant de mettre à niveau le serveur de sécurité suivant et son instance du Serveur de connexion couplée. Cette stratégie permet d'éviter les interruptions. Si cette instance n'est pas couplée à un serveur de sécurité, suivez la procédure [Mise à niveau de Serveurs de connexion dans un groupe répliqué](#).

Les premières étapes de cette procédure impliquent la mise à niveau de l'instance du Serveur de connexion. Après la mise à niveau du Serveur de connexion et avant la mise à niveau du serveur de sécurité, l'une des étapes décrit la suppression des règles IPsec pour le serveur de sécurité. Lorsque 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 défaut, la communication entre un serveur de sécurité et son instance du Serveur de connexion couplée est régie par des règles IPsec. Si les règles IPsec existantes ne sont pas supprimées avant la mise à niveau ou la réinstallation, le couplage entre le serveur de sécurité et le Serveur de connexion échoue, et il n'est pas possible de mettre en place de nouvelles règles IPsec après la mise à niveau.

Conditions préalables

- Déterminez quand effectuer cette procédure. Choisissez une période de maintenance de poste de travail disponible. Prévoyez 15 à 30 minutes pour chaque serveur de sécurité et son instance du Serveur de connexion couplée.
- Si vous utilisez View Composer, vérifiez qu'il a été mis à niveau. Reportez-vous à la section [Mise à niveau de View Composer](#). Après avoir effectué la mise à niveau du Serveur de connexion, vous devez ajouter View Composer à l'aide d'Horizon Administrator.
- Familiarisez-vous avec les exigences liées à la sécurité d'Horizon 7 et vérifiez que ces exigences sont respectées. Reportez-vous à la section [Exigences de mise à niveau du Serveur de connexion Horizon](#). Vous devez obtenir et installer un certificat de serveur TLS signé par une autorité de certification qui inclut des informations de révocation de certificat, vérifier que le Pare-feu Windows avec sécurité avancée est défini sur **on** et configurer des pare-feu principaux pour prendre en charge IPsec.
- Vérifiez que les machines virtuelles ou physiques sur lesquelles le serveur de sécurité actuel et les instances du Serveur de connexion sont installés satisfont les exigences système.
Reportez-vous à la section [Exigences du Serveur de connexion Horizon](#).
- Effectuez les tâches répertoriées dans la section [Préparation du Serveur de connexion pour une mise à niveau](#)
- Vérifiez que vous possédez une licence pour la nouvelle version.
- Vérifiez que vous possédez un compte d'utilisateur disposant de privilèges d'administration sur les hôtes que vous allez utiliser pour exécuter le programme d'installation et effectuer la mise à niveau.
- 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.

Procédure

- 1 Si vous utilisez un équilibrage de charge pour gérer des serveurs de sécurité couplés avec des instances du Serveur de connexion, désactivez le serveur de sécurité couplé avec l'instance du Serveur de connexion que vous êtes sur le point de mettre à niveau.
- 2 Mettez à niveau l'instance du Serveur de connexion couplée à ce serveur de sécurité.
Suivez les étapes 2 à 6 de [Mise à niveau de Serveurs de connexion dans un groupe répliqué](#).
- 3 Supprimez les règles IPsec pour le serveur de sécurité couplé à l'instance du Serveur de connexion que vous venez de mettre à niveau.
 - a Dans Horizon Administrator, cliquez sur **Configuration de View > Serveurs**.
 - b 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.
 - c 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.
- 4 Configurez un mot de passe de couplage de serveur de sécurité à l'aide de la dernière version d'Horizon Administrator. Reportez-vous à la section « Configurer un mot de passe de couplage de serveur de sécurité » dans le document *Installation d'Horizon 7*.
- 5 Sur l'hôte du serveur de sécurité, téléchargez et exécutez le programme d'installation de la dernière version du 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. Le programme d'installation détermine qu'une version antérieure est déjà installée et effectue une mise à niveau. Le programme d'installation affiche moins d'options d'installation qu'au cours d'une nouvelle installation.

Vous serez invité à fournir le mot de passe de couplage de serveur de sécurité.

Vous pourrez être invité à faire disparaître une boîte de message vous informant que le service du serveur de sécurité a été arrêté. Le programme d'installation arrête le service en préparation pour la mise à niveau.
- 6 Quand l'assistant du programme d'installation a terminé, vérifiez que le service du serveur de sécurité VMware Horizon View a démarré.
- 7 Si vous utilisez un équilibreur de charge pour gérer ce serveur de sécurité, ajoutez de nouveau ce serveur au groupe faisant l'objet de l'équilibrage de charge.
- 8 Ouvrez une session sur Horizon Administrator, sélectionnez le serveur de sécurité dans le tableau de bord et vérifiez que le serveur de sécurité est maintenant à la dernière version.
- 9 Vérifiez que vous pouvez ouvrir une session sur un poste de travail distant.

- 10** Dans Horizon Administrator, accédez à l'onglet **Configuration de View > Serveurs > Serveurs de sécurité** et supprimez les serveurs de sécurité en double dans la liste.

Le mécanisme de couplage de serveur de sécurité automatisé peut produire des entrées en double dans la liste **Serveurs de sécurité** si le nom de système complet ne correspond pas au nom qui a été affecté lors de la création du serveur de sécurité.

- 11** Utilisez l'utilitaire `vdmexport.exe` pour sauvegarder la base de données View LDAP mise à niveau.

Si vous possédez plusieurs instances du Serveur de connexion dans un groupe répliqué, vous devez exporter les données à partir d'une seule instance.

- 12** Ouvrez une session sur Horizon Administrator et examinez le tableau de bord pour vérifier que les icônes de vCenter Server et View Composer sont vertes.

Si l'une des icônes est rouge et que la boîte de dialogue Certificat non valide détecté apparaît, vous devez cliquer sur **Vérifier** et accepter l'empreinte numérique du certificat non approuvé, comme décrit dans « Étape suivante », ou installer un certificat SSL signé par une autorité de certification valide.

Pour plus d'informations sur le remplacement du certificat par défaut pour vCenter Server, consultez le document *Exemples et scénarios VMware vSphere*.

- 13** Vérifiez que les icônes du tableau de bord des instances du Serveur de connexion sont également vertes.

Si des instances ont des icônes rouges, cliquez sur l'instance pour déterminer l'état de réplication. La réplication peut être affectée pour l'une des raisons suivantes :

- Un pare-feu peut bloquer la communication
- Le service VDMDS de VMware peut être arrêté pour une instance du Serveur de connexion
- Les options VDMS DSA de VMware peuvent bloquer les réplifications
- Un problème de réseau s'est produit

Étape suivante

Pour utiliser un certificat par défaut ou auto-signé à partir de vCenter Server ou View Composer, reportez-vous à la section [Accepter l'empreinte numérique d'un certificat TLS par défaut](#).

En cas d'échec de la mise à niveau sur une ou plusieurs instances du Serveur de connexion, reportez-vous à la section [Créer un groupe répliqué après avoir rétabli un snapshot du Serveur de connexion](#)

Important Si vous prévoyez d'utiliser le mode de sécurité des messages amélioré pour les messages JMS, assurez-vous que les pare-feu permettent aux instances du Serveur de connexion de recevoir du trafic JMS entrant sur le port 4002 à partir des postes de travail et des serveurs de sécurité. Ouvrez également le port 4101 pour accepter des connexions d'autres instances du Serveur de connexion.

Si vous réinstallez le Serveur de connexion sur un serveur doté d'un ensemble de collecteur de données configuré pour contrôler les données de performances, arrêtez l'ensemble de collecteur de données et redémarrez-le.

Remplacement d'un serveur de sécurité par un dispositif Unified Access Gateway

Vous pouvez remplacer un serveur de sécurité par un dispositif Unified Access Gateway.

Conditions préalables

Pour utiliser des dispositifs Unified Access Gateway au lieu de serveurs de sécurité, vous devez mettre à niveau les instances du Serveur de connexion vers Horizon 6 version 6.2 ou version ultérieure avant d'installer et de configurer les dispositifs Unified Access Gateway pour qu'ils pointent vers les instances du Serveur de connexion ou l'équilibrage de charge associé aux instances.

Procédure

- 1 Désinstallez le logiciel du serveur de sécurité.
- 2 Supprimez la configuration IPsec du serveur de sécurité. Reportez-vous à la section *Supprimer les règles IPsec pour le serveur de sécurité* dans le document *Installation d'Horizon 7*.
- 3 Supprimez l'entrée LDAP du serveur de sécurité. Consultez la section *Suppression de l'entrée pour une instance du Serveur de connexion ou un serveur de sécurité à l'aide de l'option -S* dans le document *Administration d'Horizon 7*.
- 4 Dans Horizon Administrator, enregistrez le dispositif Unified Access Gateway.
- 5 Au niveau du pare-feu de réseau entre Unified Access Gateway et le Serveur de connexion, supprimez les règles de pare-feu associées au serveur de sécurité supprimé et ajoutez des règles de pare-feu associées à la passerelle Unified Access Gateway entrante. Unified Access Gateway doit communiquer avec le Serveur de connexion sur le port TCP 443.

Les règles de pare-feu principal pour le serveur de sécurité vers le Serveur de connexion sont les suivantes :

Source	Port par défaut	Protocole	Destination	Port par défaut	Remarques
Serveur de sécurité	UDP 500	ISAKMP	Serveur de connexion	UDP 500	Négociation de phase 1 IPsec.
Serveur de sécurité	UDP 4500	NAT-T	Serveur de connexion	UDP 4500	Trafic AJP13 encapsulé lorsque NAT est utilisé.
Serveur de sécurité		ESP	Serveur de connexion		Trafic AJP13 encapsulé lorsque NAT Traversal n'est pas requis. ESP est le protocole IP 50. Les numéros de ports ne sont pas spécifiés.
Serveur de sécurité		AJP13	Serveur de connexion	TCP 8009	Trafic AJP13 sans IPsec et pendant le couplage.
Serveur de sécurité		JMS	Serveur de connexion	TCP 4001	Canal de message pour la négociation des clés.
Serveur de sécurité		JMS-TLS	Serveur de connexion	TCP 4002	Canal de message pour la gestion.

6 Configurez et démarrez le dispositif Unified Access Gateway.

Consultez le document *Déploiement et configuration de VMware Unified Access Gateway* à l'adresse <https://docs.vmware.com/fr/Unified-Access-Gateway/index.html>.

Mise à niveau d'un environnement Architecture Cloud Pod

La fonctionnalité Architecture Cloud Pod utilise des composants Horizon 7 standard pour permettre l'administration de plusieurs centres de données. Avec la fonctionnalité Architecture Cloud Pod, vous liez plusieurs espaces ensemble afin de fournir un environnement unique et volumineux d'échange et de gestion de postes de travail et d'applications. Un espace se compose d'un ensemble d'instances de Serveur de connexion, d'un stockage partagé, d'un serveur de base de données et des infrastructures vSphere et réseau requises pour héberger les pools de postes de travail et d'applications.

Utilisez le processus suivant pour mettre à niveau un environnement Architecture Cloud Pod.

- 1 Mettez à niveau toutes les instances de Serveur de connexion d'un espace en suivant le processus habituel de mise à niveau d'une instance de Serveur de connexion unique.
- 2 Répétez l'étape précédente pour les autres espaces de la fédération d'espaces pour mettre les espaces à niveau un par un.

Pendant le processus de mise à niveau, certaines instances du Serveur de connexion utilisent la dernière version d'Horizon 7 et certaines utilisent l'ancienne version. Même si cet environnement comprenant plusieurs versions est pris en charge à partir d'Horizon 7 version 7.4, les nouvelles fonctionnalités ne sont pas opérationnelles dans un environnement mixte. Par exemple, une nouvelle fonctionnalité qui figure dans Horizon Administrator sur un serveur mis à niveau n'est pas visible dans Horizon Administrator sur un serveur non mis à niveau.

Pour plus d'informations sur la conception et le paramétrage d'un environnement Architecture Cloud Pod, consultez *Administration d'Architecture Cloud Pod dans Horizon 7*.

Mise à niveau de serveurs Horizon 7 pour autoriser HTML Access

Lors de la mise à niveau d'instances du Serveur de connexion ou de serveurs de sécurité derrière un équilibrage de charge ou derrière une passerelle, telle qu'Unified Access Gateway, vous devez modifier la configuration pour continuer à utiliser HTML Access.

Pour plus d'informations, consultez les sections « Autoriser HTML Access via un équilibrage de charge » et « Autoriser HTML Access via une passerelle » dans le document *Installation d'Horizon 7*.

Mettre à niveau vCenter Server

Exécutez une mise à niveau de vCenter Server lors de la période de maintenance au cours de laquelle vous mettez à niveau d'autres composants de serveur Horizon 7. Avant de mettre à niveau vCenter Server, vous devez sauvegarder certaines données d'Horizon 7. Après la mise à niveau, si View Composer est exécuté sur le même serveur, vous devez redémarrer le service View Composer.

Note Lors de la mise à niveau de vCenter Server, les sessions d'applications et de postes de travail distants ne seront pas déconnectées. La fonctionnalité suivante ne sera cependant pas disponible lors de la mise à niveau de vCenter Server :

- Les postes de travail à distance en état de provisionnement ne seront pas activés.
- Les nouveaux postes de travail ne seront pas activés.
- Les opérations de View Composer ne sont pas autorisées.

Conditions préalables

- Déterminez quand effectuer cette procédure. Choisissez une période de maintenance de poste de travail disponible. Pour plus d'informations sur le temps nécessaire, reportez-vous au *Guide de mise à niveau de VMware vSphere*.
- Sauvegardez les bases de données vCenter Server et View Composer.
- Sauvegardez la base de données View LDAP à partir d'une instance du Serveur de connexion à l'aide de l'utilitaire `vdmexport.exe`.

Pour obtenir des instructions, reportez-vous au document *Administration d'Horizon 7*. Si vous possédez plusieurs instances du Serveur de connexion dans un groupe répliqué, vous devez exporter les données à partir d'une seule instance.

- Effectuez les tâches répertoriées dans la section [Préparation de mises à niveau incluant vSphere](#).
- Vérifiez que le serveur sur lequel vCenter Server est installé possède un certificat de serveur TLS signé par une autorité de certification installé et configuré. Après la mise à niveau du Serveur de connexion, si vCenter Server n'utilise pas de certificat signé par une autorité de certification, le certificat auto-signé par défaut est affiché comme étant non valide dans Horizon Administrator, et un message indique que vCenter Server n'est pas disponible.
- Remplissez les conditions préalables répertoriées dans le *Guide de mise à niveau de VMware vSphere*, en utilisant la version du guide qui correspond à la version de vSphere vers laquelle vous prévoyez d'effectuer la mise à niveau.
- Pour mettre à niveau vCenter Server lorsque des Instant Clones sont en cours d'utilisation, reportez-vous aux étapes décrites dans l'article de la base de connaissances de VMware <https://kb.vmware.com/s/article/52573>.

Procédure

- 1 Mettez à niveau vCenter Server de la manière décrite dans le *Guide de mise à niveau de VMware vSphere*.

Important Si vos clusters contiennent des banques de données vSAN, reportez-vous également au chapitre sur la mise à niveau du cluster vSAN, dans le document *Administration de VMware vSAN*. Ce chapitre contient une rubrique sur la mise à niveau de vCenter Server.

- 2 Si View Composer est installé sur le même hôte, redémarrez le service View Composer.
- 3 Connectez-vous à Horizon Administrator et examinez le tableau de bord pour vérifier que les icônes de vCenter Server et de View Composer sont vertes.

Si l'une des icônes est rouge et que la boîte de dialogue Certificat non valide détecté apparaît, vous devez cliquer sur **Vérifier** et accepter l'empreinte numérique du certificat non approuvé, comme décrit dans « Étape suivante », ou installer un certificat SSL signé par une autorité de certification valide.

Pour plus d'informations sur le remplacement du certificat par défaut pour vCenter Server, consultez le document *Exemples et scénarios VMware vSphere*.

Étape suivante

Pour utiliser un certificat par défaut ou auto-signé à partir de vCenter Server ou de View Composer, reportez-vous à [Accepter l'empreinte numérique d'un certificat TLS par défaut](#).

Si vous avez terminé la mise à niveau des composants du serveur Horizon 7, dans la prochaine fenêtre de maintenance, continuez la mise à niveau d'Horizon 7.

- Si vous mettez aussi à niveau des composants vSphere, reportez-vous à la section [Chapitre 6 Mettre à niveau des hôtes ESXi et leurs machines virtuelles](#).
- Si vous mettez à niveau uniquement des composants Horizon 7, reportez-vous à la section [Mettre à niveau View Agent ou Horizon Agent](#).

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 des certificats TLS, reportez-vous à la section « Configuration de certificats TLS pour des serveurs View Server » dans le document *Installation d'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.

Utilisation des fichiers de modèle d'administration de stratégie de groupe Horizon 7

Horizon 7 fournit plusieurs fichiers de modèle d'administration ADMX de stratégie de groupe propres à un composant. Vous pouvez optimiser et sécuriser des applications et des postes de travail distants en ajoutant les paramètres de stratégie des fichiers de modèle ADMX à un nouveau GPO ou à un GPO existant dans Active Directory.

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 mettre à niveau des stratégies de groupe, utilisez l'Éditeur d'objets de stratégie de groupe sur votre serveur Active Directory pour ajouter la nouvelle version des fichiers de modèle.

Les modèles de fichier ADMX d'Horizon 7 contiennent des stratégies de groupe Configuration d'ordinateur et Configuration d'utilisateur.

- Les stratégies Configuration d'ordinateur définissent des stratégies qui s'appliquent à tous les postes de travail distants, quelle que soit la personne qui se connecte au poste de travail.

- Les stratégies Configuration d'utilisateur définissent des stratégies qui s'appliquent à tous les utilisateurs, quel que soit l'application ou le poste de travail distant auquel ils se connectent. Les stratégies Configuration d'utilisateur remplacent les stratégies Configuration d'ordinateur équivalentes.

Microsoft Windows applique les stratégies au démarrage du poste de travail et lorsque les utilisateurs se connectent.

Mettre à niveau des hôtes ESXi et leurs machines virtuelles

6

La mise à niveau d'hôtes ESXi et de machines virtuelles est l'aspect le plus long de cette phase intermédiaire d'une mise à niveau d'Horizon 7.

Cette procédure offre une vue d'ensemble des tâches que vous devez effectuer lors de la deuxième période de maintenance et des suivantes. Pour effectuer certaines de ces tâches, vous aurez peut-être besoin d'instructions pas à pas disponibles dans le *Guide de mise à niveau de VMware vSphere* et le document *Administration d'Horizon 7*.

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.

Important Le tableau suivant présente les fonctionnalités d'Horizon 7 qui dépendent de versions spécifiques du matériel virtuel et qui, par conséquent, peuvent requérir que la machine virtuelle soit mise à niveau.

Tableau 6-1. Versions du matériel virtuel requises pour des fonctionnalités spécifiques

Fonction	Version de matériel virtuel	Version vSphere correspondante
Format de disque à optimisation d'espace pour les pools de clone lié	9 ou version ultérieure	vSphere 5.1 ou version ultérieure
Banques de données VMware [®] vSAN [®] , première version	10 ou version ultérieure	vSphere 5.5 Update 1 ou version ultérieure
Banques de données VMware vSAN, seconde version	11 ou version ultérieure	vSphere 6.0 ou version ultérieure
Banque de données VMware Virtual Volumes	11 ou version ultérieure	vSphere 6.0 ou version ultérieure
Technologie de snapshot NFS natif (VAAI)	9 ou version ultérieure	vSphere 5.1 ou version ultérieure
Accélération graphique virtuelle partagée	8 ou version ultérieure	vSphere 5.0 ou version ultérieure
Accélération graphique virtuelle dédiée	9 ou version ultérieure	vSphere 5.1 ou version ultérieure
Accélération graphique NVIDIA GRID vGPU	11 ou version ultérieure	vSphere 6.0 ou version ultérieure

Conditions préalables

- Effectuez la procédure décrite dans la section [Mise à niveau de Serveurs de connexion dans un groupe répliqué](#)

- Effectuez les tâches de préparation de la mise à niveau d'ESXi répertoriées dans le *Guide de mise à niveau de VMware vSphere*.

Procédure

1 Mettez à niveau des hôtes ESXi, cluster par cluster.

Pour obtenir des instructions, consultez le *Guide de mise à niveau de VMware vSphere*. Si vos clusters contiennent des banques de données vSAN, reportez-vous également au chapitre sur la mise à niveau du cluster vSAN, dans le document *Administration de VMware vSAN*. Ce chapitre contient une rubrique sur la mise à niveau des hôtes ESXi.

Si vous possédez beaucoup de clusters, cette étape peut nécessiter plusieurs périodes de maintenance pour être réalisée. La mise à niveau des hôtes ESXi peut inclure les tâches suivantes :

- a Utilisez VMware vSphere® vMotion® pour enlever les machines virtuelles de l'hôte ESXi.
- b Mettez l'hôte en mode maintenance.
- c Effectuez la mise à niveau.
- d Utilisez VMotion pour remettre les machines virtuelles sur l'hôte.
- e Effectuez les tâches qui suivent la mise à niveau pour les hôtes ESXi.

Tous les hôtes doivent être membres d'un cluster, comme mentionné dans les conditions préalables.

- 2 Si un hôte mis à niveau ne se reconnecte pas de lui-même à vCenter Server, utilisez vSphere Client pour reconnecter l'hôte à vCenter Server.
- 3 Si vous utilisez View Composer, une fois tous les hôtes ESXi mis à niveau, sur l'hôte vCenter Server, redémarrez le service View Composer.
- 4 (Facultatif) Mettez à niveau VMware® Tools™ et les machines virtuelles sur toutes les machines virtuelles parentes, les modèles de machine virtuelle et les machines virtuelles qui hébergent des composants de serveur Horizon 7, tels que des instances du Serveur de connexion.
 - a Prévoyez un temps d'arrêt, comme décrit dans le *Guide de mise à niveau de VMware vSphere*.
 - b Mettez à jour VMware Tools et mettez à niveau le matériel de machine virtuelle pour les machines virtuelles qui seront utilisées comme sources pour les postes de travail distants.

Pour obtenir des instructions pas à pas si vous prévoyez de ne pas utiliser VMware vSphere® Update Manager™, reportez-vous au chapitre sur la mise à niveau de machines virtuelles du document *VMware vSphere Administration de machines virtuelles*.

Si vous utilisez VMware vSphere Update Manager, vous pouvez mettre à jour VMware Tools, puis la version du matériel virtuel dans le bon ordre pour toutes les machines virtuelles d'un dossier particulier. Consultez le *Guide de mise à niveau de VMware vSphere*.

- 5 (Facultatif) Si vous utilisez des postes de travail de clone complet, sur chaque machine virtuelle, mettez à niveau VMware Tools et le matériel virtuel des machines virtuelles qui seront utilisées comme sources pour les postes de travail distants.

Pour obtenir des instructions pas à pas si vous prévoyez de ne pas utiliser VMware vSphere® Update Manager™, reportez-vous au chapitre sur la mise à niveau de machines virtuelles du document *VMware vSphere Administration de machines virtuelles*.

Si vous utilisez vSphere Update Manager, vous pouvez mettre à jour VMware Tools, puis la version du matériel virtuel dans le bon ordre pour toutes les machines virtuelles d'un dossier particulier. Consultez le *Guide de mise à niveau de VMware vSphere*.

Étape suivante

Mettez à niveau le logiciel agent. Reportez-vous à la section [Mettre à niveau View Agent ou Horizon Agent](#).

Mise à niveau des postes de travail publiés et virtuels

7

Mettez à niveau des postes de travail publiés, des postes de travail virtuels et Horizon Agent, qui s'exécute dans les systèmes d'exploitation de postes de travail virtuels ou publiés et des hôtes RDS Microsoft.

Important Ce chapitre ne couvre pas la mise à niveau d'Horizon Agent sur une machine virtuelle Linux. Pour obtenir des informations à ce sujet, consultez le document *Configuration des postes de travail Horizon 7 for Linux*.

Ce chapitre contient les rubriques suivantes :

- [Exigences liées à la sécurité pour la mise à niveau de postes de travail](#)
- [Mettre à niveau les hôtes RDS qui fournissent des postes de travail basés sur une session](#)
- [Mettre à niveau View Agent ou Horizon Agent](#)
- [Mise à niveau de pools de postes de travail View Composer](#)
- [Mettre à niveau des pools de postes de travail d'Instant Clone](#)

Exigences liées à la sécurité pour la mise à niveau de postes de travail

RC4, SSLv3 et TLSv1.0 sont désactivés par défaut dans les composants Horizon 7. Si vous devez réactiver RC4, SSLv3 ou TLSv1.0 sur un poste de travail virtuel ou publié, consultez la section « Protocoles et chiffrements anciens désactivés dans Horizon 7 » dans le document *Sécurité d'Horizon 7*.

Pour des informations complètes sur les fonctionnalités de sécurité de View Agent, Horizon Agent et Horizon Client, consultez le document *Sécurité d'Horizon Client et d'Horizon Agent*.

Mettre à niveau les hôtes RDS qui fournissent des postes de travail basés sur une session

Sur les hôtes RDS disposant de Windows Server 2008 R2 ou d'un système d'exploitation de version ultérieure, vous pouvez mettre à niveau le logiciel View Agent ou Horizon Agent et modifier les paramètres de pool pour que l'hôte RDS puisse fournir des postes de travail distants et des applications Windows distantes.

Avec VMware Horizon 6.0 et versions ultérieures, vous pouvez utiliser des hôtes Microsoft RDS pour fournir des applications distantes, en plus de postes de travail distants. Avec cette nouvelle fonctionnalité, le nom de la batterie de serveurs précédemment masqué est dorénavant affiché dans Horizon Administrator.

Conditions préalables

- Vérifiez qu'au moins une instance du Serveur de connexion Horizon dans le groupe répliqué a été mise à niveau. Le Serveur de connexion doit d'abord être mis à niveau pour que le mécanisme de couplage JMS sécurisé puisse fonctionner avec Horizon Agent.
- Vérifiez que l'hôte RDS hébergeant actuellement des postes de travail distants exécute Windows Server 2008 R2, Windows Server 2012 ou Windows Server 2012 R2. Windows Server 2008 (services Terminal Server) était pris en charge par les versions antérieures de Horizon 7 mais ne l'est plus dans cette version. Si vous ne disposez pas d'un système d'exploitation Windows Server pris en charge, vous devez effectuer une toute nouvelle installation plutôt qu'une mise à niveau. Pour consulter la liste des systèmes d'exploitation pris en charge, reportez-vous à [Systèmes d'exploitation pris en charge pour Horizon Agent](#).
- Vérifiez que le rôle Hôte RDS est installé dans le système d'exploitation. Consultez la procédure « Installer les services Bureau à distance sur Windows Server 2008 R2 » dans le document *Configuration d'applications et de postes de travail publiés dans Horizon 7*.
- Familiarisez-vous avec la procédure d'exécution du programme d'installation d'Horizon Agent. Consultez la procédure « Installer Horizon Agent sur un hôte des services Bureau à distance » dans *Configuration d'applications et de postes de travail publiés dans Horizon 7*, disponible en cliquant sur le bouton **Aide** dans Horizon Administrator.
- Vérifiez que vous avez fermé votre session sur tous les postes de travail distants et sur toutes les applications distantes.
- Vérifiez que vous possédez un compte d'utilisateur de domaine avec des privilèges d'administration sur les hôtes que vous allez utiliser pour exécuter le programme d'installation et réaliser la mise à niveau.

Procédure

- 1 Dans Horizon Administrator, modifiez les paramètres de pool de postes de travail du pool pour désactiver celui-ci.

Accédez à **Catalogue > Pools de postes de travail**, sélectionnez le pool, puis cliquez sur **Modifier**.

- 2 Sur l'hôte RDS, téléchargez et exécutez le programme d'installation pour la nouvelle version d'Horizon Agent.

Vous pouvez télécharger le programme d'installation sur le site Web de VMware.

- 3 Dans Horizon Administrator, modifiez les paramètres de batterie de serveurs et définissez le protocole d'affichage par défaut sur **PCoIP** ou **VMware Blast**.

Accédez à **Ressources > Batteries de serveurs**, sélectionnez la batterie de serveurs, puis cliquez sur **Modifier**.

Vous pouvez également utiliser un paramètre qui permet à l'utilisateur final de choisir le protocole. Pour utiliser des applications distantes, le protocole doit être PCoIP ou VMware Blast. Les applications distantes ne sont pas prises en charge avec RDP.

- 4 Dans Horizon Administrator, modifiez les paramètres de pool de postes de travail du pool pour activer celui-ci.

Cet hôte peut dorénavant fournir des applications distantes en plus de postes de travail distants. Dans Horizon Administrator, si vous choisissez **Catalogue > Pools de postes de travail**, vous voyez que le type de pool est **Pool de postes de travail RDS**. Si vous choisissez **Ressources > Batteries de serveurs**, un ID de batterie de serveurs s'affiche dans la liste ; il correspond à l'ID du pool.

Étape suivante

Mettez à niveau les clients. Reportez-vous à la section [Chapitre 3 Mettre à niveau l'application cliente](#).

Mettre à niveau View Agent ou Horizon Agent

La stratégie pour mettre le logiciel agent à niveau dépend du type de source de poste de travail.

Note Pour mettre à niveau le système d'exploitation d'un poste de travail de machine virtuelle Windows 8 vers Windows 8.1, vous devez désinstaller Horizon Agent, mettre à niveau le système d'exploitation Windows 8 vers Windows 8.1, puis réinstaller Horizon Agent. Vous pouvez également effectuer une nouvelle installation de Windows 8.1, puis installer Horizon Agent.

Cette procédure offre une vue d'ensemble des tâches que vous devez effectuer pour mettre à niveau le logiciel agent dans des machines virtuelles utilisées comme des sources de postes de travail. Pour effectuer certaines de ces tâches, vous pouvez avoir besoin d'instructions pas à pas disponibles dans l'aide en ligne de vSphere Client ou dans le document *Configuration des postes de travail virtuels dans Horizon 7*, disponible en cliquant sur le bouton **Aide** dans Horizon Administrator. Pour mettre à niveau le logiciel agent sur un hôte des services Terminal Server ou un hôte Microsoft RDS, reportez-vous à la section [Mettre à niveau les hôtes RDS qui fournissent des postes de travail basés sur une session](#). Pour mettre à niveau le logiciel agent sur une machine virtuelle Linux, consultez le document distinct *Configuration des postes de travail Horizon 7 for Linux*.

Si vous prévoyez de déployer des clones instantanés, vous pouvez utiliser cette procédure pour créer une machine virtuelle parente pour un pool de postes de travail de clone instantané. Lorsque vous effectuez la mise à niveau d'Horizon Agent sur une machine virtuelle parente, sélectionnez simplement l'option appropriée pour un pool de postes de travail de clone instantané.

Important Le programme d'installation d'Horizon Agent inclut désormais tous les composants inclus précédemment dans Remote Experience Agent, qui faisait partie de VMware Horizon™ View™ Feature Pack. Pour mettre à niveau les fonctionnalités qui étaient installées avec Remote Experience Agent, il vous suffit d'exécuter le programme d'installation d'Horizon Agent. Ce programme d'installation supprime Remote Experience Agent avant d'effectuer la mise à niveau. Si, pour certaines raisons, vous décidez de supprimer manuellement Remote Experience Agent, assurez-vous de le faire avant d'exécuter le programme d'installation de la nouvelle version d'Horizon Agent.

Conditions préalables

- Vérifiez qu'au moins une instance du Serveur de connexion dans le groupe répliqué a été mise à niveau. Le Serveur de connexion doit d'abord être mis à niveau pour que le mécanisme de couplage JMS sécurisé puisse fonctionner avec Horizon Agent.
- Si vous effectuez la mise à niveau d'hôtes ESXi et de machines virtuelles, effectuez la procédure décrite dans la section [Chapitre 6 Mettre à niveau des hôtes ESXi et leurs machines virtuelles](#).
- Vérifiez que vous possédez un compte d'utilisateur de domaine avec des privilèges d'administration sur les hôtes que vous allez utiliser pour exécuter le programme d'installation et réaliser la mise à niveau.

Procédure

- 1 Si vous prévoyez de déployer des clones instantanés ou des clones liés View Composer, mettez à niveau le logiciel agent sur une machine virtuelle parente et créez un pool de postes de travail à des fins de test.
 - a Téléchargez et exécutez la nouvelle version du programme d'installation d'Horizon Agent sur une machine virtuelle parente.

Vous pouvez télécharger le programme d'installation sur le site Web de VMware.
 - b Créez un petit pool de postes de travail à partir de cette machine virtuelle.
 - c Testez un poste de travail de machine virtuelle du pool de postes de travail pour vérifier que tous les scénarios d'utilisation fonctionnent correctement.

Par exemple, créez un pool de postes de travail qui contient un poste de travail de machine virtuelle et vérifiez que vous pouvez utiliser Horizon Client pour ouvrir une session sur ce poste de travail.

Des instructions pas à pas sur l'exécution du programme d'installation d'Horizon Agent et la création de pools de postes de travail sont incluses dans le document *Configuration des postes de travail virtuels dans Horizon 7*, disponible en cliquant sur le bouton **Aide** dans Horizon Administrator.

Important Si vous mettez à niveau View 5.1.x ou version antérieure, que vous utilisez Sysprep et que vos utilisateurs connecteront des périphériques USB à leurs poste de travail distant, vous devez suivre la procédure décrite dans l'article de la base de connaissances VMware, à l'adresse <http://kb.vmware.com/kb/2051801>. Dans le cas contraire, après la mise à niveau du logiciel agent, la fonctionnalité de redirection USB risque de ne pas fonctionner.

- 2 Sur les autres machines virtuelles parentes et modèles de machine virtuelle, téléchargez et exécutez le programme d'installation de la nouvelle version d'Horizon Agent.

Des instructions pas à pas sur l'exécution du programme d'installation d'Horizon Agent et la création de pools de postes de travail sont incluses dans le document *Configuration des postes de travail virtuels dans Horizon 7*, disponible en cliquant sur le bouton **Aide** dans Horizon Administrator.

- 3 Si vous prévoyez de créer des pools de postes de travail de clone instantané ou de clone lié View Composer, prenez un snapshot de chaque machine virtuelle parente mise à niveau.

Utilisez le nouveau snapshot pour créer un pool de postes de travail de clone instantané ou de clone lié, ou pour recomposer un pool de postes de travail de clone lié existant.

Pour plus d'instructions sur la prise de snapshots, consultez l'aide en ligne de vSphere Client.
- 4 Si vous utilisez des postes de travail de clone complet ou d'autres machines virtuelles que vous avez ajoutées en tant que postes de travail individuels ou en tant que partie d'un pool manuel, mettez à niveau le logiciel agent à l'aide des outils tiers que vous utilisez généralement pour des mises à niveau logicielles.
- 5 Pour les pools Windows 7 et 8 automatisés et manuels qui ne sont pas des pools de clone instantané ou de clone lié, pour utiliser la fonctionnalité de rendu 3D, modifiez le pool et mettez hors tension, puis sous tension les postes de travail de machine virtuelle.

a Configurez les paramètres de pool suivants :

- Définissez le pool pour qu'il utilise le protocole d'affichage PCoIP ou VMware Blast.
- Définissez **Autoriser les utilisateurs à choisir un protocole** sur **Non**.
- Activez la fonction **Convertisseur 3D**.

b Mettez chaque machine virtuelle hors tension puis sous tension de nouveau.

Le redémarrage d'une machine virtuelle, plutôt qu'une mise hors puis sous tension, n'entraîne pas la prise d'effet du paramètre.

- 6 Si vous utilisez des PC physiques ou des machines virtuelles comme hôtes Microsoft RDS, pour fournir des applications ou des postes de travail distants, téléchargez et exécutez le programme d'installation de la nouvelle version d'Horizon Agent sur ces machines.

Vous pouvez télécharger le programme d'installation sur le site Web de VMware.

Important Lorsque vous exécutez le programme d'installation sur l'hôte RDS d'une machine virtuelle, le composant **View Composer Agent** est désélectionné. Ne sélectionnez pas ce composant durant une mise à niveau. Si vous souhaitez utiliser ce composant pour créer une batterie automatisée (il s'agit d'une fonctionnalité mise en place dans Horizon 6 version 6.2), désinstallez la version précédente du logiciel agent avant d'installer la nouvelle version en sélectionnant le composant **View Composer Agent**.

- 7 Si vous utilisez des PC physiques en tant que sources de poste de travail, téléchargez et exécutez le programme d'installation de la nouvelle version d'Horizon Agent sur ces machines physiques.

Vous pouvez télécharger le programme d'installation sur le site Web de VMware.
- 8 Utilisez une instance d'Horizon Client qui n'a pas été mise à niveau pour vérifier que vous pouvez ouvrir une session sur les sources de postes de travail distants mises à niveau avec votre ancien logiciel client.

Étape suivante

Si vous utilisez des pools de postes de travail View Composer, recomposez ou recréez les pools. Reportez-vous à la section [Mise à niveau de pools de postes de travail View Composer](#).

Mettez à jour les clients. Reportez-vous à la section [Chapitre 3Mettre à niveau l'application cliente](#).

Mise à niveau de pools de postes de travail View Composer

Une partie de la phase finale d'une mise à niveau d'Horizon comprend la mise à niveau de pools de postes de travail View Composer.

Pour mettre à niveau les pools créés avec View Composer, vous devez utiliser un snapshot pris après la mise à niveau d'Horizon Agent sur la machine virtuelle parente.

Important Si vous utilisez des clones liés View Composer et que vous voulez utiliser la fonctionnalité de récupération d'espace disponible avec des machines virtuelles vSphere 5.1 et version ultérieure, vous devez configurer certains paramètres dans View LDAP et dans Horizon Administrator, en plus d'effectuer les étapes de cette procédure. Pour voir une liste complète des tâches, reportez-vous à la section [Tâches de mise à niveau de pools de postes de travail pour utiliser la récupération d'espace](#).

Note Si vous mettez également à niveau la version matérielle virtuelle, comme la mise à niveau vers la version matérielle virtuelle 8 ou ultérieure, incluse avec vSphere 5 ou version ultérieure, le snapshot de la machine virtuelle parent mise à niveau est utilisé pour mettre à niveau la version matérielle virtuelle du reste des machines virtuelles dans le pool de clone lié.

Cette mise à niveau, d'une version de matériel virtuel (ou niveau de compatibilité) à une version supérieure, est prise en charge. Toutefois, vous ne pouvez pas recomposer de clones liés sur un matériel avec une version inférieure à la version actuelle. Par exemple, vous ne pouvez pas recomposer des clones avec le matériel version 8 sur une machine virtuelle parente avec le matériel version 7.

Conditions préalables

- Effectuez la procédure décrite dans la section [Mise à niveau de View Composer](#)
- Effectuez la procédure décrite dans la section [Mise à niveau de Serveurs de connexion dans un groupe répliqué](#)
- Si vous effectuez également la mise à niveau d'hôtes ESXi et de machines virtuelles, effectuez la procédure décrite dans la section [Chapitre 6Mettre à niveau des hôtes ESXi et leurs machines virtuelles](#).

Pour obtenir des informations sur les versions de vSphere requises pour diverses nouvelles fonctionnalités, reportez-vous à [Tableau 6-1](#).

- Effectuez la procédure décrite dans la section [Mettre à niveau View Agent ou Horizon Agent](#) pour la mise à niveau de l'agent dans la machine virtuelle parent.

Important Si vous mettez à niveau View 5.1.x ou version antérieure, que vous utilisez Sysprep et que vos utilisateurs connecteront des périphériques USB à leurs poste de travail distant, vous devez suivre la procédure décrite dans l'article de la base de connaissances VMware, à l'adresse <http://kb.vmware.com/kb/2051801>. Dans le cas contraire, après la mise à niveau du logiciel agent, la fonctionnalité de redirection USB risque de ne pas fonctionner.

- Prévoyez soigneusement des fenêtres de maintenance pour que la création et la recomposition des pools de postes de travail ne surchargent pas la baie de stockage et les hôtes ESXi.

Procédure

- 1 Si vous désactivez le provisionnement de nouvelles machines virtuelles en préparation pour la mise à niveau, activez de nouveau le provisionnement.
- 2 Pour activer la fonctionnalité de rendu 3D, modifiez le pool afin de configurer les paramètres suivants :
 - Définissez le pool pour qu'il utilise le protocole d'affichage PCoIP ou VMware Blast.
 - Définissez **Autoriser les utilisateurs à choisir un protocole** sur **Non**.
 - Activez la fonctionnalité **Rendu 3D**.
- 3 Pour activer la fonctionnalité de récupération d'espace disponible avec les machines virtuelles vSphere 5.1, dans la section **Stockage avancé** des paramètres de pool, sélectionnez **Récupérer l'espace disque de machine virtuelle** et définissez le seuil pour la récupération d'espace sur 1 Go.
- 4 Pour activer View Storage Accelerator, disponible avec des machines virtuelles vSphere 5.0 ou version ultérieure, dans la section **Stockage avancé** des paramètres de pool, vérifiez que la case **Utiliser View Storage Accelerator** est cochée.

View Storage Accelerator peut améliorer les performances lors des tempêtes de démarrage et des tempêtes d'E/S d'analyse antivirus en permettant à des hôtes ESXi de mettre en cache des données de disque de machine virtuelle communes.

Important Cette fonctionnalité est activée par défaut. View Storage Accelerator requiert 1 Go de RAM par hôte ESXi.

- 5 Utilisez le snapshot que vous avez créé après la mise à niveau de la machine virtuelle parente pour recomposer des pools de postes de travail.
- 6 Si vous avez modifié le paramètre **Actualiser le disque du système d'exploitation à la fermeture de session** d'un pool sur **Jamais** en préparation pour la mise à niveau, remodifiez le paramètre pour refléter la règle d'actualisation appropriée.
- 7 Si vous avez annulé une opération d'actualisation ou de recomposition pour un pool de postes de travail, replanifiez ces tâches.

Étape suivante

Mettez à niveau les clients. Reportez-vous à la section [Chapitre 3 Mettre à niveau l'application cliente](#).

Effectuez les tâches répertoriées dans la section [Chapitre 9 Tâches postérieures à la mise à niveau pour activer de nouvelles fonctionnalités dans votre configuration d'Horizon](#) qui s'appliquent à votre configuration.

Mettre à niveau des pools de postes de travail d'Instant Clone

Si vous mettez à niveau vCenter Server afin d'utiliser vSphere 6.7, vous devez également mettre à niveau les pools de postes de travail d'Instant Clone.

Conditions préalables

- Effectuez la configuration système requise pour une mise à niveau vers Horizon 7 version 7.5 ou ultérieure.
- Effectuez les procédures décrites dans la section [Mise à niveau du Serveur de connexion VMware Horizon](#).
- Effectuez la procédure décrite dans la section [Mettre à niveau View Agent ou Horizon Agent](#) pour la mise à niveau de l'agent dans la VM parente.
- Remplissez les conditions préalables répertoriées dans le *Guide de mise à niveau de VMware vSphere*, en utilisant la version du guide qui correspond à la version de vSphere vers laquelle vous prévoyez d'effectuer la mise à niveau.

Note Si vous mettez à niveau vCenter Server vers vSphere 6.7, certains ou tous les hôtes ESXi du cluster doivent être mis à niveau vers vSphere 6.7. Sinon, les pools de postes de travail d'Instant Clone ne peuvent pas fonctionner correctement.

- Identifiez les hôtes ESXi que vous prévoyez de mettre à niveau et vérifiez que vous laissez suffisamment d'hôtes en ligne pour les pools de postes de travail existants.

Procédure

- 1 Prenez un snapshot de la VM parente sur laquelle vous mettez à niveau Horizon Agent vers Horizon 7 version 7.5 ou ultérieure. Ce snapshot est l'image maître pour les Instant Clones.
- 2 Définissez le seuil de migration du DRS (Distributed Resource Scheduler) de stockage sur 3 dans le cluster.
- 3 Désactivez les pools de postes de travail d'Instant Clone.
- 4 Mettez à niveau vCenter Server vers vSphere 6.7.

- 5 Pour mettre en mode de maintenance les hôtes que vous prévoyez de mettre à niveau, choisissez l'une des options suivantes.

- Mettez l'hôte directement en mode de maintenance à partir de vSphere Web Client, puis mettez à niveau l'hôte vers vSphere 6.7. Une fois la mise à niveau terminée, utilisez vSphere Web Client pour quitter le mode de maintenance.
- Utilisez l'utilitaire `icmaint.cmd` pour marquer un hôte pour la maintenance avec l'option **ON**. Le fait de marquer un hôte pour la maintenance supprime les images maîtres, qui sont les VM parentes dans vCenter Server à partir de l'hôte ESXi. Mettez l'hôte en mode de maintenance et effectuez la mise à niveau vers vSphere 6.7 ESXi. Une fois la mise à niveau terminée, sortez l'hôte du mode de maintenance. Ensuite, utilisez `icmaint.cmd` pour annuler le marquage de l'hôte pour la maintenance avec l'option **OFF**.

- 6 Activez les pools de postes de travail d'Instant Clone.

- 7 Effectuez une opération d'image de transfert pour chaque pool de postes de travail d'Instant Clone qui utilise le nouveau snapshot.

Seuls les hôtes qui sont mis à niveau vers vSphere ESXi 6.7 sont utilisés pour le provisionnement. Les Instant Clones créés lors de l'opération d'image de transfert peuvent être migrés vers d'autres hôtes qui ne se trouvent pas encore sur vSphere 6.7.

- 8 Vérifiez que tous les hôtes du cluster sont mis à niveau vers vSphere 6.7.

- 9 Si vous mettez la VM parente à niveau à partir d'une version précédente pour qu'elle soit compatible avec ESXi 6.7 et version ultérieure (VM version 14), mettez VMware Tools à niveau sur la VM parente. Vous devez prendre un nouveau snapshot de la VM parente, qui est l'image maître des Instant Clones, et effectuer une opération d'image de transfert sur tous les pools de postes de travail d'Instant Clone qui utilisaient la version précédente de cette image maître.

- 10 Si le commutateur virtuel distribué (vDS) est mis à niveau, mettez sous tension la VM parente pour vérifier qu'il n'y a pas de problème de réseau. Après la mise à niveau d'un vDS, vous devez prendre un nouveau snapshot de la VM parente et effectuer une opération d'image de transfert sur tous les pools de postes de travail d'Instant Clone.

Mettre à niveau le dispositif virtuel Horizon 7 Cloud Connector

8

Effectuez la mise à niveau vers la dernière version du dispositif virtuel Horizon 7 Cloud Connector pour ponter vos espaces Horizon 7 avec les dernières fonctionnalités de VMware Horizon Cloud Service.

Conditions préalables

- Installez et déployez le dispositif virtuel Horizon 7 Cloud Connector. Reportez-vous au document *Installation d'Horizon 7*.
- Vérifiez que le nouveau dispositif virtuel Horizon 7 Cloud Connector et le dispositif virtuel Horizon 7 Cloud Connector existant qui requiert la mise à niveau se trouvent sur le même réseau pour que le nouveau dispositif virtuel puisse établir une communication SSH avec le dispositif virtuel existant.
- Utilisez vSphere Web Client pour prendre un snapshot du dispositif virtuel Horizon 7 Cloud Connector existant.
- Lorsqu'un domaine Active Directory est déjà joint, vérifiez que vous disposez des informations d'identification pour un compte Active Directory dans ce domaine avec des autorisations d'accès.

Procédure

- 1 Dans vSphere Web Client, mettez sous tension le dispositif Horizon 7 Cloud Connector existant.
L'adresse IP de l'interface utilisateur du dispositif Horizon 7 Cloud Connector s'affiche.
- 2 Si vous effectuez la mise à niveau à partir de la version 1.0 du dispositif virtuel Horizon 7 Cloud Connector, connectez-vous en tant qu'utilisateur racine à partir de vCenter Server au dispositif virtuel Horizon 7 Cloud Connector existant et entrez la commande `chage -E -1 -M -1 tomcat8`.

Par exemple, entrez la commande suivante : `root@example.com [~]# chage -E -1 -M -1 tomcat8`

Note Cette étape n'est pas requise pour la version 1.1 et versions ultérieures du dispositif virtuel Horizon 7 Cloud Connector.

- 3 Dans un navigateur Web, entrez l'adresse IP du dispositif virtuel 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. Cette étape vérifie que la connexion d'Horizon Cloud existante a été correctement configurée avec le Serveur de connexion qui est hébergé sur site.

- 4 Déployez la dernière version du dispositif virtuel Horizon 7 Cloud Connector et utilisez vos informations d'identification du compte My VMware pour vous connecter.

Note Si l'environnement associé au compte My VMware dispose d'un domaine Active Directory joint, la fenêtre de connexion Active Directory s'affiche et vous devez vous connecter avec les informations d'identification Active Directory.

- 5 Connectez la dernière version du 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 Cliquez sur **Mettre à niveau** dans la boîte de dialogue.

- 9 Dans le champ **Ancienne adresse de Cloud Connector**, entrez l'adresse IP du dispositif virtuel Horizon 7 Cloud Connector antérieur, puis cliquez sur **Se connecter**.

- 10 Cochez la case pour vérifier l'empreinte numérique de la connexion SSH.

- 11 Cliquez sur **Mettre à niveau**.

L'espace Horizon 7 est correctement mis à niveau et couplé avec VMware Horizon Cloud Service.

Dépanner la mise à niveau du dispositif virtuel Horizon 7 Cloud Connector

La version antérieure du dispositif virtuel Horizon 7 Cloud Connector est désactivée uniquement à la fin du processus de mise à niveau. S'il existe un problème de mise à niveau, vous pouvez restaurer la mise à niveau vers la version antérieure du dispositif virtuel Horizon 7 Cloud Connector.

Note Lorsque vous effectuez des tâches de dépannage, ne déconnectez pas la dernière version déployée du dispositif Horizon 7 Cloud Connector.

Procédure

- 1 Si la mise à niveau échoue et que la version antérieure du dispositif virtuel Horizon 7 Cloud Connector est toujours accessible, vous pouvez continuer à utiliser cette version du dispositif virtuel. Après avoir consulté les fichiers journaux et vérifié les informations de configuration du nouveau dispositif virtuel Horizon 7 Cloud Connector, vous pouvez de nouveau effectuer la tâche de mise à niveau.
- 2 Si la mise à niveau échoue et que la version antérieure du dispositif virtuel Horizon 7 Cloud Connector n'est pas accessible, procédez comme suit :
 - a Éteignez le nouveau dispositif virtuel Horizon 7 Cloud Connector.
 - b Restaurez le dispositif virtuel Horizon 7 Cloud Connector existant au snapshot de dispositif virtuel effectué avant la mise à niveau. Vérifiez que le dispositif virtuel Horizon 7 Cloud Connector est accessible à partir du navigateur Web et qu'il affiche l'état couplé.
 - c Effectuez la tâche de mise à niveau pour déployer à nouveau la dernière version du dispositif Horizon 7 Cloud Connector. Si le problème persiste, contactez le Support VMware.

Tâches postérieures à la mise à niveau pour activer de nouvelles fonctionnalités dans votre configuration d'Horizon

9

Dès que vous avez terminé la mise à niveau des serveurs, des machines virtuelles et du logiciel agent pour les pools de postes de travail et d'applications, vous pouvez configurer votre installation pour tirer parti des avantages de certaines nouvelles fonctionnalités.

Outre les tâches décrites dans les rubriques de ce chapitre, le cas échéant, vous pouvez utiliser Horizon Administrator pour modifier des options de stockage avancées pour des pools de postes de travail et modifier l'étendue du partage de page transparente. Par défaut, par mesure de sécurité, le partage de mémoire n'est pas autorisé entre machines virtuelles sur un hôte ESXi. Pour obtenir plus d'informations, reportez-vous à la rubrique « Modification des paramètres dans un pool de postes de travail existant » du document *Administration d'Horizon 7*.

Ce chapitre contient les rubriques suivantes :

- [Passer le mode de sécurité des messages JMS sur Amélioré](#)
- [Tâches de mise à niveau de pools de postes de travail pour utiliser la récupération d'espace](#)
- [Tâches de mise à niveau si vous utilisez les banques de données VMware vSAN](#)
- [Configurer la page du portail Web de VMware Horizon pour les utilisateurs finaux](#)

Passer le mode de sécurité des messages JMS sur Amélioré

Lorsque vous effectuez une mise à niveau, le paramètre du mode de sécurité des messages JMS existant défini dans la version précédente est conservé. À partir d'Horizon 6 version 6.1, vous pouvez utiliser Horizon Administrator pour passer ce paramètre sur **Amélioré**.

Cette procédure indique comment utiliser Horizon Administrator pour passer le mode de sécurité des messages sur **Amélioré** et surveiller l'avancement du changement pour tous les composants Horizon. Vous pouvez également utiliser l'utilitaire de ligne de commande `vdmutil` pour changer de mode et surveiller le changement. Reportez-vous au document *Administration d'Horizon 7*.

Note Avec Horizon 6 version 6.2 et ultérieures, il est possible d'utiliser les dispositifs Access Point au lieu de serveurs de sécurité Horizon. Access Point utilise un protocole HTTP(S) standard pour les communications avec le Serveur de connexion. JMS, IPsec et AJP13 ne sont pas utilisés.

Pour utiliser des dispositifs Access Point au lieu de serveurs de sécurité Horizon, vous devez mettre à niveau les instances du Serveur de connexion vers la version 6.2 ou une version ultérieure avant d'installer et de configurer les dispositifs Access Point pour qu'ils pointent vers les instances du Serveur de connexion ou l'équilibrage de charge associé aux instances. Pour plus d'informations, consultez le document *Déploiement et configuration d'Unified Access Gateway*.

Conditions préalables

Vérifiez que vous avez mis à niveau toutes les instances du Horizon Connection Server, tous les serveurs de sécurité et tous les postes de travail Horizon vers Horizon 6 version 6.1 ou une version ultérieure. Les composants View antérieurs à Horizon 6 version 6.1 ne peuvent pas communiquer avec une instance du Serveur de connexion 6.1 utilisant le mode Amélioré.

Procédure

- 1 Configurez les règles de pare-feu principal pour permettre aux serveurs de sécurité d'envoyer du trafic JMS sur le port 4002 vers des instances du Serveur de connexion.
- 2 Dans Horizon Administrator, accédez à **Configuration de View > Paramètres généraux**, puis sur l'onglet **Sécurité**, définissez **Mode de sécurité des messages** sur **Amélioré**.
- 3 Redémarrez manuellement le service Composant du bus de message VMware Horizon sur tous les hôtes du Serveur de connexion de l'espace ou redémarrez les instances du Serveur de connexion.

Dès que les services ont redémarré, les instances du Serveur de connexion reconfigurent le mode de sécurité des messages sur tous les postes de travail et serveurs de sécurité pour passer au mode **Amélioré**.

- 4 Pour surveiller l'avancement dans Horizon Administrator, accédez à **Configuration de View > Paramètres généraux**.

Dans l'onglet **Sécurité**, l'élément **État de sécurité amélioré** affiche **Amélioré** lorsque tous les composants ont effectué la transition vers le mode Amélioré.

Lorsque les serveurs communiquent avec les clients, ils configurent ces derniers sur le mode de sécurité des messages amélioré.

Tâches de mise à niveau de pools de postes de travail pour utiliser la récupération d'espace

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. Mettre à niveau des pools pour utiliser cette fonctionnalité implique de modifier des paramètres dans vCenter Server, View LDAP et des paramètres de pool, puis de recomposer le pool.

Note La fonctionnalité de récupération d'espace n'est pas prise en charge si vos postes de travail de machine virtuelle sont hébergés sur des banques de données vSAN ou des banques de données Virtual Volumes.

Même si la fonction de récupération d'espace réduit la quantité d'espace disque utilisée pour une machine virtuelle, elle ne peut récupérer que l'espace qui n'est pas utilisé. Cette fonction ne peut pas récupérer l'espace disque créé par des machines virtuelles qui n'ont pas été optimisées. Pour optimiser une image du système d'exploitation, vous pouvez désactiver les services Windows, tels que le service Indexeur, le service Défragmenteur et les points de restauration. Pour plus de détails, consultez les rubriques « Optimiser les performances du système d'exploitation Windows invité », « Optimiser les performances du système d'exploitation invité Windows 7 et Windows 8 » et « Optimisation de Windows 7 et Windows 8 pour les postes de travail de clone lié » dans *Configuration des postes de travail virtuels dans Horizon 7*.

Important Comme cette procédure implique la recomposition du pool de postes de travail, toutes les modifications apportées par les utilisateurs au disque du système d'exploitation seront perdues.

- 1 Si toutes les instances de vCenter Server et les hôtes ESXi pour le pool ne sont pas à la version VMware vSphere 5.1 ou version ultérieure, mettez-les à niveau vers la version 5.1 ou ultérieure.
Pour obtenir des instructions, consultez le *Guide de mise à niveau de VMware vSphere*.
- 2 Si tous les postes de travail de machine virtuelle dans le pool ne sont pas des machines virtuelles VMware vSphere 5.1 (version matérielle virtuelle 9) ou version ultérieure, mettez-les à niveau.
 - Dans la machine virtuelle parent, mettez à niveau VMware Tools vers la dernière version de VMware vSphere 5.1 ou version ultérieure et mettez à niveau la machine virtuelle vers la dernière version, qui doit être la version matérielle virtuelle 9 ou ultérieure.
Pour obtenir des instructions, consultez le *Guide de mise à niveau de VMware vSphere*.
 - Prenez un snapshot de la machine virtuelle parente. Pour plus d'instructions sur la prise de snapshots, consultez l'aide en ligne de vSphere Client.
 - Utilisez le snapshot de la machine virtuelle parente que vous venez de créer pour recomposer le pool de postes de travail. Pour obtenir des instructions sur la recomposition de pools, cliquez sur le bouton **Aide** dans Horizon Administrator.

La recomposition du pool à partir d'un snapshot d'une machine virtuelle mise à niveau n'est qu'une simple méthode de mise à niveau de toutes les machines virtuelles dans un pool de clone lié. Vous pouvez également mettre à niveau les machines virtuelles une par une.

- 3 Mettez à niveau le format de disque utilisé pour les machines virtuelles.
 - Sur l'hôte du Serveur de connexion, utilisez ADSIEdit pour accéder au groupe de serveurs qui correspond au pool et modifiez la valeur dans le champ **pae-UseSparseFormat** de **0** à **1**.
 - Recomposez le pool de postes de travail.
- 4 Utilisez Horizon Administrator pour modifier les paramètres de vCenter Server, accédez à l'onglet **Stockage** et sélectionnez **Récupérer l'espace disque de machine virtuelle**.

Pour obtenir des instructions sur la modification des paramètres du serveur, cliquez sur le bouton **Aide** dans Horizon Administrator.
- 5 Utilisez Horizon Administrator pour modifier les paramètres du pool, accédez à la section **Stockage avancé**, sélectionnez **Récupérer l'espace disque de machine virtuelle** et définissez le seuil pour la récupération d'espace sur 1 Go.

Tâches de mise à niveau si vous utilisez les banques de données VMware vSAN

À partir de vSphere 5.5 Update 1, vous pouvez utiliser la fonctionnalité vSAN pour le stockage haute performance et la gestion basée sur la stratégie.

Avec vSAN, les disques de stockage physiques connectés localement et disponibles sur un cluster d'hôtes vSphere sont agrégés en une banque de données virtuelle. Vous spécifiez cette banque de données à la création d'un pool de postes de travail, et les différents composants, comme les fichiers, réplicas, données utilisateur et fichiers de système d'exploitation de la machine virtuelle sont placés sur les disques à circuits intégrés (SSD) ou les disques durs à connexion directe (HDD) appropriés.

Horizon 7 définit les exigences de stockage de la machine virtuelle, comme la capacité, les performances et la disponibilité, sous la forme de profils par défaut de stratégie de stockage, en fonction des paramètres de pool utilisés. Le stockage est approvisionné et configuré automatiquement selon les stratégies affectées.

Note La fonctionnalité de récupération d'espace n'est pas prise en charge si vos postes de travail de machine virtuelle sont hébergés sur des banques de données vSAN.

Mettre à niveau une banque de données non-vSAN vers une banque de données vSAN

La mise à niveau de pools pour utiliser les banques de données VMware vSAN implique de modifier un paramètre du pool et de rééquilibrer ce dernier.

Les tâches présentées dans cette procédure décrivent la mise à niveau d'une banque de données non-vSAN vers une banque de données vSAN. La mise à niveau d'une banque de données vSAN sur un cluster vSphere 5.5 ou version antérieure (fonctionnalité de la présentation technique) n'est pas prise en charge.

Important Comme cette procédure implique la recomposition du pool de postes de travail, toutes les modifications apportées par les utilisateurs au disque du système d'exploitation seront perdues.

Conditions préalables

- Vérifiez que tous les hôtes ESXi du cluster utilisés pour le pool sont mis à niveau vers la version 5.5 Update 1 ou ultérieure et qu'ils respectent la configuration système requise de la fonctionnalité vSAN. VMware recommande de procéder à la mise à niveau vers vSphere 6.0 ou version ultérieure, car la fonctionnalité vSAN disponible avec vSphere 6.0 et versions ultérieures contient de nombreuses améliorations de performance par rapport aux fonctionnalités disponibles avec vSphere 5.5 Update 1. Avec vSphere 6.0, cette fonctionnalité dispose également d'une compatibilité matérielle (HCL) élargie.

Pour en savoir plus sur les mises à niveau, reportez-vous à [Chapitre 6 Mettre à niveau des hôtes ESXi et leurs machines virtuelles](#) et au *Guide de mise à niveau de VMware vSphere*. Pour plus d'informations sur les spécifications et les mises à niveau de vSAN, reportez-vous au document *Administration de VMware vSAN*.

- Dans vCenter Server, vérifiez que les privilèges suivants sont ajoutés au rôle Composer :

```
Profile-Driven Storage: All
Folder: Create Folder & Delete Folder
Host: Configuration: Advanced settings
```

Procédure

- 1 Utilisez vCenter Server 5.5 Update 1 ou version ultérieure pour activer vSAN pour le cluster vSphere. Pour plus d'informations, reportez-vous au document *vSphere Storage*.

- 2 Mettez à niveau le pool de postes de travail vers la version la plus récente, tel que décrit dans [Mise à niveau de pools de postes de travail View Composer](#).

Ce processus inclut l'installation de la version la plus récente d'Horizon Agent sur la machine virtuelle parente et la prise d'un snapshot.

- 3 Recomposez le pool sur la banque de données non-vSAN à l'aide du snapshot de la machine virtuelle parente que vous venez de créer.

Pour obtenir des instructions sur la recomposition de pools, cliquez sur le bouton **Aide** dans Horizon Administrator.

- 4 Modifiez les paramètres du pool de postes de travail récemment mis à niveau pour activer le paramètre de pool **Utiliser VMware Virtual SAN**, modifiez la banque de données pour passer d'une banque de données non-vSAN à une banque de données vSAN, et utilisez la commande **Rééquilibrer**.

Pour des instructions sur la modification des paramètres du serveur et l'utilisation de la commande **Rééquilibrer**, cliquez sur le bouton **Aide** dans Horizon Administrator.

Mettre à niveau à partir de la version 1 du format de disque vSAN

Après la mise à niveau de VMware vSphere 5.5 Update 1 vers vSphere 6.0 ou version ultérieure, vous devez également mettre à niveau le format de disque vSAN.

VMware recommande de procéder à la mise à niveau vers vSphere 6.0 ou version ultérieure, car la fonctionnalité vSAN disponible avec vSphere 6.0 et versions ultérieures contient de nombreuses améliorations de performance par rapport aux fonctionnalités disponibles avec vSphere 5.5 Update 1. Avec vSphere 6.0, cette fonctionnalité dispose également d'une compatibilité matérielle (HCL) élargie.

Important Cette procédure décrit un processus de mise à niveau pour vSAN si vous disposez actuellement de pools de postes de travail sur des banques de données vSAN disponibles avec vSphere 5.5 Update 1 ou une version de mise à jour ultérieure. Si vos pools de postes de travail n'utilisent actuellement pas de banque de données vSAN, reportez-vous à la section [Mettre à niveau une banque de données non-vSAN vers une banque de données vSAN](#).

La mise à niveau d'une banque de données VMware vSAN est un processus en plusieurs phases qui inclut la mise à niveau du logiciel vSphere sur chaque hôte ESXi, puis la mise à niveau du format de disque, un groupe de disques à la fois. Un chapitre entier du document *vSphere 6 Administration de VMware vSAN* est consacré au processus de mise à niveau. Les étapes de la procédure suivante décrivent l'ordre des tâches à effectuer au niveau de l'hôte ESXi, dans vCenter Server, et au niveau du pool de postes de travail, dans View Administrator.

Conditions préalables

- Vérifiez que vos pools de postes de travail utilisent View Agent 6.0 ou une version ultérieure. Si vos machines virtuelles utilisent View Agent 5.3.x sur des banques de données vSAN, reportez-vous à la section [Mise à niveau d'Horizon View 5.3.x sur une banque de données vSAN](#).
- Dans vCenter Server, vérifiez que les privilèges suivants sont ajoutés au rôle Composer :

```
Profile-Driven Storage: All
Folder: Create Folder & Delete Folder
Host: Configuration: Advanced settings
```

- Familiarisez-vous avec le processus de mise à niveau de vSAN. Consultez le chapitre sur la mise à niveau de vSAN dans le document *Administration de VMware vSAN*, disponible à l'adresse <https://docs.vmware.com/fr/VMware-vSAN/index.html>.

Procédure

- 1 Mettez à niveau vCenter Server et vos hôtes ESXi vers vSphere 6 ou version ultérieure, de la manière décrite dans le chapitre sur la mise à niveau du cluster vSAN du document *Administration de VMware vSAN*, disponible dans le centre de documentation de vSphere 6.0.

À ce stade, le pool de postes de travail utilise toujours le format de disque 1 de vSAN, et les machines virtuelles et VMware Tools n'ont pas encore été mis à niveau vers la version 11 du matériel virtuel vSphere 6.0.

- 2 Mettez à niveau le pool de postes de travail à la dernière version, de la manière décrite dans [Mettre à niveau View Agent ou Horizon Agent](#) et [Mise à niveau de pools de postes de travail View Composer](#).

Ce processus inclut l'installation de la dernière version d'Horizon Agent sur la machine virtuelle parente, du modèle de machine virtuelle ou des machines virtuelles de clone complet dans le pool. Pour les pools de clone lié, le processus inclut également la prise d'un snapshot et la recomposition du pool.

View Agent 6.1 ou version ultérieure est maintenant installé sur les machines virtuelles du pool de postes de travail, et les machines virtuelles résident toujours sur les banques de données vSAN disponibles avec vSphere 5.5 Update 1. À ce stade, le pool de postes de travail utilise le format de disque 1 de vSAN.

- 3 Mettez à niveau le format de disque vSAN de la version 1 vers la version 2.

Pour obtenir des instructions complètes, reportez-vous à la rubrique « Mise à niveau du format de disque vSAN » du chapitre sur la mise à niveau du document *Administration de VMware vSAN* disponible à l'adresse <https://docs.vmware.com/fr/VMware-vSAN/index.html>.

Vous pouvez utiliser l'outil de ligne de commande RVC pour cette mise à niveau ou vSphere Web Client si vous disposez de vSphere 6 Update 1. Ruby vSphere Console (RVC) est une console de ligne de commande basée sur Ruby pour les hôtes VMware ESXi et vCenter Server. La console RVC est incluse dans les versions Windows et Linux de vCenter Server. Pour obtenir des informations détaillées sur l'utilisation des commandes RVC, reportez-vous au *Guide de référence de la ligne de commande RVC*.

- 4 Dès que les disques sont mis à niveau pour tous les hôtes ESXi du cluster, de la machine virtuelle parente, du modèle de machine virtuelle ou des machines virtuelles de clone complet du pool, exécutez les tâches suivantes dans l'ordre indiqué ci-dessous.

- a Si la machine virtuelle parente se trouve sur une banque de données vSAN, supprimez tous les snapshots.

La machine virtuelle ne peut pas commencer à utiliser le nouveau format de snapshot disponible avec le format de disque 2 de vSAN tant que tous les snapshots précédents basés sur redo log n'ont pas été supprimés. Si la machine virtuelle ne se trouve pas sur une banque de données vSAN, vous n'avez pas besoin de supprimer les snapshots.

- b Mettez à niveau le matériel de la machine virtuelle vers la version 11 et mettez à niveau VMware Tools.

- 5 Pour les pools de clone lié, prenez un nouveau snapshot et recomposez le pool de postes de travail en utilisant le nouveau snapshot.

Le pool de postes de travail utilise maintenant le format de disque 2 de vSAN.

Mise à niveau d'Horizon View 5.3.x sur une banque de données vSAN

Horizon 6.0 introduit de nouvelles stratégies de stockage par défaut pour vSAN. Ces stratégies ne s'appliquent pas automatiquement aux postes de travail de machine virtuelle existants créés sur vSAN par Horizon 7 5.3.x après la mise à niveau du pool de postes de travail.

En outre, lorsque vous mettez à niveau Horizon 7 5.3.x, le paramètre de pool **Utiliser VMware Virtual SAN** ne sera pas automatiquement activé, même si le pool réside dans une banque de données vSAN. Vous disposez des options de mise à niveau suivantes :

- Si vous continuez à utiliser VMware vSphere 5.5 Update 1, après la mise à niveau, continuez à utiliser les stratégies de stockage par défaut qui étaient utilisées avec Horizon 7 5.3.x. Si vous choisissez cette option, modifiez les paramètres de pool pour activer **Utiliser VMware Virtual SAN**.
- Utilisez la procédure décrite dans cette rubrique de sorte que le pool de postes de travail utilise les nouvelles stratégies de stockage par défaut. Cette procédure implique le rééquilibrage du pool de postes de travail dans une banque de données non-vSAN, puis la mise à niveau et le rééquilibrage dans la banque de données vSAN.

Important Les tâches présentées dans cette procédure décrivent la mise à niveau d'un pool de postes de travail Horizon 7 5.3.x à l'aide d'une banque de données vSAN sur un cluster VMware vSphere 5.5 Update 1. La mise à niveau d'une banque de données vSAN sur un cluster VMware vSphere 5.5 ou version antérieure (fonctionnalité tech preview) n'est pas prise en charge.

De plus, comme cette procédure implique la recomposition du pool de postes de travail, toutes les modifications apportées par les utilisateurs finaux au disque du système d'exploitation seront perdues.

Conditions préalables

- Vérifiez que toutes les machines virtuelles du pool sont des machines virtuelles VMware vSphere 5.5 Update 1 ou version ultérieure. VMware recommande de procéder à la mise à niveau vers VMware vSphere 6.0 ou version ultérieure, car la fonctionnalité vSAN disponible avec vSphere 6.0 et versions ultérieures contient de nombreuses améliorations de performance par rapport aux fonctionnalités disponibles avec vSphere 5.5 Update 1. Avec vSphere 6.0, cette fonctionnalité dispose également d'une compatibilité matérielle (HCL) élargie.

Pour en savoir plus sur les mises à niveau, reportez-vous à [Chapitre 6 Mettre à niveau des hôtes ESXi et leurs machines virtuelles](#), ainsi que le *Guide de mise à niveau de VMware vSphere*. Pour plus d'informations sur les spécifications et les mises à niveau de vSAN, reportez-vous au document *Administration de VMware vSAN*.

- Dans vCenter Server, vérifiez que les privilèges suivants sont ajoutés au rôle Composer :

```
Profile-Driven Storage: All
Folder: Create Folder & Delete Folder
Host: Configuration: Advanced settings
```

Procédure

- 1 Modifiez les paramètres du pool de postes de travail afin de passer d'une banque de données vSAN à une banque de données non-vSAN, et utilisez la commande **Rééquilibrer**.

Pour obtenir des instructions sur la modification des paramètres du serveur et l'utilisation de la commande **Rééquilibrer**, cliquez sur le bouton **Aide** dans View Administrator.
- 2 Mettez à niveau le pool de postes de travail vers la version la plus récente, tel que décrit dans [Mise à niveau de pools de postes de travail View Composer](#).

Ce processus inclut l'installation de la version la plus récente d'Horizon Agent sur la machine virtuelle parente et la prise d'un snapshot.
- 3 Recomposez le pool sur la banque de données non-vSAN à l'aide du snapshot de la machine virtuelle parente que vous venez de créer.

Pour obtenir des instructions sur la recomposition de pools, cliquez sur le bouton **Aide** dans View Administrator.
- 4 Modifiez les paramètres du pool de postes de travail récemment mis à niveau afin de passer d'une banque de données non-vSAN à une banque de données vSAN, et utilisez la commande **Rééquilibrer**.

Étape suivante

Si vous avez mis à niveau vos machines virtuelles vers VMware vSphere 6.0, pour procéder à une mise à niveau afin d'utiliser vSAN 2 plutôt que vSAN 1, reportez-vous à la section [Mettre à niveau à partir de la version 1 du format de disque vSAN](#).

Configurer la page du portail Web de VMware Horizon pour les utilisateurs finaux

Vous pouvez configurer cette page Web pour afficher ou masquer l'icône de téléchargement d'Horizon Client ou l'icône de connexion à un poste de travail distant via HTML Access. Vous pouvez également configurer d'autres liens sur cette page.

Par défaut, la page du portail Web affiche à la fois une icône pour télécharger et installer le client Horizon Client natif et une icône pour se connecter via HTML Access. Le lien de téléchargement utilisé est déterminé à partir des valeurs par défaut définies dans le fichier `portal-links-html-access.properties`.

Toutefois, dans certains cas, vous voudrez peut-être que les liens pointent vers un serveur Web interne ou que des versions de client spécifiques puissent être disponibles sur votre propre serveur. Vous pouvez reconfigurer la page du portail pour qu'elle pointe vers une URL de téléchargement différente en modifiant le contenu du fichier `portal-links-html-access.properties`. Si ce fichier n'est pas disponible ou s'il est vide, et que le fichier `oslinks.properties` existe, le fichier `oslinks.properties` est utilisé pour déterminer la valeur de lien du fichier du programme d'installation.

Le fichier `oslinks.properties` est installé dans le dossier *répertoire-installation\VMware\VMware View\Server\broker\webapps\portal\WEB-INF*. Si ce fichier est manquant lors de la session HTML Access, le lien de téléchargement dirigera les utilisateurs vers <https://www.vmware.com/go/viewclients> par défaut. Le fichier contient les valeurs par défaut suivantes :

```
link.download=https://www.vmware.com/go/viewclients
# download Links for particular platforms
link.win32=https://www.vmware.com/go/viewclients#win32
link.win64=https://www.vmware.com/go/viewclients#win64
link.linux32=https://www.vmware.com/go/viewclients#linux32
link.linux64=https://www.vmware.com/go/viewclients#linux64
link.mac=https://www.vmware.com/go/viewclients#mac
link.ios=https://itunes.apple.com/us/app/vmware-view-for-ipad/id417993697
link.android=https://play.google.com/store/apps/details?id=com.vmware.view.client.android
link.chromeos=https://chrome.google.com/webstore/detail/vmware-horizonclient/
pckbpdplfajmgaipljfamclkinbjdnma
link.winmobile=https://www.microsoft.com/en-us/store/p/vmware-horizon-client/9nblggh51p19
```

Vous pouvez créer des liens de programme d'installation pour des systèmes d'exploitation clients spécifiques dans le fichier `portal-links-html-access.properties` ou `oslinks.properties`. Par exemple, si vous accédez à la page de portail depuis un système Mac OS X, le lien du programme d'installation Mac OS X natif s'affiche. Pour les clients Windows ou Linux, vous pouvez créer des liens distincts pour les programmes d'installation 32 et 64 bits.

Important Si vous avez mis à niveau le Serveur de connexion View 5.x ou une version antérieure et que le composant HTML Access n'est pas installé, et si vous aviez précédemment modifié la page du portail pour qu'elle pointe vers votre propre serveur pour télécharger Horizon Client, ces personnalisations peuvent être masquées après l'installation du Serveur de connexion 6.0 ou version ultérieure. Avec Horizon 6 ou version ultérieure, le composant HTML Access est installé automatiquement pendant une mise à niveau du Serveur de connexion.

Si vous avez déjà installé le composant HTML Access séparément de Horizon 7 5.x, toutes les personnalisations que vous avez apportées à la page Web sont conservées. Si le composant HTML Access n'était pas installé, toutes les personnalisations que vous avez apportées sont masquées. Les personnalisations des versions antérieures se situent dans le fichier `portal-links.properties` qui n'est plus utilisé.

Procédure

- 1 Sur l'hôte du Serveur de connexion, ouvrez le fichier `portal-links-html-access.properties` avec un éditeur de texte.

Ce fichier se trouve dans `CommonAppDataFolder\VMware\VDM\portal\portal-links-html-access.properties`. Pour les systèmes d'exploitation Windows Server 2008, le dossier `CommonAppDataFolder` est `C:\ProgramData`. Pour afficher le dossier `C:\ProgramData` dans l'Explorateur Windows, vous devez utiliser la boîte de dialogue Options des dossiers pour afficher les dossiers cachés.

Si le fichier `portal-links-html-access.properties` n'existe pas et que le fichier `oslinks.properties` existe, ouvrez le fichier `<répertoire-installation>\VMware\VMware View\Server\broker\webapps\portal\WEB-INF\oslinks.properties` pour modifier les URL à utiliser pour télécharger des fichiers de programme d'installation spécifiques.

Note Pour Horizon 7 5.x et versions antérieures, les personnalisations se situaient dans le fichier `portal-links.properties` qui se trouve dans le même répertoire `CommonAppDataFolder\VMware\VDM\portal\` que le fichier `portal-links-html-access.properties`.

- 2 Modifiez les propriétés de la configuration pour les définir convenablement.

Par défaut, les icônes du programme d'installation et de HTML Access sont toutes deux activées et un lien pointe vers la page de téléchargement du client sur le site Web de VMware. Pour désactiver une icône, ce qui la supprime de la page Web, définissez la propriété sur `false`.

Note Le fichier `oslinks.properties` ne peut être utilisé que pour configurer les liens vers les fichiers de programme d'installation spécifiques. Il ne prend pas en charge les autres options répertoriées ci-dessous.

Option	Paramètre propriété
Désactiver HTML Access	<code>enable.webclient=false</code> Si cette option est définie sur <code>false</code> alors que l'option <code>enable.download</code> est définie sur <code>true</code> , l'utilisateur est dirigé vers une page Web pour télécharger le programme d'installation natif d'Horizon Client. Si ces deux options sont définies sur <code>false</code> , l'utilisateur obtient le message suivant : « Contactez votre administrateur local pour obtenir des instructions sur l'accès à ce serveur de connexion. »
Désactiver le téléchargement d'Horizon Client	<code>enable.download=false</code> Si cette option est définie sur <code>false</code> alors que l'option <code>enable.webclient</code> est définie sur <code>true</code> , l'utilisateur est dirigé vers la page Web de connexion à HTML Access. Si ces deux options sont définies sur <code>false</code> , l'utilisateur obtient le message suivant : « Contactez votre administrateur local pour obtenir des instructions sur l'accès à ce serveur de connexion. »
Changer l'URL de la page Web pour le téléchargement d'Horizon Client	<code>link.download=https://url-of-web-server</code> Utilisez cette propriété si vous prévoyez de créer votre propre page Web

Option	Paramètre propriété
Créer des liens pour des programmes d'installation spécifiques	<p>Les exemples suivants montrent des URL complètes, mais vous pouvez utiliser des URL relatives si vous placez les fichiers du programme d'installation dans le répertoire downloads, situé sous le répertoire C:\Program Files\VMware\VMware View\Server\broker\webapps\ sur le Serveur de connexion, comme décrit à l'étape suivante.</p> <ul style="list-style-type: none"> ■ Lien général pour télécharger le programme d'installation : <div>link.download=https://server/downloads</div> ■ Programme d'installation de Windows 32 bits : <div>link.win32=https://server/downloads/VMware-Horizon-Client-x86-build#.exe</div> ■ Programme d'installation de Windows 64 bits : <div>link.win64=https://server/downloads/VMware-Horizon-Client-x86_64-build#.exe</div> ■ Programme d'installation de Windows Phone : <div>link.winmobile=https://server/downloads/VMware-Horizon-Client-build#.appx</div> ■ Programme d'installation de Linux 32 bits : <div>link.linux32=https://server/downloads/VMware-Horizon-Client-build#.x86.bundle</div> ■ Programme d'installation de Linux 64 bits : <div>link.linux64=https://server/downloads/VMware-Horizon-Client-build#.x64.bundle</div> ■ Programme d'installation de Mac OS X : <div>link.mac=https://server/downloads/VMware-Horizon-Client-build#.dmg</div> ■ Programme d'installation d'iOS : <div>link.ios=https://server/downloads/VMware-Horizon-Client-iPhoneOS-build#.ipa</div> ■ Programme d'installation d'Android : <div>link.android=https://server/downloads/VMware-Horizon-Client-AndroidOS-build#.apk</div>

Option	Paramètre propriété
	<ul style="list-style-type: none"> Programme d'installation de Chrome OS : <div> <pre>link.chromeos=https://server/downloads/VMware-Horizon-Client-ChromeOS-build#.apk</pre> </div>
Changer l'URL du lien de l'aide sur la page de connexion	<pre>link.help</pre> <p>Par défaut, ce lien pointe vers un système d'aide hébergé sur le site Web de VMware. Le lien de l'aide apparaît en bas de la page de connexion.</p>

- Pour permettre aux utilisateurs de télécharger les programmes d'installation depuis un emplacement différent du site Web VMware, placez les fichiers des programmes d'installation sur le serveur HTTP où ils résideront.

Cet emplacement doit correspondre aux URL que vous avez spécifiées dans le fichier `portal-links-html-access.properties` ou `oslinks.properties` à l'étape précédente. Par exemple, pour placer les fichiers dans un répertoire `downloads` sur l'hôte du Serveur de connexion, utilisez le chemin suivant :

```
C:\Program Files\VMware\VMware View\Server\broker\webapps\downloads
```

Les liens vers les fichiers du programme d'installation pourront alors utiliser des URL relatives au format `/downloads/client-installer-file-name`.

- Redémarrez le service du composant Web Horizon.

Mise à niveau séparée de composants vSphere dans un environnement Horizon 7

10

Si vous mettez à niveau des composants vSphere séparément des composants Horizon 7, vous devez sauvegarder certaines données Horizon 7 et réinstaller des logiciels Horizon 7.

Plutôt que d'effectuer une mise à niveau intégrée des composants Horizon 7 et vSphere, vous pouvez commencer par mettre à niveau tous les composants Horizon 7, puis les composants vSphere, ou l'inverse. Vous pouvez aussi ne mettre à niveau que les composants vSphere lorsqu'une nouvelle version ou une mise à jour de vSphere est proposée.

Lorsque vous mettez à niveau des composants vSphere séparément des composants Horizon 7, vous devez effectuer les tâches supplémentaires suivantes :

- 1 Avant de mettre à niveau vCenter Server, sauvegardez les bases de données vCenter Server et View Composer.
- 2 Avant de mettre à niveau vCenter Server, sauvegardez la base de données Horizon LDAP à partir d'une instance du Horizon Connection Server à l'aide de l'utilitaire `vdmexport.exe`.

Pour obtenir des instructions, reportez-vous au document *Administration d'Horizon 7*. Si vous possédez plusieurs instances du Serveur de connexion dans un groupe répliqué, vous devez exporter les données à partir d'une seule instance.

- 3 Si vous utilisez View Composer, après avoir mis à niveau tous les hôtes ESXi gérés par une instance vCenter Server particulière, redémarrez le service View Composer sur cet hôte.
- 4 Une fois que VMware Tools a été mis à niveau sur les machines virtuelles utilisées en tant que postes de travail distants, réinstallez Horizon Agent.

La réinstallation d'Horizon Agent garantit que les pilotes de la machine virtuelle restent compatibles avec les autres composants Horizon 7.

Des instructions pas à pas pour l'exécution du programme d'installation d'Horizon Agent apparaissent dans le document *Configuration des postes de travail virtuels dans Horizon 7*.