

Afficher les mises à niveau

VMware Horizon 6.0

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

FR-001476-00

vmware[®]

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

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

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

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

docfeedback@vmware.com

Copyright © 2009–2014 VMware, Inc. Tous droits réservés. [Copyright et informations sur les marques.](#)

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

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

Table des matières

Mises à niveau de View	5	
1	Matrice de compatibilité des composants View	7
2	Présentation de la mise à niveau d' View	11
3	Configuration requise pour les mises à niveau	13
	Exigences de View Composer	13
	Exigences de Serveur de connexion View	16
	Exigences de View Administrator	18
	Exigences d' Horizon Client	19
	Systèmes d'exploitation pris en charge pour View Agent	19
4	Préparation de la mise à niveau d' View	21
	Préparation de vCenter Server et de View Composer pour une mise à niveau	21
	Préparation de Serveur de connexion View pour une mise à niveau	23
	Se préparer à mettre à niveau ou à réinstaller un serveur de sécurité	24
5	Mise à niveau des composants d' View Server	27
	Mise à niveau de View Composer	28
	Mise à niveau de Serveurs de connexion View dans un groupe répliqué	37
	Mise à niveau du serveur de sécurité View	43
	Mettre à niveau vCenter Server	44
	Utilisation des fichiers de modèle d'administration de stratégie de groupe View	45
6	Mettre à niveau des hôtes ESXi et leurs machines virtuelles	47
7	Mise à niveau des postes de travail distants et d' Horizon Client	49
	Mettre à niveau les hôtes RDS qui fournissent des postes de travail basés sur une session	49
	Mise à niveau de View Agent	50
	Mise à niveau de pools de postes de travail View Composer	53
	Tâches de mise à niveau de pools de postes de travail pour utiliser la récupération d'espace	54
	Tâches de mise à niveau des pools de postes de travail pour utiliser une banque de données Virtual SAN	55
	Mettre à niveau l'application cliente	58
	Configurer la page du portail Web de VMware Horizon pour les utilisateurs finaux	59
8	Application de correctifs View	63
	Appliquer un correctif pour View Composer	63
	Appliquer un correctif pour le Serveur de connexion View	64
	Appliquer un correctif pour View Agent	65

Appliquer un correctif à Horizon Client 66

9 Mise à niveau séparée de composants vSphere dans un environnement View 69

Index 71

Mises à niveau de View

Mises à niveau de View fournit des instructions pour la mise à niveau de Horizon View 5.x (incluant 5.0.1, 5.1.3, 5.2, 5.3 et 5.3.1) vers VMware Horizon™ avec View™ 6.0. Vous pouvez également utiliser ce guide lorsque vous effectuez la mise à niveau vers des versions de maintenance et de correctif View.

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'View.

Pour les versions de correctif d'View, reportez-vous à la section [Chapitre 8, « Application de correctifs View »](#), page 63.

Public cible

Ce guide est destiné à toute personne devant effectuer une mise à niveau vers cette dernière version d'View. 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.

Matrice de compatibilité des composants View

1

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

La compatibilité du serveur de connexion View avec View Agent est limitée à l'interopérabilité lors d'une mise à niveau du serveur de connexion View. Vous devez mettre View Agents à niveau dès que possible pour correspondre à la version de Serveur de connexion View qui les gère.

Les tableaux suivants répertorient les composants d'View et indiquent s'ils sont compatibles avec d'autres composants dont la version est différente. Pour plus d'informations sur la compatibilité avec vSphere, reportez-vous à la matrice d'interopérabilité des produits VMware à l'adresse http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Tableau 1-1. Matrice de compatibilité pour VMware Horizon avec des composants View 6.0 et Horizon View 5.3.x

	Serveur de connexion 5.3.x	Serveur de sécurité 5.3.x (PCoIP et RDP)	View Composer 5.3	View Agent 5.3.x	View Client (Windows) 5.x
Serveur de connexion 6.0	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 6.0 (PCoIP et RDP)	Non	S/O	Non	Uniquement lors des mises à niveau	Oui
View Composer 6.0	Uniquement lors des mises à niveau	Uniquement lors des mises à niveau	S/O	Uniquement lors des mises à niveau	S/O
View Agent 6.0	Uniquement lors des mises à niveau	Non	Non	S/O	Uniquement lors des mises à niveau
Horizon Client 3.0	Oui	Oui	Oui	Oui	S/O

Tableau 1-2. Matrice de compatibilité pour VMware Horizon avec des composants View 6.0 et Horizon View 5.2.x

	Serveur de connexion 5.2.x	Serveur de sécurité 5.2.x (PCoIP et RDP)	View Composer 5.2	View Agent 5.2.x	View Client (Windows) 5.x
Serveur de connexion 6.0	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 6.0 (PCoIP et RDP)	Non	S/O	Non	Uniquement lors des mises à niveau	Oui
View Composer 6.0	Uniquement lors des mises à niveau	Uniquement lors des mises à niveau	S/O	Uniquement lors des mises à niveau	S/O
View Agent 6.0	Uniquement lors des mises à niveau	Non	Non	S/O	Uniquement lors des mises à niveau
Horizon Client 3.0	Oui	Oui	Oui	Oui	S/O

Tableau 1-3. Matrice de compatibilité pour VMware Horizon avec des composants View 6.0 et Horizon View 5.1.x

	Serveur de connexion 5.1.3	Serveur de sécurité 5.1.3 (PCoIP et RDP)	View Composer 3.0	View Agent 5.1.3	View Client (Windows) 5.1.x
Serveur de connexion 6.0	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 6.0 (PCoIP et RDP)	Non	S/O	Non	Uniquement lors des mises à niveau	Oui
View Composer 6.0	Uniquement lors des mises à niveau	Uniquement lors des mises à niveau	S/O	Uniquement lors des mises à niveau	S/O
View Agent 6.0	Uniquement lors des mises à niveau	Non	Non	S/O	Uniquement lors des mises à niveau
Horizon Client 3.0	Oui	Oui	Oui	Oui	S/O

Tableau 1-4. Matrice de compatibilité pour VMware Horizon avec des composants View 6.0 et Horizon View 5.0.1

	Serveur de connexion 5.0.1	Serveur de sécurité 5.0.1 (PCoIP et RDP)	View Composer 2.7	View Agent 5.0.1	View Client (Windows) 5.0.x
Serveur de connexion 6.0	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 6.0 (PCoIP et RDP)	Non	S/O	Non	Uniquement lors des mises à niveau	Oui
View Composer 6.0	Uniquement lors des mises à niveau	Uniquement lors des mises à niveau	S/O	Uniquement lors des mises à niveau	S/O

Tableau 1-4. Matrice de compatibilité pour VMware Horizon avec des composants View 6.0 et Horizon View 5.0.1 (suite)

	Serveur de connexion 5.0.1	Serveur de sécurité 5.0.1 (PCoIP et RDP)	View Composer 2.7	View Agent 5.0.1	View Client (Windows) 5.0.x
View Agent 6.0	Non	Non	Non	S/O	Uniquement lors des mises à niveau
Horizon Client 3.0	Serveur de connexion 5.0.1 uniquement	Oui	Oui	Oui	S/O

Même si les versions récentes de View Client et Horizon Client peuvent fonctionner avec Serveur de connexion View 5.0.0, les améliorations de sécurité et la vérification des certificats introduites avec View 5.1 ne sont disponibles qu'avec Serveur de connexion View 5.0.1 et version ultérieure.



AVERTISSEMENT Pendant une mise à niveau, View 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 View continuent d'exécuter la version précédente. Vous pouvez exécuter ces opérations uniquement lorsque toutes les instances de Serveur de connexion View et de View Composer ont été mises à niveau vers la dernière version.

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

Présentation de la mise à niveau d'View

2

La mise à niveau du déploiement d'View 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 VMware View® Composer™ avant celle de Serveur de connexion View et des autres serveurs View.

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 l'utilisation de VMware® Mirage™, inclus avec VMware Horizon 6.0. Pour plus d'informations, reportez-vous à View Notes de mise à jour, accessible à l'adresse https://www.vmware.com/support/pubs/view_pubs.html.

Pendant une mise à niveau, View 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 View continuent d'exécuter la version précédente. Vous pouvez exécuter ces opérations uniquement lorsque toutes les instances du Serveur de connexion View 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.

REMARQUE Cette présentation concerne les mises à niveau pour des versions majeures, mineures et de maintenance. Pour plus d'informations sur les correctifs, reportez-vous à la section [Chapitre 8, « Application de correctifs View »](#), page 63.

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

- 1 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 »](#), page 21.

Pour plus d'informations sur les versions d'View compatibles avec les versions de vCenter Server et d'ESXi, consultez la matrice d'interopérabilité des produits VMware à l'adresse http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
- 2 Sur les machines physiques ou virtuelles qui hébergent des instances de Serveur de connexion View, faites des sauvegardes et enregistrez divers paramètres de configuration et système. Reportez-vous à la section [« Préparation de Serveur de connexion View pour une mise à niveau »](#), page 23.
- 3 Si vous utilisez des serveurs de sécurité, effectuez les tâches de la section [« Se préparer à mettre à niveau ou à réinstaller un serveur de sécurité »](#), page 24

- 4 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](#) », page 28.
- 5 Mettez le Serveur de connexion View à niveau sur l'hôte existant ou migrez vers une nouvelle machine. Reportez-vous à la section « [Mise à niveau de Serveurs de connexion View dans un groupe répliqué](#) », page 37.

IMPORTANT Dès qu'une instance du Serveur de connexion View 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 View 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, mettez-les à niveau. Reportez-vous à la section « [Mise à niveau du serveur de sécurité View](#) », page 43.
- 7 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 View](#) », page 45.
- 8 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](#) », page 44.
- 9 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 »](#), page 47.
- 10 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](#) », page 49
- 11 Mettez à niveau le logiciel Horizon[™] 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 « [Mise à niveau de View Agent](#) », page 50.
- 12 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](#) », page 53.
- 13 Mettez à niveau le logiciel Horizon Client qui s'exécute sur des périphériques clients d'utilisateurs finaux. Reportez-vous à la section « [Mettre à niveau l'application cliente](#) », page 58.

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.

Configuration requise pour les mises à niveau

3

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

Ce chapitre aborde les rubriques suivantes :

- [« Exigences de View Composer », page 13](#)
- [« Exigences de Serveur de connexion View », page 16](#)
- [« Exigences de View Administrator », page 18](#)
- [« Exigences d'Horizon Client », page 19](#)
- [« Systèmes d'exploitation pris en charge pour View Agent », page 19](#)

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

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

Si vous prévoyez d'installer View Composer sur une machine physique ou virtuelle autre que vCenter Server, reportez-vous à [« Exigences matérielles de View Composer autonome », page 14](#).

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 3-2. 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 utiliser une adresse IP statique.

Exigences de base de données pour View Composer

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

Si une instance du serveur de base de données existe déjà pour vCenter Server, View Composer peut utiliser cette instance existante s'il s'agit d'une version répertoriée dans [Tableau 3-3](#). Par exemple, View Composer peut utiliser l'instance Microsoft SQL Server fournie avec vCenter Server. Si aucune instance du serveur de base de données n'existe, vous devez en installer une.

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

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

Le tableau suivant répertorie les serveurs de base de données pris en charge et leurs versions. Pour la liste complète des versions de base de données prises en charge avec vCenter Server, reportez-vous aux matrices d'interopérabilité des produits VMware à l'adresse

http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Les versions de vCenter Server répertoriées dans les titres de colonne de tableau sont générales. Pour les versions de mise à jour spécifiques prises en charge de chaque version de vCenter Server, reportez-vous aux matrices d'interopérabilité des produits VMware à l'adresse

http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Tableau 3-3. Serveurs de base de données pris en charge pour View Composer

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

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 SSL 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 SSL, mais vous devez configurer le certificat séparément pour chaque composant.

Pour plus d'informations sur les exigences des certificats de sécurité, consultez « Configuration de certificats SSL pour serveurs View Server » dans le guide *Installation de View*.

- Les certificats pour les serveurs vCenter Server, View Composer et View doivent inclure des listes de révocation de certificat (CRL). Pour plus d'informations, reportez-vous à « Configuration de la vérification de révocation de certificat sur des certificats de serveur » dans le guide *Installation de View*.
- Vérifiez qu'aucune application exécutée sur l'ordinateur View Composer n'utilise de bibliothèques Windows SSL qui requièrent la version 2 de SSL (SSLv2) fournie via le package de sécurité Microsoft Secure Channel (Schannel). Le programme d'installation de View Composer désactive SSLv2 sur Microsoft Schannel. Des applications telles que Tomcat, qui utilise Java SSL, ou Apache, qui utilise OpenSSL, ne sont pas affectées par cette contrainte.
- Pour 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 « Désactiver les suites de chiffrement faible sur View Composer Server » dans le guide *Installation de View*.

Exigences de Serveur de connexion View

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

Exigences matérielles de Serveur de connexion View

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

Tableau 3-4. Exigences matérielles de Serveur de connexion View

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

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

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

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

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

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

Tableau 3-5. Prise en charge de systèmes d'exploitation pour le Serveur de connexion View

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

Exigences de mise à niveau pour le Serveur de connexion View

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

- Serveur de connexion View 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 de Serveur de connexion View doit disposer de privilèges administratifs sur l'hôte de Serveur de connexion View. L'administrateur de Serveur de connexion View doit disposer d'informations d'identification administratives pour vCenter Server.
- Lorsque vous exécutez le programme d'installation, vous autorisez un compte d'administrateur View. Vous pouvez spécifier le groupe d'administrateurs local ou un compte d'utilisateur ou de groupe de domaine. View affecte des droits d'administration de View complets, y compris le droit d'installer des instances répliquées du serveur de connexion View, à ce compte uniquement. Si vous spécifiez un utilisateur ou un groupe de domaine, vous devez créer le compte dans Active Directory avant d'exécuter le programme d'installation.
- Lorsque vous sauvegardez Serveur de connexion View, la configuration de View LDAP est exportée sous forme de données LDIF cryptées. Pour restaurer la configuration de View de sauvegarde cryptée, vous devez fournir le mot de passe de récupération de données. Le mot de passe doit contenir entre 1 et 128 caractères.

Exigences liées à la sécurité

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

En outre, les clients mis à jour attendent des informations sur le certificat du serveur à communiquer dans le cadre de négociation SSL 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 « Configuration de certificats SSL pour serveurs View Server » dans le guide *Installation de View*. Reportez-vous également au document *Scénarios de configuration de connexions SSL à View*, qui décrit la configuration de serveurs intermédiaires effectuant des tâches comme le rééquilibrage de charge et le déchargement des connexions SSL.

REMARQUE Si vos serveurs d'origine ont déjà des certificats SSL signés par une autorité de certification, lors de la mise à niveau, View 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 View 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 guide *Installation de View*.

IMPORTANT Si votre entreprise utilise des paramètres proxy pour l'accès Internet, vous devez peut-être configurer vos hôtes de Serveur de connexion View 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 Serveur de connexion View. Pour plus d'informations, consultez « Dépannage de la vérification de la révocation des certificats de View Server » dans le guide *Administration de View*.

- Si vous prévoyez de coupler un serveur de sécurité avec cette instance du serveur de connexion View, vérifiez que le Pare-feu Windows avec sécurité avancée est défini sur **activé** dans les profils actifs. Il vous est recommandé de régler ce paramètre sur **activé** pour tous les profils. Par défaut, des règles IPsec régissent les connexions entre le serveur de sécurité et le serveur de connexion View et requièrent que le Pare-feu Windows avec sécurité avancée soit activé.
- Si votre topologie de réseau inclut un pare-feu entre un serveur de sécurité et une instance du serveur de connexion View, vous devez configurer le pare-feu pour qu'il prenne en charge IPsec. Consultez le document *Installation de View*.

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

Exigences de logiciel de virtualisation pour le serveur de connexion View

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

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

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

Exigences de View Administrator

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

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

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

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

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

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

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

Exigences d' Horizon Client

Horizon Client s'exécute sur de nombreux types de périphériques : postes de travail et ordinateurs portables Windows, Mac et Linux ; clients légers et zéro Linux ; tablettes et téléphones. Tous ces périphériques ont des exigences spécifiques.

Pour plus d'informations sur les exigences de système d'exploitation, les exigences matérielles et les exigences de navigateur d'un périphérique client de type spécifique, rendez-vous sur https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html et consultez le document pour ce type de périphérique client.

IMPORTANT Les fonctions disponibles pour les périphériques de client léger et les clients zéro sont déterminées par le fournisseur, le modèle et la configuration qu'une entreprise choisit d'utiliser. Pour plus d'informations sur les fournisseurs et les modèles de périphériques clients légers et zéro, reportez-vous au [Guide de compatibilité VMware](#), disponible sur le site Web de VMware.

Systèmes d'exploitation pris en charge pour View Agent

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

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

Tableau 3-6. Systèmes d'exploitation pour postes de travail distants de clone lié ou de clone complet

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

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

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

Tableau 3-7. Systèmes d'exploitation pour hôtes RDS, fournissant des applications ou des postes de travail distants

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

Préparation de la mise à niveau d'View

4

Avant de commencer le processus de mise à niveau, vous devez revoir les exigences système de la nouvelle version, sauvegarder des bases de données, prendre des snapshots de machines virtuelles qui hébergent des composants de serveur et fournir des paramètres de configuration.

Ce chapitre aborde les rubriques suivantes :

- [« Préparation de vCenter Server et de View Composer pour une mise à niveau », page 21](#)
- [« Préparation de Serveur de connexion View pour une mise à niveau », page 23](#)
- [« Se préparer à mettre à niveau ou à réinstaller un serveur de sécurité », page 24](#)

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'View 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 », page 15.](#)
- 3 Si vous mettez à niveau View 5.0.x ou une version antérieure, vérifiez que le serveur sur lequel vCenter Server est installé dispose d'un certificat de serveur SSL signé par une autorité de certification CA, installé et configuré. Après la mise à niveau du Serveur de connexion View, 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 View Administrator, et un message indique que vCenter Server n'est pas disponible. Pour plus d'informations sur le remplacement du certificat par défaut pour vCenter Server, reportez-vous au document *vSphere Exemples et scénarios*. Ce problème ne se produit pas si vous mettez à niveau View 5.1 ou une version ultérieure.
- 4 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™.

- 5 Si le nom de l'ordinateur comporte plus de 15 caractères, raccourcissez-le à 15 caractères ou moins.
- 6 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.
- 7 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.
- 8 Vérifiez que la base de données est compatible avec la nouvelle version de View Composer.
View Composer prend en charge un sous-réseau des serveurs de base de données compatibles avec vCenter Server. Si vous utilisez déjà vCenter Server avec un serveur de base de données qui n'est pas pris en charge par View Composer, continuez à utiliser ce serveur de base de données pour vCenter Server et installez un serveur de base de données distinct à utiliser pour les événements des bases de données View Composer et View.
- 9 Faites une copie du dossier qui contient des certificats SSL.
Ce dossier est situé dans %ALLUSERSPROFILE%\Application Data\VMware\VMware VirtualCenter.
- 10 Renseignez l'adresse IP et le nom du système de la machine sur laquelle vCenter Server est installé.
- 11 Pour tous les pools de postes de travail de clone lié, utilisez View Administrator pour désactiver l'approvisionnement 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.
- 12 Si des pools de poste de travail sont définis pour actualiser le disque du système d'exploitation à la fermeture de session, utilisez View Administrator pour modifier le paramètre **Poste de travail/Pools** pour ce pool et définissez **Actualiser le disque du système d'exploitation 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.
- 13 Si un pool de postes de travail est programmé pour une opération d'actualisation ou de recomposition, utilisez View Administrator pour 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 Si vous mettez à niveau View 5.0.x ou une version antérieure, vérifiez que le serveur sur lequel View Composer est installé dispose d'un certificat de serveur SSL signé par une autorité de certification, installé et configuré. Après la mise à niveau de Serveur de connexion View, si View Composer n'utilise pas de certificat signé par une autorité de certification, le certificat auto-signé par défaut est affiché comme étant non valide dans View Administrator, et un message indique que View Composer n'est pas disponible. Pour plus d'informations sur le remplacement du certificat par défaut pour View Composer, reportez-vous à la rubrique « Configuration de certificats SSL pour des serveurs View Server » dans le document *Installation de View*. Vous devez exécuter la commande `SviConfig RelaceCertificate`. Ce problème ne se produit pas si vous mettez à niveau View 5.1 ou une version ultérieure.
- 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](#) », page 15.

- 3 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.
- 4 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.
- 5 Vérifiez que la base de données est compatible avec la nouvelle version de View Composer.
View Composer prend en charge un sous-réseau des serveurs de base de données compatibles avec vCenter Server. Si vous utilisez déjà vCenter Server avec un serveur de base de données qui n'est pas pris en charge par View Composer, continuez à utiliser ce serveur de base de données pour vCenter Server et installez un serveur de base de données distinct à utiliser pour les événements des bases de données View Composer et View.
- 6 Faites une copie du dossier qui contient des certificats SSL.
Ce dossier est situé dans %ALLUSERSPROFILE%\Application Data\VMware\VMware VirtualCenter.
- 7 Renseignez l'adresse IP et le nom du système de la machine sur laquelle vCenter Server est installé.
- 8 Pour tous les pools de postes de travail de clone lié, utilisez View Administrator pour désactiver l'approvisionnement 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.
- 9 Si des pools de poste de travail sont définis pour actualiser le disque du système d'exploitation à la fermeture de session, utilisez View Administrator pour modifier le paramètre **Poste de travail/Pools** pour ce pool et définissez **Actualiser le disque du système d'exploitation 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.
- 10 Si un pool de postes de travail est programmé pour une opération d'actualisation ou de recomposition, utilisez View Administrator pour annuler ces tâches.

Préparation de Serveur de connexion View pour une mise à niveau

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

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

Reportez-vous à la section « [Exigences de Serveur de connexion View](#) », page 16.

- Si le Serveur de connexion View est installé sur une machine virtuelle, prenez un snapshot de la machine virtuelle. Si vous possédez un groupe répliqué d'instances de Serveur de connexion View, prenez un snapshot d'une seule instance de Serveur de connexion View.

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 de Serveur de connexion View 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.

- Si votre déploiement utilise actuellement la fonctionnalité Mode local, demandez aux utilisateurs finaux de vérifier sur leurs postes de travail en mode local ou utilisez View Administrator pour restaurer les postes de travail en mode local afin qu'aucun poste de travail ne soit marqué comme emprunté dans View Administrator.

IMPORTANT Si l'un des postes de travail en mode Local est emprunté au moment où vous exécutez le programme d'installation de Serveur de connexion View pour installer la mise à niveau, celle-ci échouera.

- Si votre déploiement utilise actuellement la fonctionnalité Mode local, ouvrez View Administrator, accédez à **Configuration de View > Serveurs** et supprimez toutes les instances de Serveur de transfert.
- Ouvrez View Administrator et renseignez tous les paramètres généraux et les paramètres des postes de travail et des pools : sections Pools et Postes de travail dans l'arborescence Inventaire, et section Paramètres généraux dans l'arborescence Configuration de View.

Par exemple, prenez une capture d'écran des paramètres applicables. Si vous possédez plusieurs instances de Serveur de connexion View dans un groupe répliqué, vous devez fournir les paramètres pour une seule instance.

- Utilisez l'utilitaire `vdmexport.exe` pour sauvegarder la base de données LDAP.
Pour plus d'instructions, consultez le guide d'administration de votre version actuelle du document *Administration de View*. Si vous possédez plusieurs instances de Serveur de connexion View dans un groupe répliqué, vous devez exporter les données à partir d'une seule instance.
- Renseignez l'adresse IP et le nom de système de la machine sur laquelle le Serveur de connexion View 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 de Serveur de connexion View, et si c'est le cas, fournissez leurs noms et leurs emplacements.
- Si vous utilisez des équilibres de charge pour le Serveur de connexion View, fournissez les paramètres de configuration des équilibres de charge.

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

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

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

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

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

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

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

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



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

Procédure

- 1 Dans View Administrator, cliquez sur **Configuration de View > Serveurs**.
- 2 Sous l'onglet **Serveurs de sécurité**, sélectionnez un serveur de sécurité et cliquez sur **Plus de commandes > Préparer la mise à niveau ou la réinstallation**.

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

- 3 Cliquez sur **OK**.

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

Mise à niveau des composants d'View Server

5

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

REMARQUE La fonctionnalité Mode local d'Horizon Client a été supprimée et les instances du Serveur de transfert View ne sont plus requises. À la place de la fonctionnalité Mode local, VMware recommande d'utiliser Mirage, qui est inclus avec VMware Horizon 6. Pour plus d'informations, reportez-vous aux Notes de mise à jour d'View, accessibles à l'adresse https://www.vmware.com/support/pubs/view_pubs.html.

Pendant une mise à niveau, View 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 View continuent d'exécuter la version précédente. Vous pouvez exécuter ces opérations uniquement lorsque toutes les instances du Serveur de connexion View et de View Composer ont été mises à niveau.

Pour les versions de correctif d'View, reportez-vous à la section [Chapitre 8, « Application de correctifs View »](#), page 63.

Ce chapitre aborde les rubriques suivantes :

- [« Mise à niveau de View Composer »](#), page 28
- [« Mise à niveau de Serveurs de connexion View dans un groupe répliqué »](#), page 37
- [« Mise à niveau du serveur de sécurité View »](#), page 43
- [« Mettre à niveau vCenter Server »](#), page 44
- [« Utilisation des fichiers de modèle d'administration de stratégie de groupe View »](#), page 45

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 View ne sont pas mis à niveau.

IMPORTANT Si votre version actuelle de View Composer est installée sur un ordinateur avec un système d'exploitation Windows Server 2003, consultez la procédure intitulée « Migrer manuellement View Composer vers la nouvelle machine » dans le document *Mise à niveau de VMware View 4.6*. Après avoir migré View Composer 2.6 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.

Pour migrer un système View Composer déjà mis à niveau vers une autre machine physique ou virtuelle, reportez-vous à « [Migrer View Composer vers une autre machine](#) », page 32.

Prérequis

- Déterminez quand effectuer cette procédure. Choisissez une période de maintenance de poste de travail disponible. Prévoyez 15 à 30 minutes pour chaque instance.
- Effectuez les tâches répertoriées dans la section « [Préparation de mises à niveau de View Composer uniquement](#) », page 22
- Vérifiez que le serveur sur lequel View Composer 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 View, si View Composer n'utilise pas de certificat signé par une autorité de certification, le certificat auto-signé par défaut est affiché comme étant non valide dans View 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 View*.

- 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.

Suivant

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](#) », page 29.

Lors de la fenêtre de maintenance suivante, continuez la mise à niveau d'View. Reportez-vous à la section « [Mise à niveau de Serveurs de connexion View dans un groupe répliqué](#) », page 37.

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 View 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.

Prérequis

- 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 -dsnnname=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.

Suivant

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](#) », page 31.

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](#) », page 30

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.

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

Code	Description
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. REMARQUE Un poste de travail supprimé peut sembler exister dans View 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 View. 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. Par exemple, si View Composer 2.6, inclus avec View 4.6, est installé sur un système d'exploitation Windows Server 2003, consultez la procédure intitulée « Migrer manuellement View Composer vers la nouvelle machine » dans le document *Mises à niveau de VMware View 4.6*. Après avoir migré View Composer 2.6 vers un système disposant d'un système d'exploitation Windows Server qui est pris en charge pour cette mise à jour, vous pouvez effectuer une mise à niveau sur place vers la dernière version de View Composer.

- [Conseils sur la migration de View Composer](#) page 33

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](#) page 33

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](#) page 35

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](#) page 36

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](#) page 36

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.

REMARQUE 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.

Prérequis

- Familiarisez-vous avec les exigences de migration de View Composer. Reportez-vous à la section « [Conseils sur la migration de View Composer](#) », page 33.

- 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](#) », page 36 et « [Migrer le conteneur de clés RSA vers le nouveau service View Composer](#) », page 36.
- Familiarisez-vous avec l'installation du service VMware Horizon View Composer. Consultez la section « Installation de View Composer » dans le document *Installation de View*.
- Familiarisez-vous avec la configuration d'un certificat SSL pour View Composer. Consultez « Configuration de certificats SSL pour des serveurs View Server » dans le document *Installation de View*.
- Familiarisez-vous avec la configuration de View Composer dans View Administrator. Consultez les rubriques sur la configuration des paramètres de View Composer et des domaines View Composer dans le document *Administration de View*.

Procédure

- 1 Désactivez le provisionnement de machine virtuelle dans l'instance de vCenter Server associée au service VMware Horizon View Composer.
 - a Dans View 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 View Administrator, configurez les nouveaux paramètres de View Composer.
 - a Dans View 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.

Prérequis

- Familiarisez-vous avec l'installation du service VMware Horizon View Composer. Consultez la section « Installation de View Composer » dans le document *Installation de View*.
- Familiarisez-vous avec la configuration d'un certificat SSL pour View Composer. Consultez « Configuration de certificats SSL pour des serveurs View Server » dans le document *Installation de View*.
- Familiarisez-vous avec les étapes de suppression de View Composer de View Administrator. Consultez la rubrique sur la suppression de View Composer de View Administrator dans le document *Administration de View*.

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 View Administrator. Consultez les rubriques sur la configuration des paramètres de View Composer et des domaines View Composer dans le document *Administration de View*.

Procédure

- 1 Dans View Administrator, supprimez View Composer de View 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 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.
- 5 Dans View Administrator, configurez les nouveaux paramètres de View Composer.
 - a Dans View 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.

Prérequis

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.

Suivant

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](#) », page 36.

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.

Prérequis

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](#) », page 36.

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.

Suivant

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 de View*.

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](#) », page 33.

Mise à niveau de Serveurs de connexion View dans un groupe répliqué

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.

Pour utiliser les nouvelles fonctions de la dernière version d'View, vous devez effectuer la mise à niveau. Pour voir une liste des nouvelles fonctions incluses dans la dernière version, consultez les notes de mise à jour.

REMARQUE 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 de Serveur de connexion View sur une machine différente](#) », page 41.

Prérequis

- 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 de Serveur de connexion View 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](#) », page 28. Après avoir effectué la mise à niveau de Serveur de connexion View, vous devez ajouter View Composer à l'aide de View Administrator.
- Familiarisez-vous avec les exigences liées à la sécurité d'View et vérifiez que ces exigences sont respectées. Reportez-vous à la section « [Exigences de mise à niveau pour le Serveur de connexion View](#) », page 16. 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 View, 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 View Administrator, et un message indique que vCenter Server n'est pas disponible.
- Effectuez les tâches répertoriées dans la section « [Préparation de Serveur de connexion View pour une mise à niveau](#) », page 23

IMPORTANT Si l'un des postes de travail en mode Local est emprunté au moment où vous exécutez le programme d'installation de Serveur de connexion View pour installer la mise à niveau, celle-ci échouera.

- Vérifiez que vous possédez une licence pour la nouvelle version.
- 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 les instructions pour l'utiliser à partir du document *Administration de View* pour votre version actuelle de View. Vous utiliserez cet utilitaire pour sauvegarder la base de données View LDAP dans le cadre de la procédure de mise à niveau.
- Si vous utilisez des serveurs de sécurité, familiarisez-vous avec les instructions sur l'exécution du programme d'installation pour créer un serveur de sécurité qui utilise le nouveau mécanisme de couplage de serveur de sécurité. Consultez le document *Installation de View* pour votre version actuelle de View.

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

Procédure

- 1 Arrêtez le service appelé service Serveur de connexion VMware Horizon View sur toutes les instances de Serveur de connexion dans le groupe.

N'arrêtez pas le service VMwareVDMDS. Le service VMwareVDMDS doit être exécuté pour que la base de données View LDAP puisse être mise à niveau.

- 2 Sur l'hôte de l'une des instances de Serveur de connexion View dans le groupe, exécutez le programme d'installation de la nouvelle version de Serveur de connexion View.

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.

- 3 Vérifiez que le service Serveur de connexion VMware Horizon View redémarre lorsque l'assistant du programme d'installation se ferme.
- 4 Vérifiez que vous pouvez ouvrir une session sur le Serveur de connexion View, et cliquez sur **À propos de** dans View Administrator pour vérifier que la nouvelle version est utilisée.
- 5 Accédez à **Configuration de View > Licence produit et utilisation**, cliquez sur **Modifier la licence**, entrez la clé de licence de VMware Horizon et cliquez sur **OK**.
- 6 Vérifiez que vous pouvez ouvrir une session sur un poste de travail distant.
- 7 Arrêtez de nouveau le service de Serveur de connexion View.
- 8 Répétez de [Étape 1](#) à [Étape 7](#) pour mettre à niveau chaque instance de Serveur de connexion View du groupe.

IMPORTANT Si vous ne mettez pas à niveau toutes les instances du serveur de connexion View dans un groupe répliqué, les indicateurs d'intégrité dans le tableau de bord View 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 Une fois que tous les serveurs dans le groupe sont mis à niveau, démarrez le service de Serveur de connexion View sur tous les serveurs.
- 10 Utilisez l'utilitaire `vdmexport.exe` pour sauvegarder la base de données View LDAP mise à niveau.
Si vous possédez plusieurs instances de Serveur de connexion View dans un groupe répliqué, vous devez exporter les données à partir d'une seule instance.
- 11 Vérifiez ou, si nécessaire, modifiez le numéro de port utilisé pour View Composer.
 - a Modifiez la configuration de l'instance de vCenter Server et assurez-vous que le port de View Composer est défini sur 18443.

Le numéro de port doit correspondre au numéro de port spécifié au cours de la mise à niveau de View Composer.
 - b Fournissez le mot de passe vCenter Server.
 - c Cochez la case **Activer View Composer** et cliquez sur **OK**.
- 12 Ouvrez une session sur View 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, reportez-vous au document *Exemples et scénarios VMware vSphere*.

Suivant

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 SSL par défaut](#) », page 40.

En cas d'échec de la mise à niveau sur une ou plusieurs instances de Serveur de connexion View, reportez-vous à la section « [Créer un groupe répliqué après avoir rétabli un snapshot du serveur de connexion View](#) », page 42

Si la mise à niveau est réussie, effectuez la mise à niveau des autres composants de View server. Si vous utilisez des serveurs de sécurité, reportez-vous à la section « [Mise à niveau du serveur de sécurité View](#) », page 43

Si vous réinstallez Serveur de connexion View 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.

Accepter l'empreinte numérique d'un certificat SSL par défaut

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

Si une instance de vCenter Server ou de View Composer est configurée avec un certificat signé par une autorité de certification, et si le certificat racine est approuvé par le Serveur de connexion View, vous n'avez pas à accepter l'empreinte du certificat. Aucune action n'est requise.

Si vous remplacez un certificat par défaut par un certificat signé par une autorité de certification, mais que Serveur de connexion View n'approuve pas le certificat racine, vous devez déterminer si vous acceptez l'empreinte numérique de certificat. Une empreinte numérique est un hachage cryptographique d'un certificat. L'empreinte numérique est utilisée pour déterminer rapidement si un certificat présenté est le même qu'un autre certificat, tel que le certificat qui a été accepté précédemment.

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

Pour plus d'informations sur la configuration des certificats SSL, consultez la section « Configuration de certificats SSL pour des serveurs View Server » dans le document *Installation de View*.

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

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

REMARQUE Vous devez également accepter une empreinte de certificat lorsque vous mettez à niveau une version antérieure et lorsqu'un certificat de vCenter Server ou de View Composer n'est pas approuvé, ou si vous remplacez un certificat approuvé par un certificat non approuvé.

Sur le tableau de bord de View Administrator, l'icône de vCenter Server ou de View Composer devient rouge et la boîte de dialogue Certificat non valide détecté s'affiche. Vous devez cliquer sur **Vérifier** et suivre la procédure indiquée ici.

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

Procédure

- 1 Lorsque View Administrator affiche la boîte de dialogue Certificat non valide détecté, cliquez sur **Afficher le certificat**.
- 2 Examinez l'empreinte numérique de certificat dans la fenêtre Informations sur le certificat.

- 3 Vérifiez l'empreinte de certificat qui a été configurée pour l'instance de vCenter Server ou de View Composer.
 - a Sur l'hôte de vCenter Server ou de View Composer, démarrez le composant logiciel enfichable MMC et ouvrez le magasin de certificats Windows.
 - b Accédez au certificat de vCenter Server ou de View Composer.
 - c Cliquez sur l'onglet Détails du certificat pour afficher l'empreinte numérique de certificat.

De la même façon, vérifiez l'empreinte de certificat d'un authentificateur SAML. Le cas échéant, exécutez les étapes précédentes sur l'hôte de l'authentificateur SAML.
- 4 Vérifiez que l'empreinte dans la fenêtre Informations sur le certificat correspond à l'empreinte de l'instance de vCenter Server ou de View Composer.
- De la même façon, vérifiez que les empreintes correspondent pour un authentificateur SAML.
- 5 Déterminez si vous acceptez l'empreinte numérique de certificat.

Option	Description
Les empreintes numériques correspondent.	Cliquez sur Accepter pour utiliser le certificat par défaut.
Les empreintes numériques ne correspondent pas.	Cliquez sur Refuser . Corrigez les certificats incompatibles. Par exemple, vous avez peut-être fourni une adresse IP incorrecte pour vCenter Server ou View Composer.

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

Dans le cadre de votre mise à niveau, vous pouvez migrer le Serveur de connexion View vers une nouvelle machine. Par exemple, si vous avez Serveur de connexion View 4.6.x sur une machine Windows 2003 Server 32 bits, vous pouvez migrer vers une machine Windows Server 2008 R2 64 bits.

Prérequis

- Mettez à niveau au moins une instance de Serveur de connexion View existante vers la version la plus récente. Reportez-vous à la section « [Mise à niveau de Serveurs de connexion View dans un groupe répliqué](#) », page 37. 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 de Serveur de connexion View. Reportez-vous aux sections « [Systèmes d'exploitation pris en charge pour le Serveur de connexion View](#) », page 16 et « [Exigences matérielles de Serveur de connexion View](#) », page 16.
- Familiarisez-vous avec les exigences liées à la sécurité d'View et vérifiez que ces exigences sont respectées. Reportez-vous à la section « [Exigences de mise à niveau pour le Serveur de connexion View](#) », page 16.
- 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. Consultez le document *Installation de View*. 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 de Serveur de connexion View est exécutée et accessible pour la nouvelle machine sur laquelle vous prévoyez d'installer le Serveur de connexion View.

Lorsque vous installez le Serveur de connexion View sur le nouvel hôte, vous pointerez vers cette instance existante.

- 2 Sur la nouvelle machine, installez une instance répliquée de Serveur de connexion View.

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 View de l'ancien hôte en utilisant l'utilitaire **Ajout/Suppression de programmes** de Windows.

- 4 Dans View Administrator, accédez à l'onglet **Configuration de View > Serveurs > Serveurs de connexion** et déterminez si l'instance de Serveur de connexion View qui a été désinstallée continue de figurer dans la liste.

- 5 Si l'instance désinstallée de Serveur de connexion View apparaît toujours dans la liste, utilisez une commande `vdmadmin` pour la supprimer.

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

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

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

Suivant

Effectuez la mise à niveau des autres composants de View Server.

Si vous réinstallez Serveur de connexion View 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 View

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 View, vous devez désinstaller les autres instances du serveur de connexion View dans le groupe et recréer le groupe répliqué.

Si vous rétablissez le snapshot d'une machine virtuelle de serveur de connexion View, 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 View LDAP.

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

Prérequis

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

Procédure

- 1 Sur toutes les instances du serveur de connexion View hormis celle choisie comme nouvelle instance du serveur de connexion View standard, désinstallez le serveur de connexion View 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 View 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 View, exécutez le programme d'installation du serveur de connexion View, 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 View.

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

Mise à niveau du serveur de sécurité View

Après avoir mis à niveau le serveur de connexion View, vous pouvez mettre à niveau les serveurs de sécurité qui sont couplés avec lui.

Prérequis

- 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 avez mis à niveau le serveur de connexion View. Pour plus d'informations, reportez-vous à la section « [Mise à niveau de Serveurs de connexion View dans un groupe répliqué](#) », page 37.
- Vérifiez que la machine virtuelle ou physique sur laquelle le serveur de sécurité actuel est installé satisfait les exigences système.

Reportez-vous à la section « [Exigences de Serveur de connexion View](#) », page 16.

- Familiarisez-vous avec les exigences liées à la sécurité d'View et vérifiez que ces exigences sont respectées. Reportez-vous à la section « [Exigences de mise à niveau pour le Serveur de connexion View](#) », page 16. 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 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.
- Si vous n'avez pas configuré de mot de passe de couplage de serveur de sécurité, utilisez la dernière version de View Administrator pour le faire. Le programme d'installation vous invitera à fournir ce mot de passe au cours de l'installation. Reportez-vous à la rubrique intitulée « Configurer un mot de passe de couplage de serveur de sécurité » dans le document *Installation de View*.
- Si vous effectuez la mise à niveau d'un serveur de sécurité View 5.1 ou version ultérieure, supprimez les règles IPsec existantes pour le serveur de sécurité. Reportez-vous à la section « [Se préparer à mettre à niveau ou à réinstaller un serveur de sécurité](#) », page 24.

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

Procédure

- 1 Exécutez le programme d'installation pour la dernière version de Serveur de connexion View.
 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.
- 2 Quand l'assistant du programme d'installation a terminé, vérifiez que le service du serveur de sécurité VMware Horizon View a démarré.
- 3 Ouvrez une session sur View Administrator, sélectionnez le serveur de sécurité dans le tableau de bord et vérifiez que le serveur de sécurité est maintenant à la dernière version.
- 4 Vérifiez que vous pouvez ouvrir une session sur un poste de travail distant.
- 5 Dans View 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.

Suivant

Mettez à niveau les autres composants de View Server, par exemple vCenter Server. Reportez-vous à la section [Chapitre 5, « Mise à niveau des composants d'View Server »](#), page 27.

Si vous avez terminé la mise à niveau des composants de View Server, dans la fenêtre de maintenance suivante, continuez la mise à niveau d'View.

- 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 »](#), page 47.
- Si vous mettez à niveau uniquement des composants View, reportez-vous à la section [« Mise à niveau de View Agent »](#), page 50.

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 View Server. Avant de mettre à niveau vCenter Server, vous devez sauvegarder certaines données de View. Après la mise à niveau, si View Composer est exécuté sur le même serveur, vous devez redémarrer le service View Composer.

Prérequis

- 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 View à l'aide de l'utilitaire `vdmexport.exe`.

Pour obtenir des instructions, reportez-vous au document *Administration de View*. Si vous possédez plusieurs instances de Serveur de connexion View 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](#) », page 21.
- 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 View, 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 View 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.

Procédure

- 1 Mettez à niveau vCenter Server de la manière décrite dans le *Guide de mise à niveau de VMware vSphere*.
- 2 Si View Composer est installé sur le même hôte, redémarrez le service View Composer.
- 3 Ouvrez une session sur View 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, reportez-vous au document *Exemples et scénarios VMware vSphere*.

Suivant

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 SSL par défaut](#) », page 40.

Si vous avez terminé la mise à niveau des composants de View Server, dans la fenêtre de maintenance suivante, continuez la mise à niveau d'View.

- 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 »](#), page 47.
- Si vous mettez à niveau uniquement des composants View, reportez-vous à la section « [Mise à niveau de View Agent](#) », page 50.

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

View fournit plusieurs fichiers de modèle d'administration (ADM et 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 de ces fichiers de modèle ADM et ADMX à un nouveau GPO ou à un GPO existant dans Active Directory.

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

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

Les fichiers de modèle ADM et ADMX de View 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'View.

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 de View*.

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

IMPORTANT Pour utiliser la fonctionnalité de format de disque à optimisation d'espace pour les pools de clone lié, vous devez mettre à niveau vCenter Server, les hôtes ESXi, les machines virtuelles et le logiciel VMware Tools dans les machines virtuelles vers VMware vSphere 5.1 ou version ultérieure.

Pour utiliser la fonctionnalité VMware[®] Virtual SAN[™], vous devez procéder à une mise à niveau vers vSphere 5.5 Update 1 ou version ultérieure.

Prérequis

- Effectuez la procédure décrite dans la section « [Mise à niveau de Serveurs de connexion View dans un groupe répliqué](#) », page 37
- 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 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 parents, les modèles de machine virtuelle et les machines virtuelles qui hébergent des composants de serveur View, tels que des instances de Serveur de connexion View.
 - a Prévoyez le 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 utiliser la fonctionnalité de rendu 3D Windows 7, vous devez mettre à niveau le matériel de machine virtuelle vers la version 8 ou version ultérieure.

Pour utiliser la fonctionnalité de format de disque à optimisation d'espace, vous devez mettre à niveau le matériel de machine virtuelle vers la version 9 ou version ultérieure. Cette fonction concerne les pools de clone lié.

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. Reportez-vous au *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 utiliser la fonctionnalité de rendu 3D Windows 7, vous devez mettre à niveau le matériel de machine virtuelle vers la version 8 ou version ultérieure.

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. Reportez-vous au *Guide de mise à niveau de VMware vSphere*.

Suivant

Mettez View Agent à niveau. Reportez-vous à la section « [Mise à niveau de View Agent](#) », page 50.

Mise à niveau des postes de travail distants et d' Horizon Client

7

Les composants de poste de travail distant et client que vous pouvez mettre à niveau comprennent Horizon Client pour les plates-formes de postes de travail et de clients mobiles prises en charge, des clients légers fournis par des partenaires de VMware et View Agent, qui s'exécute dans les systèmes d'exploitation de postes de travail distants et les hôtes Microsoft RDS.

Ce chapitre aborde les rubriques suivantes :

- [« Mettre à niveau les hôtes RDS qui fournissent des postes de travail basés sur une session », page 49](#)
- [« Mise à niveau de View Agent », page 50](#)
- [« Mise à niveau de pools de postes de travail View Composer », page 53](#)
- [« Tâches de mise à niveau de pools de postes de travail pour utiliser la récupération d'espace », page 54](#)
- [« Tâches de mise à niveau des pools de postes de travail pour utiliser une banque de données Virtual SAN », page 55](#)
- [« Mettre à niveau l'application cliente », page 58](#)
- [« Configurer la page du portail Web de VMware Horizon pour les utilisateurs finaux », page 59](#)

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 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, 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 caché est dorénavant affiché dans View Administrator.

Prérequis

- Vérifiez qu'au moins une instance de Serveur de connexion View dans le groupe répliqué a été mise à niveau. Serveur de connexion View doit d'abord être mis à niveau pour que le mécanisme de couplage JMS sécurisé puisse fonctionner avec View Agent.
- Vérifiez que l'hôte RDS hébergeant actuellement les postes de travail distants exécute Windows Server 2008 R2. Windows Server 2008 (services Terminal Server) était pris en charge par les versions antérieures de View mais le n'est plus dans cette version. Si vous n'utilisez pas Windows Server 2008 R2, vous devez effectuer une 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 View Agent », page 19](#).

- Vérifiez que le rôle Hôte RDS est installé dans le système d'exploitation. Reportez-vous à la procédure « Installer les services Bureau à distance sur Windows Server 2008 R2 » dans le document *Configuration de pools de postes de travail et d'applications dans View*.
- 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 View 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 Windows Server 2008 R2 RDS, téléchargez et exécutez le programme d'installation pour la nouvelle version de View Agent.

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

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

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.

- 4 Dans View 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 View 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**, vous voyez un ID de batterie de serveurs dans la liste qui correspond à l'ID du pool.

Suivant

Mettez à niveau les clients. Reportez-vous à la section « [Mettre à niveau l'application cliente](#) », page 58.

Mise à niveau de View Agent

La stratégie pour mettre View Agent à niveau dépend du type de source de postes de travail.

REMARQUE 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 View Agent, mettre à niveau le système d'exploitation de Windows 8 vers Windows 8.1, puis réinstaller View Agent. Vous pouvez également effectuer une nouvelle installation de Windows 8.1 et réinstaller View Agent.

Cette procédure offre une vue d'ensemble des tâches que vous devez effectuer pour mettre à niveau View 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 de pools de postes de travail et d'applications de VMware ViewView*, disponible en cliquant sur le bouton **Aide** dans View Administrator. Pour mettre à niveau View Agent sur un hôte des services Terminal Server ou un hôte Microsoft RDS, reportez-vous à « [Mettre à niveau les hôtes RDS qui fournissent des postes de travail basés sur une session](#) », page 49.

IMPORTANT Le programme d'installation de View 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 de View 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 de View Agent.

Prérequis

- Vérifiez qu'au moins une instance de Serveur de connexion View dans le groupe répliqué a été mise à niveau. Serveur de connexion View doit d'abord être mis à niveau pour que le mécanisme de couplage JMS sécurisé puisse fonctionner avec View 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 »](#), page 47.
- 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 utilisez View Composer, mettez à niveau View 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 de View 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 de clone lié 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 pour l'exécution du programme d'installation de View Agent et la création de pools de postes de travail s'affichent dans *Configuration de pools de postes de travail et d'applications dans View*, disponible en cliquant sur le bouton **Aide** dans View 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 vers View Agent 6.0, la fonctionnalité 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 de View Agent.

Des instructions pas à pas pour l'exécution du programme d'installation de View Agent et la création de pools de postes de travail s'affichent dans *Configuration de pools de postes de travail et d'applications dans View*, disponible en cliquant sur le bouton **Aide** dans View Administrator.
- 3 Si vous utilisez View Composer, prenez un snapshot de chaque machine virtuelle parente mise à niveau que vous utilisez pour créer des pools de postes de travail de clone lié.

Vous utilisez le nouveau snapshot pour recomposer toutes les machines virtuelles dans le pool.

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 View 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 lié, pour utiliser la fonctionnalité de rendu 3D, modifiez le pool, puis mettez hors et sous tension les postes de travail de machine virtuelle.
 - a Configurez les paramètres de pool suivants :
 - Réglez le pool pour qu'il utilise le protocole d'affichage PCoIP.
 - Définissez **Autoriser les utilisateurs à choisir un protocole** sur **Non**.
 - Activez la fonctionnalité **Rendu 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 en tant que sources de poste de travail, téléchargez et exécutez le programme d'installation de la nouvelle version de View Agent sur ces machines physiques.

Vous pouvez télécharger le programme d'installation sur le site Web de VMware.
- 7 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.

Suivant

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](#) », page 53.

Mettez à jour les clients. Reportez-vous à la section « [Mettre à niveau l'application cliente](#) », page 58.

Mise à niveau de pools de postes de travail View Composer

Une partie de la phase finale d'une mise à niveau d'View 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 de View 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 View 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](#) », page 54.

REMARQUE 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.

Prérequis

- Effectuez la procédure décrite dans la section « [Mise à niveau de View Composer](#) », page 28
- Effectuez la procédure décrite dans la section « [Mise à niveau de Serveurs de connexion View dans un groupe répliqué](#) », page 37
- Si vous effectuez également 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 »](#), page 47.

Pour utiliser la fonctionnalité de rendu 3D, vous devez mettre à niveau le matériel virtuel vers la version 8 ou ultérieure sur les machines virtuelles Windows 7 et 8.

Pour utiliser la fonctionnalité de format de disque à optimisation d'espace, vous devez mettre à jour vCenter Server, les hôtes ESXi, les machines virtuelles et le logiciel VMware Tools des machines virtuelles vers VMware vSphere 5.1 ou version ultérieure. Cela signifie que les machines virtuelles doivent utiliser la version matérielle virtuelle 9 ou supérieure.

- Effectuez la procédure décrite dans la section « [Mise à niveau de View Agent](#) », page 50 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 vers View Agent 6.0, la fonctionnalité Redirection USB risque de ne pas fonctionner.

- Prévoyez soigneusement des fenêtres de maintenance pour que la création et la recombinaison 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 les pools composés de postes de travail Windows 7 ou 8, pour activer la fonctionnalité de rendu 3D, modifiez le pool afin de configurer les paramètres suivants :

- Réglez le pool pour qu'il utilise le protocole d'affichage PCoIP.
- Définissez **Autoriser les utilisateurs à choisir un protocole** sur **Non**.
- Activez la fonctionnalité **Rendu 3D**.

Cette fonctionnalité est disponible pour les postes de travail Windows 7 et 8 qui utilisent la version matérielle virtuelle 8 ou version ultérieure, disponible avec vSphere 5 ou version ultérieure.

- 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 5.0 et version ultérieure 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.

Suivant

Mettez à niveau les clients. Reportez-vous à la section « [Mettre à niveau l'application cliente](#) », page 58.

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

À partir de vSphere 5.1, View crée des machines virtuelles de clone lié dans un format de disque efficace qui permet à des hôtes ESXi de récupérer l'espace disque inutilisé dans les clones liés. 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.

REMARQUE 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 Virtual SAN.

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 la documentation *Configuration de pools de postes de travail et d'applicationsView*.

IMPORTANT Comme cette procédure implique la reconstitution 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 reconstituer le pool de postes de travail. Pour des instructions sur la reconstitution de pools, cliquez sur le bouton **Aide** dans View Administrator.

La reconstitution 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 de Serveur de connexion View, 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.
 - Reconstituez le pool de postes de travail.
- 4 Utilisez View Administrator pour modifier les paramètres de vCenter Server, accédez à l'onglet **Stockage** et sélectionnez **Récupérer l'espace disque de machine virtuelle**.
Pour des instructions sur la modification des paramètres du serveur, cliquez sur le bouton **Aide** dans View Administrator.
- 5 Utilisez View 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 des pools de postes de travail pour utiliser une banque de données Virtual SAN

En commençant par vSphere 5.5 Update 1, vous pouvez utiliser la fonctionnalité Virtual SAN pour le stockage haute performance et la gestion basée sur la stratégie. La mise à niveau de pools pour utiliser cette fonctionnalité implique de modifier un paramètre du pool et de rééquilibrer ce dernier.

Avec Virtual SAN, les disques de stockage physiques connectés localement 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.

View 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.

REMARQUE 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 Virtual SAN.

Mise à niveau d' View 5.3.1 sur une base de données Virtual SAN

Horizon 6.0 (avec View) introduit de nouvelles stratégies de stockage par défaut pour Virtual SAN. Ces stratégies ne s'appliqueront pas automatiquement aux postes de travail de machine virtuelle existants créés sur Virtual SAN par View 5.3.1 après la mise à niveau du pool de postes de travail vers la version 6.0. En outre, lorsque vous mettez à niveau View 5.3.1, le paramètre de pool **Utiliser VMware Virtual SAN** ne sera pas automatiquement activé, même si le pool réside dans une banque de données Virtual SAN. Vous disposez des options de mise à niveau suivantes :

- Après la mise à niveau, continuez à utiliser les stratégies de stockage par défaut qui étaient utilisées avec View 5.3.1. Si vous choisissez cette option, modifiez les paramètres de pool afin d'activer l'option **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-Virtual SAN, puis la mise à niveau et le rééquilibrage dans la banque de données Virtual SAN.

IMPORTANT Les tâches présentées dans cette procédure décrivent la mise à niveau d'un pool de postes de travail View 5.3.1 à l'aide d'une banque de données Virtual SAN sur un cluster VMware vSphere 5.5 Update 1. La mise à niveau d'une banque de données Virtual SAN sur un cluster VMware vSphere 5.5 ou version antérieure (fonctionnalité de la présentation technique) 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.

- 1 Vérifiez que toutes les machines virtuelles du pool sont des machines virtuelles VMware vSphere 5.5 Update 1 ou version ultérieure.
- 2 Modifiez les paramètres du pool de postes de travail afin de passer d'une banque de données Virtual SAN à une banque de données non-Virtual SAN, 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 View Administrator.
- 3 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](#) », page 53.

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

- 4 Recomposez le pool sur la banque de données non-Virtual SAN à l'aide du snapshot de la machine virtuelle parent que vous venez de créer.

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

- 5 Modifiez les paramètres du pool de postes de travail mis à niveau récemment à partir d'une banque de données non-Virtual SAN vers une banque de données Virtual SAN et utilisez la commande **Rééquilibrer**.

Mise à niveau d'une banque de données non-Virtual SAN vers une banque de données Virtual SAN

Les tâches présentées dans cette procédure décrivent la mise à niveau d'une banque de données non-Virtual SAN vers une banque de données Virtual SAN. La mise à niveau d'une banque de données Virtual SAN sur un cluster VMware 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.

- 1 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 de la fonctionnalité Virtual SAN.

Pour plus d'informations sur les mises à niveau, reportez-vous à [Chapitre 6, « Mettre à niveau des hôtes ESXi et leurs machines virtuelles »](#), page 47 et au *Guide de mise à niveau de VMware vSphere*. Pour plus d'informations sur les exigences de Virtual SAN, reportez-vous au document *vSphere Storage*.
- 2 Si toutes les machines virtuelles du pool ne sont pas des machines virtuelles VMware vSphere 5.5 Update 1 ou version ultérieure, mettez-les à niveau.

Pour plus d'instructions, consultez [Chapitre 6, « Mettre à niveau des hôtes ESXi et leurs machines virtuelles »](#), page 47 et reportez-vous au *Guide de VMware vSphere*.
- 3 Utilisez vCenter Server 5.5 Update 1 ou version ultérieure pour activer Virtual SAN pour le cluster vSphere.

Pour plus d'informations, reportez-vous au document *vSphere Storage*.
- 4 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 »](#), page 53.

Ce processus inclut l'installation de la version la plus récente de View Agent sur la machine virtuelle parent et la prise d'un snapshot.
- 5 Recomposez le pool sur la banque de données non-Virtual SAN à l'aide du snapshot de la machine virtuelle parent que vous venez de créer.

Pour des instructions sur la recomposition de pools, cliquez sur le bouton **Aide** dans View Administrator.
- 6 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-Virtual SAN à une banque de données Virtual SAN, 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 View Administrator.

Mettre à niveau l'application cliente

La phase finale d'une mise à niveau d'View inclut la mise à niveau vers la version la plus récente d'Horizon Client et celle du microprogramme sur des périphériques de client léger si vous les utilisez.

La fonctionnalité Mode local d'Horizon Client a été supprimée. À sa place, VMware recommande d'utiliser Mirage qui est inclus dans VMware Horizon 6. Pour en savoir plus, consultez les Notes de mise à jour d'View, disponibles à l'adresse https://www.vmware.com/support/pubs/view_pubs.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.

Prérequis

- Effectuez les procédures de mise à niveau des composants de serveur pouvant inclure Serveur de connexion View et View Composer. Reportez-vous à la section [Chapitre 5, « Mise à niveau des composants d'View Server »](#), page 27.
- 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://www.vmware.com/support/viewclients/doc/viewclients_pubs.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 View. 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>REMARQUE 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 », page 59.</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.

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 de portail affiche à la fois une icône pour télécharger et installer le client Horizon Client natif et une icône pour se connecter via HTML Access. 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 pour pointer vers une URL différente.

Vous pouvez créer des liens de programme d'installation pour les systèmes d'exploitation client spécifiques. 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, vous pouvez créer des liens distincts pour les programmes d'installation 32 bits et 64 bits.

IMPORTANT Si vous procédez à une mise à niveau depuis 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 que vous installez Serveur de connexion View 6.0. Avec cette version, le composant HTML Access est installé automatiquement pendant une mise à niveau de Serveur de connexion View.

Si vous avez déjà installé le composant HTML Access séparément de View 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 serveur de connexion View, 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.

REMARQUE Les personnalisations de View 5.x et versions antérieures se situent 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`.

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
Créer des liens pour des programmes d'installation spécifiques	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 <code>downloads</code> , situé sous le répertoire <code>C:\Program Files\VMware\VMware View\Server\broker\webapps\</code> sur le Serveur de connexion View, comme décrit à l'étape suivante. <ul style="list-style-type: none"> ■ Programme d'installation de Windows 32 bits : <code>link.win32=https://server/downloads/VMware-Horizon-Client.exe</code> ■ Programme d'installation de Windows 64 bits : <code>link.win64=https://server/downloads/VMware-Horizon-Client.exe</code> ■ Programme d'installation de Linux : <code>link.linux=https://server/downloads/VMware-Horizon-Client.tar.gz</code> ■ Programme d'installation de Mac OS X : <code>link.mac=https://server/downloads/VMware-Horizon-Client.dmg</code> ■ Programme d'installation d'iOS : <code>link.ios=https://server/downloads/VMware-Horizon-Client-iPhoneOS.zip</code> ■ Programme d'installation d'Android : <code>link.android=https://server/downloads/VMware-Horizon-Client-AndroidOS.apk</code>
Changer l'URL du lien de l'aide	<code>link.help</code> Par défaut, ce lien pointe vers un système d'aide hébergé sur le site Web de VMware. Le lien d'aide s'affiche dans le coin supérieur droit de l'écran. Pour l'écran de connexion à HTML Access et l'écran de sélection de postes de travail, le lien d'aide est une icône en forme de point d'interrogation. Dès que vous êtes connecté à un poste de travail, le lien d'aide devient une commande Aide affichée dans le menu déroulant à l'extrémité droite de la barre de menus du client.

- 3 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` à l'étape précédente. Par exemple, pour placer les fichiers dans un dossier `downloads` sur l'hôte du Serveur de connexion View, 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`.

- 4 Redémarrez le service du composant Web View.

Application de correctifs View

Les versions de correctif peuvent inclure des fichiers du programme d'installation pour les composants View suivants : View Composer, Serveur de connexion View, View Agent et divers clients. Les composants de correctif que vous devez appliquer dépendent des correctifs de bogue dont votre déploiement d'View a besoin.

En fonction des correctifs de bogue dont vous avez besoin, installez les composants View applicables dans l'ordre suivant :

- 1 View Composer
- 2 Serveur de connexion View
- 3 View Agent
- 4 Horizon Client

Ce chapitre aborde les rubriques suivantes :

- [« Appliquer un correctif pour View Composer », page 63](#)
- [« Appliquer un correctif pour le Serveur de connexion View », page 64](#)
- [« Appliquer un correctif pour View Agent », page 65](#)
- [« Appliquer un correctif à Horizon Client », page 66](#)

Appliquer un correctif pour View Composer

L'application d'un correctif implique la désinstallation de la version actuelle et l'installation de la version de correctif. Les versions de correctif n'incluent pas toutes de correctifs pour View Composer.

Prérequis

- Déterminez quand effectuer cette procédure. Choisissez une période de maintenance de poste de travail disponible. Prévoyez 15 à 30 minutes pour chaque instance de View Composer.
- Vérifiez que vous possédez un compte d'utilisateur de domaine avec des privilèges d'administration sur les hôtes que vous utiliserez pour exécuter le programme d'installation de correctif.
- 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.
- 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.

- Pour tous les pools de postes de travail de clone lié, désactivez le provisionnement des nouvelles machines virtuelles.
- Si un pool de postes de travail est programmé pour une opération d'actualisation ou de recomposition, annulez ces tâches.

Procédure

- 1 Sur la machine virtuelle hébergeant View Composer, téléchargez le fichier du programme d'installation pour la version de correctif de View Composer.
Votre contact chez VMware vous fournira des instructions sur ce téléchargement.
- 2 Utilisez l'utilitaire **Ajout/Suppression de programmes** de Windows pour supprimer View Composer installé précédemment.
- 3 Exécutez le programme d'installation que vous avez téléchargé pour la version de correctif de View Composer.
- 4 Vérifiez que le service VMware Horizon View Composer redémarre lorsque l'assistant du programme d'installation se ferme.
- 5 Le cas échéant, appliquez le correctif pour View Agent sur une machine virtuelle parente et créez un pool de postes de travail à des fins de test.
 - a Utilisez l'utilitaire **Ajout/Suppression de programmes** de Windows pour supprimer View Agent installé précédemment.
 - b Téléchargez et exécutez le programme d'installation de correctif de View Agent sur une machine virtuelle parente.
Votre contact chez VMware vous fournira des instructions sur ce téléchargement.
 - c Créez un petit pool de postes de travail de clone lié à partir de cette machine virtuelle.
 - d Testez un poste de travail virtuel 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 virtuel, et vérifiez que vous pouvez utiliser Horizon Client pour ouvrir une session sur ce poste de travail.

Des instructions pas à pas pour l'exécution du programme d'installation de View Agent et la création de pools de postes de travail s'affichent dans *Configuration de pools de postes de travail et d'applications dans View*, disponible en cliquant sur le bouton **Aide** dans View Administrator.
 - e Vérifiez que les postes de travail virtuels du pool de postes de travail de test fonctionnent comme prévu.

Suivant

Appliquez le correctif au Serveur de connexion View, le cas échéant.

Appliquer un correctif pour le Serveur de connexion View

L'application d'un correctif implique la désinstallation de la version actuelle et l'installation de la version de correctif.

Prérequis

- Déterminez quand effectuer cette procédure. Choisissez une période de maintenance de poste de travail disponible. La durée requise dépend du nombre d'instances de Serveur de connexion View dans le groupe. Prévoyez 15 à 30 minutes pour chaque instance.
- Vérifiez que vous possédez un compte d'utilisateur de domaine avec des privilèges d'administration sur les hôtes que vous utiliserez pour exécuter le programme d'installation de correctif.

Procédure

- 1 Si le Serveur de connexion View 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.
- 2 Arrêtez le service appelé service Serveur de connexion VMware Horizon View sur toutes les instances de Serveur de connexion View du groupe.
La base de données View LDAP peut être altérée si vous mettez à niveau une instance de Serveur de connexion View et que d'autres instances dans le même groupe sont en cours d'exécution. N'arrêtez pas le service VMwareVDMDS.
- 3 Sur l'une des instances de Serveur de connexion View dans un groupe répliqué, téléchargez le fichier du programme d'installation pour la version de correctif de Serveur de connexion View.
Votre contact chez VMware vous fournira des instructions sur ce téléchargement.
- 4 Utilisez l'utilitaire **Ajout/Suppression de programmes** de Windows pour supprimer le Serveur de connexion View précédemment installé, mais ne supprimez pas **Adam Instance VMwareVDMDS**.
- 5 Exécutez le programme d'installation que vous avez téléchargé pour la version de correctif de Serveur de connexion View.
Pour plus d'informations sur l'exécution du programme d'installation, consultez le document *Installation de View*.
- 6 Suivez les invites de l'assistant d'installation et cliquez sur **OK** pour continuer l'installation avec l'instance ADAM existante.
- 7 Vérifiez que le service Serveur de connexion VMware Horizon View redémarre lorsque l'assistant du programme d'installation se ferme.
- 8 Arrêtez de nouveau le service Serveur de connexion VMware Horizon View.
- 9 Répétez les étapes [Étape 3](#) à [Étape 8](#) pour les autres instances de Serveur de connexion View dans le groupe répliqué.
- 10 Une fois que tous les serveurs dans le groupe sont mis à niveau, démarrez le service de Serveur de connexion View sur tous les serveurs.
- 11 Répétez ce processus pour des serveurs de sécurité View.

Suivant

En cas d'échec de l'application du correctif sur une ou plusieurs instances de Serveur de connexion View, reportez-vous à la section « [Créer un groupe répliqué après avoir rétabli un snapshot du serveur de connexion View](#) », page 42

Appliquez le correctif sur View Agent, le cas échéant.

Appliquer un correctif pour View Agent

L'application d'un correctif implique la désinstallation de la version actuelle et l'installation de la version de correctif.

Les étapes suivantes doivent être effectuées sur la machine virtuelle parent, pour les pools de postes de travail de clone lié ou sur chaque poste de travail de machine virtuelle dans un pool de clone complet, ou sur des machines virtuelles de poste de travail individuelles pour les pools contenant un seul poste de travail de machine virtuelle.

Prérequis

Vérifiez que vous possédez un compte d'utilisateur de domaine avec des privilèges d'administration sur les hôtes que vous utiliserez pour exécuter le programme d'installation de correctif.

Procédure

- 1 Sur toutes les machines virtuelles parentes, machines virtuelles utilisées pour les modèles de clone complet, clones complets dans un pool et machines virtuelles individuelles ajoutées manuellement, téléchargez le fichier du programme d'installation pour la version de correctif de View Agent.

Votre contact chez VMware vous fournira des instructions sur ce téléchargement.
- 2 Utilisez l'utilitaire **Ajout/Suppression de programmes** de Windows pour supprimer View Agent installé précédemment.
- 3 Exécutez le programme d'installation que vous avez téléchargé pour la version de correctif de View Agent.

Des instructions pas à pas pour l'exécution du programme d'installation de View Agent s'affichent dans le document *Configuration de pools de postes de travail et d'applications pour View*.
- 4 Si vous désactivez l'approvisionnement de nouvelles machines virtuelles en préparation pour l'application d'un correctif à View Composer, activez de nouveau l'approvisionnement.
- 5 Pour les machines virtuelles parentes qui seront utilisées pour créer des pools de postes de travail de clone lié, prenez un snapshot de la machine virtuelle.

Pour plus d'instructions sur la prise de snapshots, consultez l'aide en ligne de vSphere Client.
- 6 Pour les pools de postes de travail de clone lié, utilisez le snapshot que vous avez créé pour recomposer les pools de postes de travail.
- 7 Vérifiez que vous pouvez ouvrir une session sur les pools de postes de travail corrigés avec Horizon Client.
- 8 Si vous avez annulé une opération d'actualisation ou de recomposition pour un pool de postes de travail de clone lié, replanifiez ces tâches.

Appliquer un correctif à Horizon Client

Sur les périphériques client de poste de travail, l'application d'un correctif implique la désinstallation de la version actuelle et l'installation de la version de correctif d'Horizon Client. Sur les clients mobiles, l'application d'un correctif implique l'installation de la mise à jour auprès d'un site Web qui vend des applications, tel que Google Play, Windows Store ou l'App Store d'Apple.

Procédure

- 1 Sur chaque système client, téléchargez le fichier du programme d'installation pour la version de correctif d'Horizon Client.

Votre contact chez VMware vous fournira des instructions sur ce téléchargement. Comme mentionné précédemment, pour certains clients, vous pouvez obtenir la version du correctif auprès d'un App Store.
- 2 Si le périphérique client est un poste de travail ou un ordinateur portable, supprimez la version actuelle du logiciel client de votre périphérique.

Utilisez la méthode spécifique du périphérique habituelle pour supprimer des applications.
- 3 Le cas échéant, exécutez le programme d'installation que vous avez téléchargé pour la version de correctif d'Horizon Client.

Si vous avez acheté le correctif sur l'Apple App Store ou Google Play, l'application s'installe en général lorsque vous la téléchargez, et vous n'avez pas à exécuter de programme d'installation.

- 4 Vérifiez que vous pouvez ouvrir une session sur les pools de postes de travail corrigés avec Horizon Client corrigé.

Mise à niveau séparée de composants vSphere dans un environnement View

9

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

Plutôt que d'effectuer une mise à niveau intégrée des composants View et vSphere, vous pouvez commencer par mettre à niveau tous les composants View, 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 View, 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 View LDAP à partir d'une instance de Serveur de connexion View à l'aide de l'utilitaire `vdmexport.exe`.

Pour obtenir les instructions, reportez-vous au document *Administration de View*. Si vous possédez plusieurs instances de Serveur de connexion View 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 View Agent.

La réinstallation de View Agent garantit que les pilotes de la machine virtuelle restent compatibles avec les autres composants View.

Des instructions pas à pas pour l'exécution du programme d'installation de View Agent apparaissent dans le document *Configuration de pools de postes de travail et d'applications pour View*.

Index

B

base de données View Composer,
configuration **14**
Bases de données Microsoft SQL Server **14**
Bases de données Oracle **14**
Bases de données SQL Server **14**

C

certificats, accepter l'empreinte numérique **40**
clients légers **49, 58**
codes de résultat, opération
databaseupgrade **30**
compatibilité de base de données **21**
compatibilité descendante **7**
configuration matérielle requise
Serveur de connexion View **16**
View Composer, autonome **14**
configuration système requise pour les mises à
niveau **13**
conteneur de clés RSA
migration vers View Composer **36**
utilisation de NET Framework **36**

D

databaseupgrade, codes de résultat **30**

E

empreinte numérique, accepter un certificat par
défaut **40**
équilibres de charge **23**
Exigences d'Horizon Client **19**
exigences de licence **15, 16**
exigences de navigateur Web **18**
exigences navigateur **18**

F

Fichiers de modèle d'administration (ADM),
Composants View **45**
Firefox, versions prises en charge **18**
fonction de récupération d'espace **54**
format de disque à optimisation d'espace **54**

G

gestion de postes de travail de clone lié,
procédure de mise à niveau **50**
gestion du pool de postes de travail, mise à
niveau des pools **53**

H

Horizon Client
application de correctifs pour **66**
mise à niveau **49, 58**
Hôte Microsoft RDS **49**
Hôte Services Terminal Server **49**

I

installation de Serveur de connexion View
exigences du logiciel de virtualisation **18**
présentation des exigences **16**
systèmes d'exploitation pris en charge **16**
installation de View Composer, présentation des
exigences **13**
Internet Explorer, versions prises en charge **18**

L

LDAP **23**
liste de vérification de la mise à niveau **11**

M

machines virtuelles, mise à niveau **47**
maintenance de View Composer
migration avec la base de données
existante **33**
migration d'un conteneur de clés RSA **36**
migration de View Composer vers une autre
machine **32**
recommandations pour la migration **33**
matrice de compatibilité pour composants
View **7**
migration
View Composer avec une base de données
existante **33**
View Composer sans clones liés **35**
View Composer vers une autre machine **32**
mise à niveau de base de données
sviconfig ne réussit pas **31**
View Composer sviconfig **29**
mise à niveau de LDAP **37**
mise à niveau de pool de postes de travail, pools
de clone complet et de clone lié **50**
mise à niveau de vCenter Server, tâches de
préparation de la mise à niveau **21, 69**
mise à niveau de View Composer
compatibilité avec les version de vCenter
Server **13**
exigences de système d'exploitation **13**

- la mise à niveau de base de données ne se termine pas **31**
- mise à niveau de base de données sviconfig **29**
- modification du port **28**
- présentation des exigences **13**
- procédure de mise à niveau **28, 44**
- tâches de préparation de la mise à niveau **21**
- mise à niveau de View LDAP **37**
- mises à niveau de cluster **47**
- mises à niveau de microprogramme pour clients légers **49, 58**
- mode vSphere pour View Composer **47**
- modèles GPO **37**

N

- NET Framework, migration du conteneur de clés RSA **36**

O

- outil d'inscription ASP.NET IIS, conteneur de clés RSA **36**

P

- page HTML Access **59**
- PC lame **50**
- PC physique **50**
- période de maintenance **27**
- pools de postes de travail non persistants **53**
- pools de postes de travail persistants **53**
- port, changement pour View Composer lors de la mise à niveau **28**
- portail Web **59**
- postcompatibilité **7**
- préparation de la mise à niveau
 - Composants View **21**
 - Serveur de connexion View **23**
 - vCenter Server **21**
 - View Composer **21**
- Procédure de mise à niveau d'hôte ESXi **47**
- procédure de mise à niveau de vCenter Server **44**
- procédure de mise à niveau de VirtualCenter **28**
- procédure de mise à niveau matérielle virtuelle **47**

S

- sauvegardes de base de données **21**
- sauvegardes de certificat SSL **21**
- serveur de connexion View, rétablir un snapshot **42**
- Serveur de connexion View
 - application de correctifs pour **64**
 - configuration matérielle requise **16**

- exigences de mise à niveau **16**
- migration vers une nouvelle machine **41**
- procédure de mise à niveau **37**
- tâches de préparation de la mise à niveau **23**
- serveurs de sécurité
 - exigences de système d'exploitation **16**
 - mise à niveau **37, 43**
 - préparer la mise à niveau ou la réinstallation **24**
 - supprimer des règles IPsec **24**
- service VMwareVDMDS **37, 43**
- services
 - Serveur de connexion VMware Horizon View **37, 43**
 - VMwareVDMDS **37, 43**
- SSL, accepter une empreinte numérique de certificat **40**
- stratégies de groupe, Composants View **45**
- Support technique, VMware **5**

U

- utilitaire sviconfig **29, 30**
- utilitaire vdmadmin.exe **41**
- utilitaire vdmexport.exe **23, 37**
- utilitaires
 - sviconfig **29, 30**
 - vdmadmin.exe **41**
 - vdmexport.exe **23, 37**

V

- versions de correctif **27, 63**
- View Administrator, configuration **18**
- View Agent
 - application de correctifs pour **65**
 - exigences d'installation **19**
 - procédure de mise à niveau **50, 69**
- View Composer
 - application de correctifs pour **63**
 - exigences de mise à niveau **15**
 - exigences matérielles de View Composer autonome **14**
 - mise à niveau de base de données sviconfig **29**
 - mode vSphere **47**
- View LDAP **23**
- Virtual SAN **55**
- VMotion **47**
- VMware Tools, procédure de mise à niveau **47, 69**
- vSphere, mise à niveau séparée des composants **69**
- vSphere Update Manager **47**