

Mises à niveau d'Horizon

VMware Horizon 2111

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

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

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

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

Copyright © 2021 VMware, Inc. Tous droits réservés. [Informations relatives aux copyrights et marques commerciales.](#)

Table des matières

Mise à niveau de VMware Horizon vers cette version	5
1 Présentation de la mise à niveau d'VMware Horizon	6
2 Désinstallation de fonctionnalités plus prises en charge et obsolètes	9
Remplacement d'un serveur de sécurité par un dispositif Unified Access Gateway	10
Désinstaller JMP Server	12
Supprimer View Composer d'Horizon	12
3 Mettre à niveau l'application cliente	14
4 Configuration système requise pour les mises à niveau du serveur VMware Horizon	16
Matrice de compatibilité des différentes versions des composants d'VMware Horizon	16
Exigences du Serveur de connexion Horizon	17
Configuration matérielle requise d'Horizon Connection Server	17
Systèmes d'exploitation pris en charge pour le Serveur de connexion Horizon	18
Exigences de mise à niveau du Serveur de connexion Horizon	18
Exigences et considérations pour Horizon Agent	19
5 Mise à niveau des composants d'VMware Horizon Server	21
Mise à niveau d'Horizon Connection Server	21
Préparation du Serveur de connexion pour une mise à niveau	22
Mise à niveau de Serveurs de connexion dans un groupe répliqué	23
Mise à niveau vers la version la plus récente du Serveur de connexion sur une machine différente	26
Créer un groupe répliqué après avoir rétabli un snapshot du Serveur de connexion	28
Mise à niveau des Serveurs de connexion en parallèle	29
Dépannage des erreurs lors de la mise à niveau et de l'installation de Serveurs de connexion	30
Mise à niveau des serveurs d'inscription	32
Mise à niveau d'un environnement Architecture Cloud Pod	32
Mise à niveau de serveurs VMware Horizon pour autoriser HTML Access	33
Mettre à niveau vCenter Server	33
Accepter l'empreinte numérique d'un certificat TLS par défaut	35
Utilisation des fichiers de modèle d'administration de stratégie de groupe Horizon	36
6 Mettre à niveau des hôtes ESXi et leurs machines virtuelles	38

7 Mise à niveau des postes de travail publiés et virtuels 40

Mettre à niveau Horizon Agent 41

Mettre à niveau des pools de postes de travail d'Instant Clone lorsque vous mettez à niveau vCenter Server vers vSphere 6.7 ou version ultérieure 44

Mettre à niveau les hôtes RDS qui fournissent des postes de travail basés sur une session 45

8 Mise à niveau séparée de composants vSphere dans un environnement VMware Horizon 48

Mise à niveau de VMware Horizon vers cette version

Mises à niveau d'Horizon fournit des instructions sur la mise à niveau à partir des dernières versions principales ou de maintenance de VMware Horizon™ 7.x et VMware Horizon 2xxx vers cette version. Vous pouvez également utiliser ce guide lorsque vous effectuez la mise à niveau vers des versions de maintenance d'VMware Horizon.

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'VMware Horizon.

Public cible

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

Présentation de la mise à niveau d'VMware Horizon

1

La mise à niveau du déploiement d'VMware Horizon 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.

Attention Pour obtenir les chemins de mise à niveau pris en charge, reportez-vous à la [Matrice d'interopérabilité des produits VMware](#).

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

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

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

- 1 Si vous disposez de fonctionnalités qui ne sont plus prises en charge dans la dernière version de VMware Horizon, vous devez désinstaller certaines d'entre elles avant de procéder à la mise à niveau. Reportez-vous à la section [Chapitre 2 Désinstallation de fonctionnalités plus prises en charge et obsolètes](#).
- 2 Mettez à niveau le logiciel Horizon Client qui s'exécute sur des périphériques clients d'utilisateurs finaux. Reportez-vous à la section [Chapitre 3 Mettre à niveau l'application cliente](#).
- 3 Sur les machines physiques ou virtuelles qui hébergent des instances du Serveur de connexion, faites des sauvegardes et enregistrez divers paramètres de configuration et système. Reportez-vous à la section [Préparation du Serveur de connexion pour une mise à niveau](#).

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

- 4 Mettez à niveau les instances du Serveur de connexion. Reportez-vous à la section [Mise à niveau de Serveurs de connexion dans un groupe répliqué](#).

Dans un environnement de production typique comportant au moins deux instances du Serveur de connexion renforcées par un équilibrage de charge, vous devez supprimer les instances du Serveur de connexion du cluster à équilibrage de charge pendant leur mise à niveau.

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

- 5 Mettez à niveau les stratégies de groupe utilisées dans Active Directory. Reportez-vous à la section [Utilisation des fichiers de modèle d'administration de stratégie de groupe Horizon](#).
- 6 Si vous mettez également à niveau des composants VMware vSphere, mettez à niveau vCenter Server. Reportez-vous à la section [Mettre à niveau vCenter Server](#).

Durant la mise à niveau de vCenter Server, les postes de travail à distance et les sessions d'applications ne seront pas déconnectés. Les postes de travail distants en état d'approvisionnement ne sont pas mis sous tension durant la mise à niveau de vCenter Server. Vous ne pouvez alors pas lancer de nouveaux postes de travail lors de la mise à niveau de vCenter Server.

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

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

- 8 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 2012 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](#).
- 9 Mettez à niveau le logiciel Horizon[™] Agent qui s'exécute sur les machines physiques ou virtuelles utilisées en tant que modèles pour le clonage de postes de travail, en tant que postes de travail de clone complet dans un pool et en tant que postes de travail individuels dans un pool manuel. Reportez-vous à la section [Mettre à niveau Horizon Agent](#).
- 10 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 [Mettre à niveau des pools de postes de travail d'Instant Clone lorsque vous mettez à niveau vCenter Server vers vSphere 6.7 ou version ultérieure](#).
- 11 Si vous utilisez la fonction Architecture Cloud Pod, consultez [Mise à niveau d'un environnement Architecture Cloud Pod](#).

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

Déploiement d'une branche de maintenance étendue

Environ une fois par an, VMware désigne une version de VMware Horizon comme branche de maintenance étendue (ESB). Une ESB est une branche de version parallèle aux versions actuelles (CR) du produit. En choisissant de déployer une ESB, les clients reçoivent des mises à jour de Service Packs (SP) périodiques, qui incluent des correctifs de bogues critiques et des correctifs de sécurité cumulatifs. Plus important encore, les mises à jour du fournisseur de services ne comportent aucune nouvelle fonctionnalité. Les clients peuvent ainsi s'appuyer sur une plateforme Horizon stable pour leurs déploiements critiques.

Pour plus d'informations sur l'ESB et les versions d'Horizon désignées comme ESB, reportez-vous à [l'article 86477 de la base de connaissances de VMware](#).

Désinstallation de fonctionnalités plus prises en charge et obsolètes

2

Avant de mettre à niveau VMware Horizon, vous devez désinstaller les fonctionnalités qui ne sont plus prises en charge ou qui sont obsolètes dans la dernière version de VMware Horizon.

Si vous effectuez une mise à niveau vers VMware Horizon 2012 et versions ultérieures, vous devez désinstaller les fonctionnalités suivantes disponibles dans les versions antérieures de VMware Horizon 7.x :

Fonctionnalités plus prises en charge ou obsolètes	Description
Serveur de sécurité (n'est plus pris en charge)	<p>Si vous disposez de serveurs de sécurité et si vous souhaitez effectuer une mise à niveau vers VMware Horizon 2012 et versions ultérieures, vous devez déployer un dispositif Unified Access Gateway de remplacement, puis désinstaller les serveurs de sécurité avant de mettre à niveau le Serveur de connexion.</p> <p>Note Après une mise à niveau vers VMware Horizon 2012 si vous ne supprimez pas le serveur de sécurité et si vous tentez de vous connecter à Horizon Client à l'aide du serveur de sécurité, une erreur HTTP s'affiche.</p> <p>Reportez-vous à la section Remplacement d'un serveur de sécurité par un dispositif Unified Access Gateway.</p>
JMP Server (n'est plus pris en charge)	<p>Si JMP Server est installé sur votre ordinateur, et si vous voulez effectuer la mise à niveau vers VMware Horizon 2012 et versions ultérieures, vous devez désinstaller JMP Server. Consultez la section Désinstaller JMP Server.</p> <p>Note Les attributions de poste de travail JMP précédemment créées s'affichent toujours dans Horizon Console et peuvent être modifiées ou supprimées. Les attributions d'App Volumes précédemment créées à partir des attributions JMP s'affichent toujours dans la console App Volumes et peuvent être modifiées ou supprimées. L'attribution de paramètre Dynamic Environment Manager créée à partir de l'attribution JMP si le partage Dynamic Environment Manager n'est pas supprimé lors de la désinstallation de JMP, s'affiche en mode lecture seule dans la console Dynamic Environment Manager et vous ne pouvez pas modifier ou supprimer cette attribution.</p>
View Composer (n'est plus pris en charge)	<p>Si View Composer est installé sur votre ordinateur et si vous souhaitez effectuer la mise à niveau vers VMware Horizon 2012 et versions ultérieures, vous devez supprimer View Composer et tous vos pools de postes de travail et vos batteries de serveurs de clone lié. Reportez-vous à la section Supprimer View Composer d'Horizon.</p>

Ce chapitre contient les rubriques suivantes :

- [Remplacement d'un serveur de sécurité par un dispositif Unified Access Gateway](#)
- [Désinstaller JMP Server](#)
- [Supprimer View Composer d'Horizon](#)

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

Remplacez un serveur de sécurité par un dispositif Unified Access Gateway.

Procédure

- 1 Désinstallez le logiciel du serveur de sécurité.
- 2 Supprimez l'entrée LDAP du serveur de sécurité : `vdmadmin -s [-b authentication_arguments] -r -s server`

Reportez-vous à la section *Suppression de l'entrée pour une instance d'Horizon Connection Server à l'aide de l'option -S* dans le document *Administration d'Horizon*.

- 3 Dans Horizon Console, enregistrez le dispositif Unified Access Gateway.
- 4 Au niveau du pare-feu de réseau entre Unified Access Gateway et le Serveur de connexion, supprimez les règles de pare-feu associées au serveur de sécurité supprimé et ajoutez des règles de pare-feu associées à la passerelle Unified Access Gateway entrante. Unified Access Gateway doit communiquer avec le Serveur de connexion sur le port TCP 443.

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

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

- 5 Configurez et démarrez le dispositif Unified Access Gateway.

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

Désinstaller JMP Server

Si vous disposez d'une instance de JMP Server installée et si vous souhaitez effectuer une mise à niveau vers VMware Horizon 2006 et versions ultérieures, vous devez désinstaller JMP Server avant de procéder à la mise à niveau.

Conditions préalables

- Vérifiez que vous disposez des privilèges d'administration corrects pour désinstaller JMP Server.

Procédure

- 1 Suivez les étapes ci-dessous pour supprimer les informations de partage de configuration Dynamic Environment Manager pour JMP Server.
 - a Dans Horizon Console, cliquez sur **Configuration de JMP**.
 - b Cliquez sur l'onglet **UEM**.
 - c Sélectionnez la ligne des informations sur le partage de configuration Dynamic Environment Manager que vous voulez supprimer des paramètres JMP.
 - d Cliquez sur **Supprimer** pour confirmer que vous voulez supprimer ces informations sur le partage de configuration Dynamic Environment Manager.

Si aucune attribution JMP n'utilise le partage de configuration Dynamic Environment Manager, il est supprimé.

Si le partage de configuration Dynamic Environment Manager est utilisé par une attribution JMP, une boîte de dialogue d'avertissement s'affiche. Le message d'avertissement comporte la liste d'attributions JMP qui utilisent le partage de configuration Dynamic Environment Manager. Vous pouvez supprimer les informations sur le partage de configuration Dynamic Environment Manager après les avoir supprimées des attributions JMP ou après avoir supprimé les attributions JMP qui les utilisent.

- 2 Procédez comme suit pour désinstaller JMP Server.
 - a Ouvrez la console Programmes et fonctionnalités de Microsoft Windows.
Par exemple, cliquez sur **Démarrer > Paramètres > Système > Applications et fonctionnalités**.
 - b Sélectionnez **VMware JMP** dans la liste des applications installées.
 - c Pour terminer les étapes de désinstallation, cliquez sur **Désinstaller** et suivez l'assistant.

Supprimer View Composer d'Horizon

Vous pouvez supprimer la connexion entre Horizon et le service View Composer qui est associé à une instance de vCenter Server.

Avant de désactiver la connexion à View Composer, vous devez supprimer d'Horizon toutes les machines virtuelles de clone lié créées par View Composer. Horizon vous empêche de supprimer View Composer si des clones liés associés existent toujours. Une fois que la connexion à View Composer est désactivée, Horizon ne peut plus provisionner ni gérer de nouveaux clones liés.

Procédure

1 Supprimez les pools de postes de travail de clone lié créés par View Composer.

a Dans la Horizon Console, sélectionnez **Inventaire > Postes de travail**.

b Sélectionnez un pool de postes de travail de clone lié et cliquez sur **Supprimer**.

Une boîte de dialogue vous avertit que vous allez supprimer de façon permanente d'Horizon le pool de postes de travail de clone lié. Si les machines virtuelles de clone lié sont configurées avec des disques persistants, vous pouvez détacher ou supprimer ces disques.

c Cliquez sur **OK**.

Les machines virtuelles sont supprimées de vCenter Server. De plus, les entrées de base de données View Composer associées et les réplicas créés par View Composer sont supprimés.

d Répétez ces étapes pour chaque pool de postes de travail de clone lié créé par View Composer.

2 Accédez à **Paramètres > Serveurs**.

3 Dans l'onglet **vCenter Servers**, sélectionnez l'instance de vCenter Server à laquelle View Composer est associé.

4 Cliquez sur **Modifier**.

5 Sous l'onglet **View Composer**, sous **Paramètres de View Composer Server**, sélectionnez **Ne pas utiliser View Composer** et cliquez sur **OK**.

Résultats

Vous ne pouvez plus créer de pools de postes de travail de clone lié dans cette instance de vCenter Server, mais vous pouvez continuer à créer et à gérer des pools de postes de travail de machine virtuelle complets dans l'instance de vCenter Server.

Mettre à niveau l'application cliente

3

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

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 Horizon Client 4.6.0 pour Windows ou une version antérieure, demandez-leur de supprimer le logiciel client avant de télécharger et d'exécuter le dernier programme d'installation d'Horizon Client.

Conditions préalables

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

Procédure

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

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

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

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

4

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

Ce chapitre contient les rubriques suivantes :

- Matrice de compatibilité des différentes versions des composants d'VMware Horizon
- Exigences du Serveur de connexion Horizon
- Exigences et considérations pour Horizon Agent

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

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

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

- VMware Horizon 7 version 7.x

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

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

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

Tableau 4-1. Matrice de compatibilité pour VMware Horizon 2006 ou des versions ultérieures et antérieures des composants de VMware Horizon

	Serveur de connexion : version antérieure	Horizon Agent : version antérieure	Horizon Client (Windows) : version antérieure
Serveur de connexion 2006 ou version ultérieure	Uniquement lors des mises à niveau	Uniquement lors des mises à niveau	Non
Horizon Agent 2006 ou version ultérieure	Uniquement lors des mises à niveau	S/O	Uniquement lors des mises à niveau
Horizon Client 2006 ou version ultérieure	Oui	Oui	S/O

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

Exigences du Serveur de connexion Horizon

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

Configuration matérielle requise d'Horizon Connection Server

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

Tableau 4-2. Configuration matérielle requise d'Horizon Connection Server

Composant matériel	Requis	Recommandé
Processeur	Processeur Pentium IV 2.0 GHz ou supérieur	4 CPU
Adaptateur réseau	Carte réseau de 100 Mbits/s	Des cartes réseau de 1 Gbit/s
Mémoire	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 également aux instances d'Horizon Connection Server de réplica que vous installez pour la haute disponibilité ou l'accès externe.

Important La machine physique ou virtuelle qui héberge l'Horizon Connection Server doit disposer d'une adresse IP qui ne change pas. Dans un environnement IPv4, configurez une adresse IP statique. Dans un environnement IPv6, les machines obtiennent automatiquement des adresses IP qui ne changent pas.

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

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

Pour obtenir une liste des systèmes d'exploitation Windows Server pris en charge, consultez l'article <https://kb.vmware.com/s/article/78652> de la base de connaissances VMware.

Exigences de mise à niveau du Serveur de connexion Horizon

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

- Le Serveur de connexion nécessite une licence valide pour cette dernière version. Si vous disposez d'une licence perpétuelle, vous devrez télécharger la nouvelle clé spécifique pour VMware Horizon 2006 ou version ultérieure. Si vous disposez d'une licence d'abonnement, aucune action supplémentaire n'est requise.
- Le compte d'utilisateur de domaine que vous utilisez pour installer la nouvelle version du Serveur de connexion doit disposer de privilèges administratifs sur l'hôte du Serveur de connexion. L'administrateur du Serveur de connexion doit disposer d'informations d'identification administratives pour vCenter Server.
- Lorsque vous exécutez le programme d'installation, vous autorisez un compte d'administrateur. Vous pouvez spécifier le groupe d'administrateurs locaux ou un compte d'utilisateur ou de groupe de domaine. VMware Horizon attribue des droits d'administration Horizon complets, y compris le droit d'installer des instances répliquées du Serveur de connexion, à ce compte uniquement. Si vous spécifiez un utilisateur ou un groupe de domaine, vous devez créer le compte dans Active Directory avant d'exécuter le programme d'installation.
- Lorsque vous sauvegardez le Serveur de connexion, la configuration de l'annuaire Horizon (Horizon Directory) est exportée sous forme de données LDIF chiffrées. Pour restaurer la configuration VMware Horizon de sauvegarde cryptée, vous devez fournir le mot de passe de récupération de données. Le mot de passe doit contenir entre 1 et 128 caractères.

Exigences liées à la sécurité

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

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

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

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

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

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

- Vous devrez peut-être apporter des modifications à la configuration du protocole de sécurité pour qu'il continue à être compatible avec vSphere. Si possible, appliquez des correctifs à ESXi et à vCenter Server pour prendre en charge TLSv1.1 et TLSv1.2 avant la mise à niveau du Serveur de connexion.

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

Exigences et considérations pour Horizon Agent

Le composant Horizon Agent facilite la gestion des sessions, Single Sign-On, la redirection de périphérique et d'autres fonctionnalités. Vous devez installer Horizon Agent sur l'ensemble des machines virtuelles, des systèmes physiques et des hôtes RDS.

Les types et éditions des systèmes d'exploitation invités pris en charge dépendent de la version de Windows.

Pour obtenir une liste des systèmes d'exploitation invités Windows 10, consultez l'article <https://kb.vmware.com/s/article/78714> de la base de connaissances VMware.

Pour connaître les systèmes d'exploitation Windows autres que Windows 10, consultez l'article <https://kb.vmware.com/s/article/78715> de la base de connaissances VMware.

Pour améliorer la sécurité, VMware recommande de configurer les suites de chiffrement afin de supprimer les vulnérabilités connues. Pour plus d'instructions sur la configuration d'une stratégie de domaine sur les suites de chiffrement pour les machines Windows qui exécutent Horizon Agent, consultez la rubrique sur la désactivation des chiffrements faibles pour Horizon Agent dans le document *Installation d'Horizon*.

Mise à niveau des composants d'VMware Horizon Server

5

Les composants de serveur à mettre à niveau comprennent le Horizon Connection Server et des serveurs répliqués.

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

Ce chapitre contient les rubriques suivantes :

- Mise à niveau d'Horizon Connection Server
- Mise à niveau des Serveurs de connexion en parallèle
- Mise à niveau des serveurs d'inscription
- Mise à niveau d'un environnement Architecture Cloud Pod
- Mise à niveau de serveurs VMware Horizon pour autoriser HTML Access
- Mettre à niveau vCenter Server
- Accepter l'empreinte numérique d'un certificat TLS par défaut
- Utilisation des fichiers de modèle d'administration de stratégie de groupe Horizon

Mise à niveau d'Horizon Connection Server

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

Une fois que vous avez effectué une nouvelle installation ou mise à niveau de toutes les instances du Serveur de connexion vers VMware Horizon 2006, vous ne pouvez pas rétrograder les instances du Serveur de connexion vers une version antérieure à Horizon 7 version 7.2, car les clés utilisées pour protéger les données LDAP ont été modifiées.

Pour avoir malgré tout la possibilité de rétrograder des instances du Serveur de connexion dont vous planifiez la mise à niveau vers VMware Horizon 2006, vous devez sauvegarder ces instances du Serveur de connexion avant de commencer la mise à niveau. Si vous avez besoin de rétrograder les instances du Serveur de connexion, vous devez rétrograder toutes les instances du Serveur de connexion, puis appliquer la sauvegarde au dernier Serveur de connexion rétrogradé.

Lors de la mise à niveau depuis une version d'VMware Horizon antérieure à la version d'Horizon 7.7.8, certains paramètres d'authentification utilisateur changent. La façon dont ces paramètres d'authentification utilisateur affectent l'expérience utilisateur dépend du client. Consultez la documentation Horizon Client à l'adresse <https://docs.vmware.com/fr/VMware-Horizon-Client/index.html>. Vous devez comprendre la sécurité et la facilité d'utilisation des paramètres d'authentification utilisateur avant de les modifier. Consultez la section « Paramètres de serveur liés à la sécurité pour l'authentification utilisateur » dans le document *Sécurité d'Horizon*.

Si vous disposez d'une licence perpétuelle, après la mise à niveau d'un Serveur de connexion dans un espace vers VMware Horizon 2006, vous ne pouvez pas démarrer un poste de travail à partir de ce Serveur de connexion, mais vous pouvez le démarrer à partir d'autres Serveurs de connexion de l'espace. Pour démarrer un poste de travail à partir du Serveur de connexion mis à niveau, démarrez Horizon Console sur ce Serveur de connexion et entrez une clé de licence 2006. Ensuite, vous pouvez démarrer des postes de travail à partir de tous les Serveurs de connexion de l'espace.

Après la mise à niveau d'une instance du Serveur de connexion, effectuez un rechargement matériel du navigateur Horizon Console afin qu'il sélectionne le dernier code source de l'interface utilisateur HTML5 du Serveur de connexion.

Préparation du Serveur de connexion pour une mise à niveau

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

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

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

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

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

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

- Ouvrez Horizon Console et documentez tous les paramètres généraux et les paramètres des postes de travail et des pools.

Vous pouvez également effectuer une capture d'écran des paramètres applicables.

- Utilisez l'utilitaire `vdmexport.exe` pour sauvegarder Horizon LDAP.

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

Tâches à effectuer pour chaque instance avant la mise à niveau

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

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

- Renseignez l'adresse IP et le nom de système de la machine sur laquelle le Serveur de connexion est installé.
- Déterminez si votre entreprise a écrit des fichiers ou des scripts de commandes qui s'exécutent dans la base de données Horizon LDAP sur l'instance du Serveur de connexion et, si c'est le cas, fournissez leurs noms et leurs emplacements.

- Ouvrez Horizon Console et documentez tous les paramètres spécifiques à cette instance.

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

Mise à niveau de Serveurs de connexion dans un groupe répliqué

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

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

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

Conditions préalables

- Déterminez quand effectuer cette procédure. Choisissez une période de maintenance de poste de travail disponible. La durée de la mise à niveau dépend du nombre d'instances du Serveur de connexion dans le groupe. Prévoyez 15 à 30 minutes pour chaque instance.
- Familiarisez-vous avec les exigences liées à la sécurité d'VMware Horizon et vérifiez que ces exigences sont respectées. Reportez-vous à la section [Exigences de mise à niveau du Serveur](#)

de connexion Horizon. Vous devez obtenir et installer un certificat de serveur SSL signé par une autorité de certification qui inclut des informations de révocation de certificat, vérifier que le Pare-feu Windows avec sécurité avancée est défini sur **on** et configurer des pare-feu principaux pour prendre en charge IPsec.

- Vérifiez que le serveur sur lequel vCenter Server est installé possède un certificat de serveur SSL signé par une autorité de certification installé et configuré. Après la mise à niveau du Serveur de connexion, si vCenter Server n'utilise pas de certificat signé par une autorité de certification, le certificat auto-signé par défaut est affiché comme étant non valide dans Horizon Console, et un message indique que vCenter Server n'est pas disponible.
- Effectuez les tâches répertoriées dans la section [Préparation du Serveur de connexion pour une mise à niveau](#).
- Vérifiez que vous possédez une licence valide pour la nouvelle version.
- Vérifiez que vous possédez un compte d'utilisateur de domaine avec des privilèges d'administration sur les hôtes que vous utilisez pour exécuter le programme d'installation et réaliser la mise à niveau.
- Si vous ne connaissez pas l'utilitaire `vdmexport.exe`, imprimez ses instructions d'utilisation à partir du document Administration de *Administration d'Horizon*. Vous utiliserez cet utilitaire pour sauvegarder la base de données Horizon LDAP dans le cadre de la procédure de mise à niveau.

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

Procédure

- 1 Si vous utilisez un équilibrage de charge pour gérer un groupe d'instances du Serveur de connexion, désactivez le serveur qui héberge l'instance du Serveur de connexion que vous êtes sur le point de mettre à niveau.
 - a Connectez-vous à Horizon Console.
 - b Accédez à **Paramètres > Serveurs** et cliquez sur l'onglet **Serveurs de connexion**.
 - c Sélectionnez l'instance du Serveur de connexion dans la liste et cliquez sur le bouton **Désactiver** au-dessus du tableau.
 - d Pour confirmer la désactivation du serveur, cliquez sur **OK**.
- 2 Sur l'hôte de l'instance du Serveur de connexion, téléchargez et exécutez le programme d'installation de la nouvelle version de Serveur de connexion.

Le nom de fichier du programme d'installation est `VMware-Horizon-Connection-Server-x86_64-y.y.y-xxxxxx.exe`, où `xxxxxx` est le numéro de build et `y.y.y` le numéro de version. Vous n'avez pas besoin d'arrêter des services avant d'effectuer la mise à niveau. Le programme d'installation s'arrête et redémarre des services si nécessaire. En fait, le service VMwareVDMDS doit être en cours d'exécution pour mettre à niveau la base de données Horizon LDAP.

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

La base de données Horizon LDAP est également mise à niveau.

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

- 3 Vérifiez que le service VMware Horizon Connection Server redémarre lorsque l'assistant du programme d'installation se ferme.
- 4 Connectez-vous à VMware Horizon et activez l'instance du Serveur de connexion que vous venez de mettre à niveau.
 - a Accédez à **Paramètres > Serveurs** et cliquez sur l'onglet **Serveurs de connexion**.
 - b Sélectionnez l'instance du Serveur de connexion dans la liste et cliquez sur le bouton **Activer** au-dessus du tableau.
 - c Dans la colonne Version, vérifiez que la nouvelle version est affichée.
- 5 Accédez à **Paramètres > Licence produit et utilisation**, cliquez sur **Modifier la licence**, entrez la clé de licence de et cliquez sur **OK**.
- 6 Si vous utilisez un équilibrage de charge pour gérer cette instance du Serveur de connexion, activez le serveur que vous venez de mettre à niveau.
- 7 Vérifiez que vous pouvez ouvrir une session sur un poste de travail distant.
- 8 Pour mettre à niveau chaque instance du Serveur de connexion dans le groupe, répétez les étapes précédentes.

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

- 9 Utilisez l'utilitaire `vdmexport.exe` pour sauvegarder la base de données Horizon LDAP récemment mise à niveau.

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

- 10 Connectez-vous et examinez Horizon Console pour vérifier que l'icône vCenter Server est verte.

Si l'icône est rouge et si la boîte de dialogue Certificat non valide détecté apparaît, cliquez sur **Vérifier** et acceptez l'empreinte numérique du certificat non approuvé ou installez un certificat SSL signé par une autorité de certification valide.

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

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

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

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

Étape suivante

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

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

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

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

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

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

Conditions préalables

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

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

Procédure

- 1 Vérifiez qu'une instance mise à niveau du Serveur de connexion est exécutée et accessible pour la nouvelle machine sur laquelle vous prévoyez d'installer le Serveur de connexion.
Lorsque vous installez le Serveur de connexion sur le nouvel hôte, vous pointerez vers cette instance existante.
- 2 Sur la nouvelle machine, installez une instance répliquée du Serveur de connexion.
L'instance d'Horizon LDAP sur la nouvelle instance réplique celle de l'instance source mise à niveau.
- 3 Le cas échéant, désinstallez le Serveur de connexion de l'ancien hôte en utilisant l'utilitaire **Ajout/Suppression de programmes** de Windows.
- 4 Dans Horizon Console, accédez à l'onglet **Paramètres > Serveurs > Serveurs de connexion** et déterminez si l'instance du Serveur de connexion qui a été désinstallée figure toujours dans la liste.
- 5 Si l'instance désinstallée du Serveur de connexion apparaît toujours dans la liste, utilisez une commande `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 du Serveur de connexion. Pour plus d'informations sur l'outil de ligne de commande `vdmadmin`, consultez le document *Administration d'Horizon*.

Résultats

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

Étape suivante

Effectuez la mise à niveau des autres composants serveur VMware Horizon.

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

Si vous utilisez des équilibrages de charge pour gérer l'accès aux Serveurs de connexion, mettez à jour la configuration de l'équilibrage de charge pour ajouter les Serveurs de connexion récemment installés et supprimez les Serveurs de connexion désaffectés (le cas échéant).

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

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

Si vous rétablissez le snapshot d'une machine virtuelle du Serveur de connexion, les objets Horizon LDAP de la base de données de cette machine virtuelle ne sont plus cohérents avec les objets Horizon 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 d'Horizon LDAP.`

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

Conditions préalables

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

Procédure

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

L'instance de base de données Horizon LDAP est appelée AD LDS Instance VMwareVDMDS.

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

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

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

Résultats

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

Mise à niveau des Serveurs de connexion en parallèle

Si votre déploiement dispose de plusieurs Serveurs de connexion, vous pouvez mettre à niveau les Serveurs de connexion en parallèle pour gagner du temps.

Avant d'effectuer une mise à niveau de plusieurs Serveurs de connexion en parallèle, vous devez vérifier les conditions préalables suivantes.

- Vérifiez qu'il n'existe aucun problème avec la réplication d'Horizon LDAP. Pour une mise à niveau réussie de plusieurs Serveurs de connexion en parallèle, l'instance d'Horizon LDAP locale et l'instance d'Horizon LDAP globale dans le cluster du Serveur de connexion doivent être dans un état cohérent. Le programme d'installation du Serveur de connexion bloque le processus de mise à niveau en cas de problèmes avec la réplication d'Horizon LDAP.

L'instance d'Horizon LDAP locale est créée lors de l'installation du premier Serveur de connexion et contient des données de configuration pour le cluster de Serveurs de connexion, ce qui inclut le Serveur de connexion et les serveurs réplica. Cette instance d'Horizon LDAP locale est répliquée sur tous les Serveurs de connexion dans un cluster unique.

L'instance d'Horizon LDAP globale est créée lorsque vous configurez l'environnement Architecture Cloud Pod et qu'elle contient des données de configuration pour une fédération de clusters ou d'espaces. Cette instance d'Horizon LDAP globale est répliquée sur tous les Serveurs de connexion de la fédération.

Pour déterminer s'il existe des problèmes lors de la réplication de l'instance d'Horizon LDAP locale, exécutez la commande suivante :

```
repadmin.exe /showrepl localhost:389
```

Pour déterminer s'il existe des problèmes lors de la réplication de l'instance d'Horizon LDAP globale dans un environnement Architecture Cloud Pod, exécutez la commande suivante :

```
repadmin.exe /showrepl localhost:22389
```

Pour obtenir des informations de dépannage supplémentaires, reportez-vous à la section [Dépannage des erreurs lors de la mise à niveau et de l'installation de Serveurs de connexion](#).

- Mettez à niveau un Serveur de connexion pour déterminer s'il existe des problèmes avec la réplication d'Horizon LDAP. Après avoir résolu les erreurs pendant le processus de mise à niveau, vous pouvez procéder à la mise à niveau de plusieurs Serveurs de connexion en parallèle.
- Placez tous les nœuds Horizon LDAP dans le cluster de Serveurs de connexion avant la mise à niveau. Cela garantit la disponibilité du nœud master du schéma sur le cluster. La mise à niveau échoue si le nœud principal du schéma est supprimé du cluster. Si le nœud master du schéma est supprimé, vous pouvez utiliser la commande `vdmadmin -X` pour faire du nœud actuel le nœud master du schéma. Pour plus d'informations sur la commande `vdmadmin -X`, reportez-vous à la section « Détection et résolution des collisions d'entrée et de schéma LDAP à l'aide de l'option -X » dans le document *Administration d'Horizon*.
- Vous pouvez mettre à niveau tous les Serveurs de connexion dans trois espaces à la fois.

Utilisez le processus suivant pour mettre à niveau tous les Serveurs de connexion dans un espace en parallèle :

- 1 Mettez à niveau toutes les instances du Serveur de connexion dans les espaces. Reportez-vous à la section [Mise à niveau de Serveurs de connexion dans un groupe répliqué](#).

Note Le programme d'installation du Serveur de connexion s'interrompt pendant une durée plus longue que d'habitude lors de la dernière étape, car il attend que tous les services démarrent.

Dépannage des erreurs lors de la mise à niveau et de l'installation de Serveurs de connexion

Le programme d'installation du Serveur de connexion présente certaines restrictions qui peuvent bloquer le processus d'installation du Serveur de connexion lorsque vous mettez à niveau des Serveurs de connexion en parallèle. Ces restrictions s'appliquent également aux mises à niveau du Serveur de connexion individuelles et aux nouvelles installations des serveurs répliqués.

Problème

Lorsque vous exécutez les programmes d'installation du Serveur de connexion lors de l'exécution d'une mise à niveau ou de l'installation de Serveurs de connexion, le programme d'installation du Serveur de connexion peut afficher des messages d'erreur et bloquer le processus d'installation.

Cause

Des erreurs d'installation ou de mise à niveau du Serveur de connexion peuvent se produire lorsque le nœud principal du schéma n'est pas disponible ou qu'il est supprimé du cluster LDAP. Le nœud principal du schéma est supprimé lorsqu'une instance du Serveur de connexion est supprimée à l'aide de la commande `vdmadmin -S` sans désinstallation propre des instances de LDAP.

Solution

- 1 Si l'erreur d'installation se produit en raison de l'indisponibilité du nœud master du schéma, activez tous les nœuds du cluster LDAP spécifiés dans le message d'erreur.

Si l'activation de tous les nœuds du cluster LDAP ne résout pas le problème, l'erreur peut se produire en raison de la suppression du nœud master du schéma du cluster. Passez à l'étape 2 pour résoudre l'erreur.

- 2 Si le nœud master du schéma est supprimé du cluster LDAP, vous devez définir un autre nœud comme nœud master du schéma sur le cluster. Les étapes pour faire d'un autre nœud le nœud maître du schéma sur le cluster varient selon la mise à niveau de tous les nœuds ou aucun d'entre eux vers VMware Horizon version 2006 sur le cluster.

- Si un nœud est mis à niveau vers VMware Horizon version 2006 sur le cluster, vous pouvez utiliser la commande `vdmadmin -X` pour faire du nœud actuel le nœud master du schéma. Pour plus d'informations sur la commande `vdmadmin -X`, reportez-vous à la section « Détection et résolution des collisions d'entrée et de schéma LDAP à l'aide de l'option -X » dans le document *Administration d'Horizon*.
- Pour faire du nœud actuel le nœud principal du schéma sur le cluster pour une instance LDAP locale, entrez la commande suivante :

```
vdmadmin -X -seizeSchemaMaster
```

- Pour faire du nœud actuel le nœud master du schéma sur le cluster pour une instance LDAP globale dans un environnement Architecture Cloud Pod, entrez la commande suivante.

```
vdmadmin -X -seizeSchemaMaster -global
```

- Si aucun des nœuds n'est mis à niveau vers VMware Horizon version 2006 sur le cluster, utilisez la commande `dsmgmt` pour faire du nœud actuel le nœud master du schéma.
- Pour faire du nœud actuel le nœud master du schéma sur le cluster pour une instance LDAP locale, entrez la commande suivante :

```
dsmgmt "roles" "connections" "connect to server localhost:389" "quit" "transfer
schema master" "quit" "quit"
```

- Pour faire du nœud actuel le nœud principal du schéma sur le cluster pour une instance LDAP globale, entrez la commande suivante :

```
dsmgmt "roles" "connections" "connect to server localhost:22389" "quit" "transfer
schema master" "quit" "quit"
```

Mise à niveau des serveurs d'inscription

Vous pouvez mettre à niveau un serveur d'inscription en exécutant la dernière version du programme d'installation du Serveur de connexion sur la machine virtuelle sur laquelle une version antérieure d'un serveur d'inscription est déjà installée. Vous pouvez également désinstaller la version antérieure d'un serveur d'inscription et installer la dernière version en exécutant la dernière version du programme d'installation du Serveur de connexion et en sélectionnant l'option Serveur d'inscription.

Un serveur d'inscription est sans état. La configuration associée à l'authentification unique réelle n'est pas conservée sur le serveur d'inscription. Le serveur d'inscription reçoit la configuration de l'authentification unique réelle du Serveur de connexion lorsque le serveur d'inscription est en cours d'exécution et que le Serveur de connexion se connecte au serveur d'inscription.

Note Après la mise à niveau, il n'est pas nécessaire d'importer manuellement le ou les certificats de couplage à partir du Serveur de connexion vers le magasin de certificats Windows du serveur d'inscription à nouveau. Le ou les certificats de couplage manuellement importés précédemment ne sont pas supprimés lors de la désinstallation ou de la mise à niveau. Lorsque le serveur d'inscription est en cours d'exécution après une mise à niveau, le Serveur de connexion peut se connecter et le ou les certificats de couplage précédemment importés sont réutilisés.

Mise à niveau d'un environnement Architecture Cloud Pod

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

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

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

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

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

Mise à niveau de serveurs VMware Horizon pour autoriser HTML Access

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

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

Mettre à niveau vCenter Server

Exécutez une mise à niveau de vCenter Server lors de la période de maintenance au cours de laquelle vous mettez à niveau d'autres composants de serveur VMware Horizon. Avant de mettre à niveau vCenter Server, vous devez sauvegarder certaines données d'VMware Horizon.

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

- Les postes de travail à distance en état de provisionnement ne seront pas activés.
- Les nouveaux postes de travail ne seront pas activés.

Conditions préalables

- Déterminez quand effectuer cette procédure. Choisissez une période de maintenance de poste de travail disponible. Pour plus d'informations sur le temps nécessaire, reportez-vous au *Guide de mise à niveau de VMware vSphere*.
- Sauvegardez la base de données vCenter Server.

- Sauvegardez la base de données de l'annuaire Horizon (Horizon Directory) à partir d'une instance du Serveur de connexion à l'aide de l'utilitaire `vdmexport.exe`.
Pour obtenir des instructions, reportez-vous au document *Administration d'Horizon*. Si vous possédez plusieurs instances du Serveur de connexion dans un groupe répliqué, vous devez exporter les données à partir d'une seule instance.
- Vérifiez que le serveur sur lequel vCenter Server est installé possède un certificat de serveur TLS signé par une autorité de certification installée et configuré. Après la mise à niveau du Serveur de connexion, si vCenter Server n'utilise pas de certificat signé par une autorité de certification, le certificat auto-signé par défaut est affiché comme étant non valide dans Horizon Console, et un message indique que vCenter Server n'est pas disponible.
- Remplissez les conditions préalables répertoriées dans le *Guide de mise à niveau de VMware vSphere*, en utilisant la version du guide qui correspond à la version de vSphere vers laquelle vous prévoyez d'effectuer la mise à niveau.
- Pour mettre à niveau vCenter Server lorsque des Instant Clones sont en cours d'utilisation, reportez-vous aux étapes décrites dans l'article de la base de connaissances de VMware <https://kb.vmware.com/s/article/52573>.

Procédure

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

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

- 2 Connectez-vous à Horizon Console et examinez le tableau de bord pour vérifier que l'icône vCenter Server est verte.

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

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

Étape suivante

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

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

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

- Si vous mettez à niveau uniquement des composants VMware Horizon, reportez-vous à la section [Mettre à niveau Horizon Agent](#).

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

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

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

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

Pour plus d'informations sur la configuration des certificats TLS, reportez-vous à la section « Configuration de certificats TLS pour des instances de VMware Horizon Server » dans le document *Installation d'Horizon*.

Vous devez ajouter d'abord vCenter Server dans Horizon Console à l'aide de l'assistant Ajouter vCenter Server. Si un certificat n'est pas approuvé et si vous n'acceptez pas l'empreinte numérique, vous ne pouvez pas ajouter vCenter Server.

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

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

Dans le tableau de bord d'Horizon Console, l'icône vCenter Server devient rouge et une boîte de dialogue Certificat non valide détecté s'affiche. Dans Horizon Console, cliquez sur **Paramètres** > **Serveurs** et sélectionnez l'instance de vCenter Server. Cliquez ensuite sur **Modifier** dans les paramètres de vCenter Server et suivez les invites pour vérifier et accepter le certificat autosigné.

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

Procédure

- 1 Lorsque Horizon Console 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 numérique de certificat qui a été configurée pour vCenter Server.
 - a Sur l'hôte vCenter Server, démarrez le composant logiciel enfichable MMC et ouvrez le magasin de certificats Windows.
 - b Accédez au certificat de vCenter Server.
 - 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 numérique dans la fenêtre Informations sur le certificat correspond à celle de vCenter Server.

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.

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

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

Tous les fichiers ADMX qui fournissent des paramètres de stratégie de groupe Horizon sont disponibles dans `VMware-Horizon-Extras-Bundle-YYMM-x.x.x-yyyyyyyyy.zip`, où *YYMM* est la version marketing, *x.x.x* est la version interne et *yyyyyyyyy* est le numéro de build. Vous pouvez télécharger le fichier sur le site de téléchargements de VMware à l'adresse <https://my.vmware.com/web/vmware/downloads>. Sous Informatique de bureau et d'utilisateur final, sélectionnez le téléchargement de VMware Horizon, qui comprend le bundle GPO contenant le fichier ZIP.

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

Les modèles de fichier ADMX d'Horizon 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'VMware Horizon.

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

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

Conditions préalables

- Effectuez la procédure décrite dans la section [Mise à niveau de Serveurs de connexion dans un groupe répliqué](#)
- Effectuez les tâches de préparation de la mise à niveau d'ESXi répertoriées dans le *Guide de mise à niveau de VMware vSphere*.

Procédure

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

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

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

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

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

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

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

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

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

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

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

Étape suivante

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

Mise à niveau des postes de travail publiés et virtuels

7

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

Important Ce chapitre ne couvre pas la mise à niveau d'Horizon Agent sur une machine virtuelle Linux. Pour obtenir ces informations, reportez-vous au document *Configuration des postes de travail Linux dans Horizon*.

La stratégie de mise à niveau dépend du type de source de poste de travail :

- Pour un pool automatisé de postes de travail de clone complet, vous devez mettre à niveau Horizon Agent individuellement sur chaque poste de travail virtuel. Vous devrez également mettre à niveau Horizon Agent dans la VM modèle que vous avez utilisée pour créer les postes de travail de clone complet. En cas de développement du pool, des postes de travail supplémentaires sont créés à l'aide de la VM modèle mise à jour.
- Pour un pool manuel de machines virtuelles vCenter, de machines virtuelles non-vCenter et de PC physiques, vous devez mettre à niveau Horizon Agent individuellement sur chaque machine.
- Pour un pool automatisé de postes de travail d'Instant Clone, vous devez mettre à niveau Horizon Agent sur l'image standard. Ensuite, vous pouvez propager la nouvelle image standard dans le pool de postes de travail d'Instant Clone en effectuant une opération d'image de transfert.
- Pour un pool de postes de travail RDS, vous devez mettre à niveau Horizon Agent sur un ou plusieurs hôtes des services Terminal Server ou sur l'hôte RDS Microsoft. Reportez-vous à la section [Mettre à niveau les hôtes RDS qui fournissent des postes de travail basés sur une session](#).

Ce chapitre contient les rubriques suivantes :

- [Mettre à niveau Horizon Agent](#)
- [Mettre à niveau des pools de postes de travail d'Instant Clone lorsque vous mettez à niveau vCenter Server vers vSphere 6.7 ou version ultérieure](#)
- [Mettre à niveau les hôtes RDS qui fournissent des postes de travail basés sur une session](#)

Mettre à niveau Horizon Agent

Vous devez mettre à niveau Horizon Agent sur l'image standard pour un pool de postes de travail d'Instant Clone.

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

Si vous prévoyez de déployer des Instant Clones, vous pouvez utiliser cette procédure pour créer une image standard pour un pool de postes de travail d'Instant Clone. Lorsque vous mettez à niveau Horizon Agent sur une image standard, sélectionnez simplement l'option appropriée pour un pool de postes de travail d'Instant Clone.

Conditions préalables

- Vérifiez que toutes les instances du Serveur de connexion dans le groupe répliqué ont été mises à niveau. Toutes les instances du Serveur de connexion doivent d'abord être mises à niveau pour que le mécanisme de couplage JMS sécurisé puisse fonctionner avec Horizon Agent.
- Si vous effectuez la mise à niveau d'hôtes ESXi et de machines virtuelles, effectuez la procédure décrite dans la section [Chapitre 6 Mettre à niveau des hôtes ESXi et leurs machines virtuelles](#).
- Vérifiez que vous possédez un compte d'utilisateur de domaine avec des privilèges d'administration sur les hôtes que vous utilisez pour exécuter le programme d'installation et réaliser la mise à niveau.

Procédure

- 1 Mettez à niveau le logiciel agent sur une image standard ou sur un modèle de VM, puis créez un pool de postes de travail d'Instant Clone ou un pool de postes de travail de clone complet, en fonction de votre cas d'utilisation à des fins de test. Vous pouvez également, si vous utilisez un pool de postes de travail manuel, le tester sur un poste de travail du pool.

- a Téléchargez et exécutez la nouvelle version du programme d'installation d'Horizon Agent sur l'image standard ou sur le modèle de VM.

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

- b Créez un petit pool de postes de travail à partir de cette machine virtuelle.
- c Testez un poste de travail de machine virtuelle du pool de postes de travail pour vérifier que tous les scénarios d'utilisation fonctionnent correctement.

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

Des instructions pas à pas pour l'exécution du programme d'installation d'Horizon Agent et la création de pools de postes de travail s'affichent dans *Configuration des postes de travail virtuels dans Horizon*, disponible en cliquant sur le bouton **Aide** dans Horizon Console.

- 2 Répétez l'étape 1 sur toutes vos images standard et tous vos modèles de machines virtuelles.
- 3 Si vous prévoyez de créer des pools de postes de travail d'Instant Clone, prenez un snapshot de chaque image standard mise à niveau.

Accédez au pool que vous souhaitez mettre à niveau et effectuez une opération d'image de transfert. Pour plus d'informations sur l'exécution d'une opération d'image de transfert, reportez-vous au document *Configuration des postes de travail virtuels dans Horizon*.

Pour plus d'instructions sur la prise de snapshots, consultez l'aide en ligne de vSphere Client.

- 4 Si vous utilisez un pool de postes de travail automatisé de clones complets ou un pool de postes de travail manuel, mettez à niveau le logiciel agent sur chaque poste de travail virtuel à l'aide des outils tiers que vous utilisez généralement pour les mises à niveau logicielles.

Si votre pool de postes de travail est un pool de postes de travail de clone complet automatisé, prenez un snapshot du nouveau modèle de VM. Si vous développez ultérieurement votre pool, de nouveaux postes de travail virtuels sont créés à partir du modèle de machine virtuelle ou du snapshot mis à jour.

- 5 Pour les pools autres qu'Instant Clone, modifiez les paramètres de pool pour activer la fonctionnalité de rendu 3D.
 - a Configurez les paramètres de pool suivants :
 - Pour les pools de postes de travail Windows, définissez le pool pour qu'il utilise le protocole d'affichage PCoIP ou VMware Blast. Pour les pools de postes de travail Linux, configurez le pool pour qu'il utilise le protocole d'affichage VMware Blast.
 - Définissez **Autoriser les utilisateurs à choisir un protocole** sur **Non**.
 - Pour les pools de postes de travail Windows, activez la fonctionnalité **Convertisseur 3D**. Pour les pools de postes de travail Linux, sélectionnez **NVIDIA GRID vGPU** si vous avez configuré ce vGPU ou sélectionnez **Gérer à l'aide de vSphere Client**.
 - b Pour les pools de postes de travail Windows uniquement, mettez la machine virtuelle hors tension et remettez-la sous tension.

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

- 6 Téléchargez et exécutez le programme d'installation de la nouvelle version d'Horizon Agent sur toutes les machines que vous utilisez comme hôtes RDS. Dans Windows, les hôtes RDS peuvent être des PC physiques ou des machines virtuelles. Dans Linux, seules les machines virtuelles peuvent servir d'hôtes RDS.

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

Important Lorsque vous exécutez le programme d'installation sur l'hôte RDS d'une machine virtuelle Windows, le composant **View Composer Agent** est désélectionné. Ne sélectionnez pas ce composant durant une mise à niveau.

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

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

Important Sur les systèmes d'exploitation Windows Server configurés pour une utilisation de poste de travail, si vous ne souhaitez pas modifier le mode d'installation de Horizon Agent pendant la mise à niveau, sélectionnez **Mode de poste de travail** dans le programme d'installation de Horizon Agent et poursuivez. Pour changer de mode, sélectionnez **Mode RDS** et suivez les instructions du programme d'installation pour procéder à la mise à niveau.

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

Mettre à niveau des pools de postes de travail d'Instant Clone lorsque vous mettez à niveau vCenter Server vers vSphere 6.7 ou version ultérieure

vSphere 6.7 dispose d'une nouvelle API pour les Instant Clones. Par conséquent, si vous utilisez des Instant Clones et si vous effectuez une mise à niveau d'une version de vSphere antérieure à 6.7 vers vSphere 6.7 ou version ultérieure, vous devez effectuer les étapes de ce processus de mise à niveau. Par exemple, si vous effectuez une mise à niveau de vSphere 6.0 vers vSphere 6.7, de vSphere 6.5 vers vSphere 6.7 ou de vSphere 6.5 vers vSphere 7.0, ce processus s'applique. Ce processus ne s'applique pas si vous effectuez une mise à niveau de vSphere 6.7 vers vSphere 7.0.

Conditions préalables

- Effectuez la configuration système requise pour une mise à niveau vers VMware Horizon 2006 ou version ultérieure.
- Effectuez les procédures décrites dans la section [Mise à niveau d'Horizon Connection Server](#).
- Effectuez la procédure décrite dans la section [Mettre à niveau Horizon Agent](#) pour la mise à niveau de l'agent sur l'image standard.
- Remplissez les conditions préalables répertoriées dans le *Guide de mise à niveau de VMware vSphere*, en utilisant la version du guide qui correspond à la version de vSphere vers laquelle vous prévoyez d'effectuer la mise à niveau.

Note Si vous effectuez la mise à niveau de vCenter Server vers vSphere 6.7 ou version ultérieure, vous devez mettre à niveau tous les hôtes ESXi du cluster ou certains d'entre eux vers la version la plus récente. Sinon, les pools de postes de travail d'Instant Clone ne seront pas approvisionnés correctement.

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

Procédure

- 1 Prenez un snapshot de l'image standard sur laquelle vous mettez à niveau Horizon Agent vers VMware Horizon 2006 ou une version ultérieure.
- 2 Définissez le seuil de migration du DRS (Distributed Resource Scheduler) de stockage sur 3 dans le cluster.
- 3 Désactivez les pools de postes de travail d'Instant Clone.
- 4 Mettez à niveau vCenter Server vers vSphere 6.7 ou version ultérieure.
- 5 Pour mettre en mode de maintenance les hôtes que vous prévoyez de mettre à niveau, choisissez l'une des options suivantes.
 - Mettez l'hôte directement en mode de maintenance à partir de vSphere Client, puis mettez à niveau l'hôte vers vSphere 6.7 ou version ultérieure. Une fois la mise à niveau terminée, utilisez vSphere Client pour quitter le mode de maintenance.

- Utilisez l'utilitaire `icmaint.cmd` pour marquer un hôte pour la maintenance avec l'option **ON**. Le marquage d'un hôte pour la maintenance supprime les images standard, qui sont les VM parentes dans vCenter Server à partir de l'hôte ESXi. Mettez l'hôte en mode de maintenance et effectuez la mise à niveau vers la nouvelle version d'ESXi. Une fois la mise à niveau terminée, sortez l'hôte du mode de maintenance. Ensuite, utilisez `icmaint.cmd` pour annuler le marquage de l'hôte pour la maintenance avec l'option **OFF**.

Note Vous devez mettre à niveau au moins un hôte afin de pouvoir reprendre l'approvisionnement des pools de postes de travail. Ensuite, vous devez mettre à niveau tous les autres hôtes.

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

Seuls les hôtes mis à niveau vers la nouvelle version d'ESXi sont utilisés pour l'approvisionnement. Les Instant Clones créés lors de l'opération d'image de transfert peuvent être migrés vers d'autres hôtes qui n'utilisent pas encore la nouvelle version de vSphere.
- 8 Vérifiez que tous les hôtes du cluster sont mis à niveau vers la nouvelle version de vSphere.
- 9 Si vous mettez l'image standard à niveau à partir d'une version précédente pour qu'elle soit compatible avec ESXi 6.7 et version ultérieure (VM version 14), mettez à niveau VMware Tools sur l'image standard. Vous devez prendre un nouveau snapshot de l'image standard qu'Horizon utilise pour effectuer une opération d'image de transfert sur tous les pools de postes de travail d'Instant Clone qui utilisaient la version précédente de cette image standard.
- 10 Si vous mettez à niveau le commutateur virtuel distribué (vDS), activez l'image standard pour vérifier l'absence de problèmes réseau. Après la mise à niveau d'un vDS, vous devez prendre un nouveau snapshot de l'image standard et effectuer une opération d'image de transfert sur tous les pools de postes de travail d'Instant Clone.

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

Sur les hôtes RDS disposant de Windows Server 2012 R2 ou d'un système d'exploitation de version ultérieure, vous pouvez mettre à niveau le logiciel Horizon Agent et modifier les paramètres de pool pour que l'hôte RDS puisse fournir des postes de travail distants et des applications Windows distantes.

Conditions préalables

- Vérifiez qu'au moins une instance du Serveur de connexion Horizon dans le groupe répliqué a été mise à niveau. Le Serveur de connexion doit d'abord être mis à niveau pour que le mécanisme de couplage JMS sécurisé puisse fonctionner avec Horizon Agent.

- Vérifiez que l'hôte RDS hébergeant actuellement des postes de travail distants exécute une version prise en charge des systèmes d'exploitation Windows Server. Si vous ne disposez pas d'un système d'exploitation Windows Server pris en charge, vous devez effectuer une toute nouvelle installation plutôt qu'une mise à niveau. Pour consulter la liste des systèmes d'exploitation pris en charge, reportez-vous à [Exigences et considérations pour Horizon Agent](#).
- Vérifiez que le rôle Hôte RDS est installé dans le système d'exploitation. Reportez-vous à la procédure intitulée « Installer les services Bureau à distance » dans le document *Configuration d'applications et de postes de travail publiés dans Horizon*.
- Familiarisez-vous avec la procédure d'exécution du programme d'installation d'Horizon Agent. Consultez la procédure « Installer Horizon Agent sur un hôte des services Bureau à distance » dans *Configuration d'applications et de postes de travail publiés dans Horizon*, disponible en cliquant sur le bouton **Aide** dans Horizon Console.
- Vérifiez que vous avez fermé votre session sur tous les postes de travail distants et sur toutes les applications distantes.
- Vérifiez que vous possédez un compte d'utilisateur de domaine avec des privilèges d'administration sur les hôtes que vous utilisez pour exécuter le programme d'installation et réaliser la mise à niveau.

Procédure

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

Accédez à **Inventaire > Postes de travail**, sélectionnez le pool, puis cliquez sur **Modifier**.

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

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

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

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

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

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

Résultats

Cet hôte peut dorénavant fournir des applications distantes en plus de postes de travail distants. Dans Horizon Console, si vous accédez à **Inventaire > Postes de travail**, vous constatez que le

type de pool est **Pool de postes de travail RDS**. Si vous accédez à **Inventaire > Batteries de serveurs**, un ID de batterie de serveurs s'affiche dans la liste ; il correspond à l'ID de pool.

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



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

Plutôt que d'effectuer une mise à niveau intégrée des composants VMware Horizon et vSphere, vous pouvez commencer par mettre à niveau tous les composants VMware Horizon, 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 VMware Horizon, vous devez effectuer les tâches supplémentaires suivantes :

- 1 Avant de mettre à niveau vCenter Server, sauvegardez la base de données vCenter Server.
- 2 Avant de mettre à niveau vCenter Server, sauvegardez la base de données de l'annuaire Horizon (Horizon Directory) à partir d'une instance du Horizon Connection Server à l'aide de l'utilitaire `vdmexport.exe`.

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