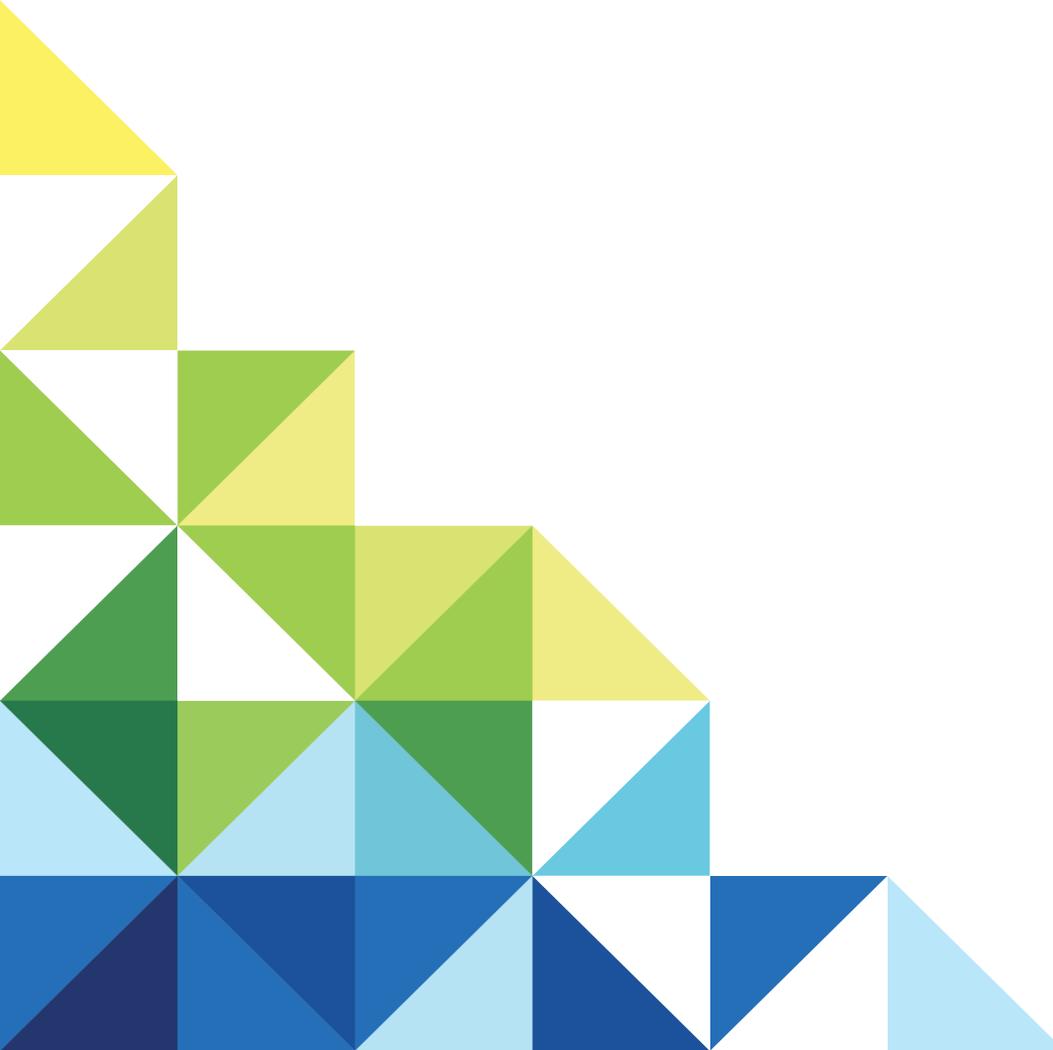


Sécurité d'Horizon Client et d'Horizon Agent

Horizon Client 3.x/4.x/5.x et View Agent 6.2.x/Horizon
Agent 7.x

14 mars 2019

VMware Horizon 7 7.8



vmware®

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

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

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

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

docfeedback@vmware.com

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

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

Copyright © 2015–2019 VMware, Inc. Tous droits réservés. [Informations sur le copyright et les marques commerciales.](#)

Table des matières

Sécurité d'Horizon Client et d'Horizon Agent	5
1 Ports externes	7
Comprendre les protocoles de communication	7
Règles de pare-feu pour View Agent ou Horizon Agent	8
Ports TCP et UDP utilisés par des clients et des agents	9
2 Services, démons et processus installés	14
Services installés par le programme d'installation de View Agent ou Horizon Agent sur des machines Windows	14
Services installés sur le client Windows	15
Démons installés dans d'autres clients et le poste de travail Linux	16
3 Ressources à sécuriser	17
Implémentation de meilleures pratiques pour sécuriser des systèmes client	17
Emplacements des fichiers de configuration	17
Comptes	18
4 Paramètres de sécurité pour le client et l'agent	20
Configuration de la vérification des certificats	20
Paramètres liés à la sécurité dans les modèles de configuration de View Agent et Horizon Agent	21
Définir des options dans des fichiers de configuration sur un poste de travail Linux	23
Paramètres de stratégie de groupe pour HTML Access	35
Paramètres de sécurité des modèles de configuration d' Horizon Client	36
Configuration du mode de vérification de certificat d' Horizon Client	40
Configuration de la protection LSA	41
5 Configuration des protocoles de sécurité et des suites de chiffrement	42
Stratégies par défaut pour les protocoles de sécurité et les suites de chiffrement	42
Configuration des protocoles de sécurité et des suites de chiffrement pour des types de client spécifiques	51
Désactiver des chiffrements faibles dans les protocoles SSL/TLS	52
Configurer des protocoles de sécurité et des suites de chiffrement pour l'agent HTML Access	53
Configurer des stratégies de proposition sur des postes de travail distants	54
6 Emplacements des fichiers journaux du client et de l'agent	55
Journaux d'Horizon Client pour Windows	55
Journaux d'Horizon Client pour Mac	58

[Journaux d'Horizon Client pour Linux](#) 59

[Journaux d'Horizon Client sur des périphériques mobiles](#) 60

[Journaux d' Horizon Agent de machines Windows](#) 62

[Journaux de poste de travail Linux](#) 63

7 Application de correctifs de sécurité 65

[Appliquer un correctif pour View Agent ou Horizon Agent](#) 65

[Appliquer un correctif à Horizon Client](#) 66

Sécurité d'Horizon Client et d'Horizon Agent

Sécurité d'Horizon Client et d'Horizon Agent est une référence concise aux fonctionnalités de sécurité de VMware Horizon[®] Client™ et d'Horizon Agent (pour Horizon 7) ou VMware View Agent[®] (pour Horizon 6). Ce guide est un complément du guide *Sécurité d'Horizon 7*, qui est produit pour chaque version majeure et mineure de VMware Horizon™ 6 et d'Horizon 7. Le guide *Sécurité d'Horizon Client et d'Horizon Agent* est mis à jour tous les trimestres, avec les versions correspondantes des logiciels client et agent.

Horizon Client est l'application que les utilisateurs finaux lancent sur leurs périphériques clients pour se connecter à une application ou un poste de travail distant. View Agent (pour Horizon 6) ou Horizon Agent (pour Horizon 7) est le logiciel agent qui s'exécute dans le système d'exploitation du poste de travail distant ou de l'hôte RDS Microsoft qui fournit les applications distantes. Le guide inclut les informations suivantes :

- Comptes de connexion au système requis. ID de connexion des comptes créés lors de l'installation ou du démarrage du système et instructions pour modifier les valeurs par défaut.
- Options et paramètres de configuration qui ont des implications en matière de sécurité.
- Ressources qui doivent être protégées, telles que des fichiers et des mots de passe de configuration liés à la sécurité, et contrôles d'accès recommandés pour un fonctionnement sécurisé.
- Emplacement des fichiers journaux et leur objectif.
- Privilèges attribués aux utilisateurs de service.
- Interfaces, ports et services externes qui doivent être ouverts ou activés pour le fonctionnement correct du client et de l'agent.
- Informations précisant comment les clients peuvent obtenir et appliquer la dernière mise à jour de sécurité ou le correctif de sécurité le plus récent.

Public visé

Ces informations s'adressent aux décideurs, architectes, administrateurs informatiques et autres personnes qui doivent se familiariser avec les composants de sécurité d'Horizon 6 ou Horizon 7, notamment le client et l'agent.

Glossaire VMware Technical Publications

Les publications techniques VMware fournissent un glossaire de termes que vous ne connaissez peut-être pas. Pour obtenir la définition des termes tels qu'ils sont utilisés dans la documentation technique de VMware, visitez la page <http://www.vmware.com/support/pubs>.

Ports externes

Pour un fonctionnement correct du produit, et selon les fonctionnalités que vous voulez utiliser, divers ports doivent être ouverts pour que les clients et l'agent sur des postes de travail distants puissent communiquer entre eux.

Ce chapitre contient les rubriques suivantes :

- [Comprendre les protocoles de communication](#)
- [Règles de pare-feu pour View Agent ou Horizon Agent](#)
- [Ports TCP et UDP utilisés par des clients et des agents](#)

Comprendre les protocoles de communication

Les composants d'Horizon 6 et Horizon 7 échangent des messages en utilisant plusieurs protocoles différents.

[Tableau 1-1](#) répertorie les ports par défaut utilisés par chaque protocole. Si nécessaire, pour respecter les stratégies d'entreprise ou pour éviter la contention, vous pouvez modifier les numéros de port utilisés.

Tableau 1-1. Ports par défaut

Protocole	Port
JMS	Port TCP 4001 Port TCP 4002
HTTP	Port TCP 80
HTTPS	Port TCP 443
MMR/CDR	Pour la redirection multimédia et la redirection de lecteur client, port TCP 9427
RDP	Port TCP 3389
PCoIP	Port TCP 4172 Ports UDP 4172, 50002, 55000
redirection USB	Port TCP 32111. Ce port est également utilisé pour la synchronisation de fuseau horaire.
VMware Blast	Ports TCP 8443, 22443
Extreme	Ports UDP 443, 8443, 22443
HTML Access	Ports TCP 8443, 22443

Règles de pare-feu pour View Agent ou Horizon Agent

Les programmes d'installation de View Agent et d'Horizon Agent peuvent éventuellement configurer des règles de pare-feu Windows sur des postes de travail distants et des hôtes RDS pour ouvrir les ports réseau par défaut. Les ports sont entrants sauf indication contraire.

Les programmes d'installation de View Agent et d'Horizon Agent configurent la règle de pare-feu locale pour les connexions RDP entrantes pour qu'elle corresponde au port RDP actuel du système d'exploitation hôte, qui est en général le port 3389.

Si vous demandez au programme d'installation de View Agent ou d'Horizon Agent de ne pas activer la prise en charge du Poste de travail distant, il n'ouvre pas les ports 3389 et 32111 et vous devez ouvrir ces ports manuellement.

Si vous modifiez le numéro du port RDP après l'installation, vous devez modifier les règles de pare-feu associées. Si vous modifiez un port par défaut après l'installation, vous devez reconfigurer manuellement les règles de pare-feu Windows pour autoriser l'accès sur le port mis à jour. Reportez-vous à la section « Remplacement des ports par défaut pour les services View » dans le document *Installation d'Horizon 7*.

Les règles de pare-feu Windows de View Agent ou d'Horizon Agent sur des hôtes RDS indiquent un bloc de 256 ports UDP contigus ouverts pour le trafic entrant. Ce bloc de ports est destiné à une utilisation interne de VMware Blast dans View Agent ou Horizon Agent. Un pilote spécial signé par Microsoft sur les hôtes RDS bloque le trafic entrant de sources externes vers ces ports. À cause de ce pilote, le pare-feu Windows traite les ports comme étant fermés.

Si vous utilisez un modèle de machine virtuelle en tant que source de postes de travail, les exceptions de pare-feu ne continuent sur les postes de travail déployés que si le modèle est membre du domaine de poste de travail. Vous pouvez utiliser les paramètres de stratégie de groupe de Microsoft pour gérer les exceptions de pare-feu locales. Pour plus d'informations, consultez l'article 875357 de la base de connaissances de Microsoft.

Tableau 1-2. Ports TCP et UDP ouverts pendant l'installation de View Agent ou d'Horizon Agent

Protocole	Ports
RDP	Port TCP 3389
Redirection USB et synchronisation de fuseau horaire	Port TCP 32111
MMR (redirection multimédia) et CDR (redirection de lecteur client)	Port TCP 9427
PCoIP	Pour les hôtes RDS, PCoIP utilise les numéros de port suivants : port TCP 4172 et port UDP 4172 (bidirectionnel). Pour les postes de travail, PCoIP utilise les numéros de port choisis dans une plage configurable. Par défaut, les ports TCP 4172 à 4173 et les ports UDP 4172 à 4182. Les règles de pare-feu de ces ports ne spécifient pas les numéros de port, mais suivent dynamiquement les ports ouverts par chaque serveur PCoIP Server. Les numéros de port choisis sont communiqués au client via le Serveur de connexion.

Tableau 1-2. Ports TCP et UDP ouverts pendant l'installation de View Agent ou d'Horizon Agent (Suite)

Protocole	Ports
VMware Blast	Port TCP 22443 Port UDP 22443 (bidirectionnel) Note UDP n'est pas utilisé sur les postes de travail Linux.
HTML Access	Port TCP 22443
XDMCP	UDP 177 Note Ce port est ouvert pour l'accès XDMCP uniquement sur les postes de travail Linux exécutant Ubuntu 18.04. Les règles de pare-feu bloquent tous les accès de l'hôte externe à ce port.
X11	TCP 6100 Note Ce port est ouvert pour l'accès XServer uniquement sur les postes de travail Linux exécutant Ubuntu 18.04. Les règles de pare-feu bloquent tous les accès de l'hôte externe à ce port.

Ports TCP et UDP utilisés par des clients et des agents

View Agent (pour Horizon 6), Horizon Agent (pour Horizon 7) et Horizon Client utilisent des ports TCP et UDP pour l'accès réseau entre eux et divers composants du serveur.

Tableau 1-3. Ports TCP et UDP utilisés par View Agent ou Horizon Agent

Source	Port	Cible	Port	Protocole	Description
Horizon Client	*	View Agent/Horizon Agent	3389	TCP	Trafic Microsoft RDP vers des postes de travail distants si des connexions directes sont utilisées à la place de connexions par tunnel.
Horizon Client	*	View Agent/Horizon Agent	9427	TCP	Redirection multimédia (MMR) Windows Media et redirection de lecteur client, si des connexions directes sont utilisées à la place de connexions par tunnel. Note Non requis pour la redirection du lecteur client lorsque VMware Blast est utilisé.
Horizon Client	*	View Agent/Horizon Agent	32111	TCP	Redirection USB et synchronisation de fuseau horaire si des connexions directes sont utilisées à la place de connexions par tunnel.
Horizon Client	*	View Agent/Horizon Agent	4172	TCP et UDP	PCoIP, si PCoIP Secure Gateway n'est pas utilisé. Note Comme le port source varie, voir la note sous ce tableau.
Horizon Client	*	Horizon Agent	22443	TCP et UDP	VMware Blast si des connexions directes sont utilisées à la place de connexions par tunnel. Note UDP n'est pas utilisé sur les postes de travail Linux.

Tableau 1-3. Ports TCP et UDP utilisés par View Agent ou Horizon Agent (Suite)

Source	Port	Cible	Port	Protocole	Description
Navigateur	*	View Agent/Horizon Agent	22443	TCP	HTML Access si des connexions directes sont utilisées à la place de connexions par tunnel.
Serveur de sécurité, Serveur de connexion ou dispositif Unified Access Gateway	*	View Agent/Horizon Agent	3389	TCP	Trafic Microsoft RDP vers des postes de travail distants quand des connexions par tunnel sont utilisées.
Serveur de sécurité, Serveur de connexion ou dispositif Unified Access Gateway	*	View Agent/Horizon Agent	9427	TCP	Redirection Windows Media MMR et redirection de lecteur client quand des connexions par tunnel sont utilisées.
Serveur de sécurité, Serveur de connexion ou dispositif Unified Access Gateway	*	View Agent/Horizon Agent	32111	TCP	Redirection USB et synchronisation de fuseau horaire quand des connexions par tunnel sont utilisées.
Serveur de sécurité, Serveur de connexion ou dispositif Unified Access Gateway	55000	View Agent/Horizon Agent	4172	UDP	PCoIP (pas SALSA20) si PCoIP Secure Gateway est utilisé.
Serveur de sécurité, Serveur de connexion ou dispositif Unified Access Gateway	*	View Agent/Horizon Agent	4172	TCP	PCoIP, si PCoIP Secure Gateway est utilisé.
Serveur de sécurité, Serveur de connexion ou dispositif Unified Access Gateway	*	Horizon Agent	22443	TCP et UDP	VMware Blast si Blast Secure Gateway est utilisé. Note UDP n'est pas utilisé sur les postes de travail Linux.
Serveur de sécurité, Serveur de connexion ou dispositif Unified Access Gateway	*	View Agent/Horizon Agent	22443	TCP	HTML Access si Blast Secure Gateway est utilisé.
View Agent/Horizon Agent	*	Serveur de connexion	4001, 4002	TCP	Trafic JMS SSL.

Tableau 1-3. Ports TCP et UDP utilisés par View Agent ou Horizon Agent (Suite)

Source	Port	Cible	Port	Protocole	Description
View Agent/Horizon Agent	4172	Horizon Client	*	UDP	PCoIP, si PCoIP Secure Gateway n'est pas utilisé. Note Comme le port cible varie, voir la note sous ce tableau.
View Agent/Horizon Agent	4172	Serveur de connexion, serveur de sécurité ou dispositif Unified Access Gateway	55000	UDP	PCoIP (pas SALSA20) si PCoIP Secure Gateway est utilisé.

Note Le numéro de port UDP que les agents utilisent pour le protocole PCoIP est susceptible de changer. Si le port 50002 est utilisé, l'agent choisira 50003. Si le port 50003 est utilisé, l'agent choisira le port 50004, etc. Vous devez configurer les pare-feu avec TOUS où un astérisque (*) est répertorié dans le tableau.

Tableau 1-4. Ports TCP et UDP utilisés par Horizon Client

Source	Port	Cible	Port	Protocole	Description
Horizon Client	*	Serveur de connexion, serveur de sécurité ou dispositif Unified Access Gateway	443	TCP	HTTPS pour la connexion à Horizon 6 ou Horizon 7. (Ce port est également utilisé pour le tunnelling quand des connexions par tunnel sont utilisées.) Note Horizon Client 4.4 et versions ultérieures prend en charge le port UDP 443 (voir ci-dessous).
Horizon Client 4.4 ou version ultérieure	*	Dispositif Unified Access Gateway 2.9 ou version ultérieure	443	UDP	HTTPS pour la connexion à Horizon 6 ou Horizon 7, si Blast Secure Gateway est utilisé et le serveur de tunnel UDP est activé. (Ce port est également utilisé pour le tunnelling quand des connexions par tunnel sont utilisées.)
Dispositif Unified Access Gateway 2.9 ou version ultérieure	443	Horizon Client 4.4 ou version ultérieure	*	UDP	HTTPS pour la connexion à Horizon 6 ou Horizon 7, si Blast Secure Gateway est utilisé et le serveur de tunnel UDP est activé. (Ce port est également utilisé pour le tunnelling quand des connexions par tunnel sont utilisées.)
Horizon Client	*	View Agent/Horizon Agent	22443	TCP	HTML Access et VMware Blast si Blast Secure Gateway n'est pas utilisé.
Horizon Client	*	Horizon Agent	22443	UDP	VMware Blast si Blast Secure Gateway n'est pas utilisé. Note Non utilisé lors de la connexion à des postes de travail Linux.

Tableau 1-4. Ports TCP et UDP utilisés par Horizon Client (Suite)

Source	Port	Cible	Port	Protocole	Description
Horizon Agent	22443	Horizon Client	*	UDP	VMware Blast si Blast Secure Gateway n'est pas utilisé. Note Non utilisé lors de la connexion à des postes de travail Linux.
Horizon Client	*	View Agent/Horizon Agent	3389	TCP	Trafic Microsoft RDP vers des postes de travail distants si des connexions directes sont utilisées à la place de connexions par tunnel.
Horizon Client	*	View Agent/Horizon Agent	9427	TCP	Redirection multimédia (MMR) Windows Media et redirection de lecteur client, si des connexions directes sont utilisées à la place de connexions par tunnel. Note Non requis pour CDR quand VMware Blast est utilisé.
Horizon Client	*	View Agent/Horizon Agent	32111	TCP	Redirection USB et synchronisation de fuseau horaire si des connexions directes sont utilisées à la place de connexions par tunnel.
Horizon Client	*	View Agent/Horizon Agent	4172	TCP et UDP	PCoIP, si PCoIP Secure Gateway n'est pas utilisé. Note Comme le port source varie, voir la note sous ce tableau.
Horizon Client	*	Serveur de connexion, serveur de sécurité ou dispositif Unified Access Gateway	4172	TCP et UDP	PCoIP (pas SALSA20) si PCoIP Secure Gateway est utilisé. Note Comme le port source varie, voir la note sous ce tableau.
View Agent/Horizon Agent	4172	Horizon Client	*	UDP	PCoIP, si PCoIP Secure Gateway n'est pas utilisé. Note Comme le port cible varie, voir la note sous ce tableau.
Serveur de sécurité, Serveur de connexion View ou dispositif Unified Access Gateway	4172	Horizon Client	*	UDP	PCoIP (pas SALSA20) si PCoIP Secure Gateway est utilisé. Note Comme le port cible varie, voir la note sous ce tableau.
Horizon Client	*	Serveur de connexion, serveur de sécurité ou dispositif Unified Access Gateway	8443	TCP	HTML Access et VMware Blast si Blast Secure Gateway est utilisé.

Tableau 1-4. Ports TCP et UDP utilisés par Horizon Client (Suite)

Source	Port	Cible	Port	Protocole	Description
Horizon Client	*	Serveur de connexion, serveur de sécurité ou dispositif Unified Access Gateway	8443	UDP	VMware Blast si Blast Secure Gateway est utilisé. Note Non utilisé lors de la connexion à un poste de travail Linux.
Serveur de connexion View, serveur de sécurité ou dispositif Unified Access Gateway	8443	Horizon Client	*	UDP	VMware Blast si Blast Secure Gateway est utilisé. Note Non utilisé lors de la connexion à un poste de travail Linux.

Note Le numéro de port UDP que les clients utilisent pour PCoIP et VMware Blast peut changer. Si le port 50002 est utilisé, le client choisit 50003. Si le port 50003 est utilisé, le client choisit le port 50004, etc. Vous devez configurer les pare-feu avec TOUS où un astérisque (*) est répertorié dans le tableau.

Services, démons et processus installés

2

Lorsque vous exécutez le client ou le programme d'installation de l'agent, plusieurs composants sont installés.

Ce chapitre contient les rubriques suivantes :

- [Services installés par le programme d'installation de View Agent ou Horizon Agent sur des machines Windows](#)
- [Services installés sur le client Windows](#)
- [Démons installés dans d'autres clients et le poste de travail Linux](#)

Services installés par le programme d'installation de View Agent ou Horizon Agent sur des machines Windows

Le fonctionnement des applications et des postes de travail distants dépend de plusieurs services Windows.

Tableau 2-1. Services de View Agent (pour Horizon 6) ou Horizon Agent (pour Horizon 7)

Nom du service	Type de démarrage	Description
VMware Blast	Automatique	Fournit des services pour HTML Access et pour utiliser le protocole VMware Blast Extreme afin de se connecter à des clients natifs.
VMware Horizon View Agent	Automatique	Fournit des services pour View Agent/Horizon Agent.
Serveur de l'agent invité VMware Horizon View Composer	Automatique	Fournit des services si cette machine virtuelle fait partie d'un pool de postes de travail de clone lié View Composer.
VMware Horizon View Persona Management	Automatique si la fonctionnalité est activée ; sinon, Désactivé	Fournit des services pour la fonctionnalité VMware Persona Management.
Hôte de script VMware Horizon View	Désactivé	Fournit la prise en charge de l'exécution des scripts de session de démarrage, le cas échéant, pour configurer des stratégies de sécurité de poste de travail avant qu'une session de poste de travail commence. Les stratégies sont basées sur le périphérique client et sur l'emplacement de l'utilisateur.

Tableau 2-1. Services de View Agent (pour Horizon 6) ou Horizon Agent (pour Horizon 7) (Suite)

Nom du service	Type de démarrage	Description
VMware Netlink Supervisor Service	Automatique	Pour prendre en charge les fonctions de redirection de scanner et de port série, fournit des services de surveillance pour le transfert d'informations entre les processus de noyau et d'espace utilisateur.
VMware Scanner Redirection Client Service	Automatique	(View Agent 6.0.2 et versions ultérieures) Fournit des services pour la fonction de redirection de scanner.
VMware Serial Com Client Service	Automatique	(View Agent 6.1.1 et versions ultérieures) Fournit des services pour la fonction de redirection de port série.
VMware Snapshot Provider	Manuel	Fournit des services pour les snapshots de machine virtuelle, qui sont utilisés pour le clonage.
VMware Tools	Automatique	Fournit la prise en charge de la synchronisation des objets entre les systèmes d'exploitation hôte et invité, ce qui améliore la performance du système d'exploitation invité des machines virtuelles et la gestion de la machine virtuelle.
VMware USB Arbitration Service	Automatique	Compte les divers périphériques USB connectés au client et détermine les périphériques à connecter au client et ceux à connecter au poste de travail distant.
VMware View USB	Automatique	Fournit des services pour la fonction de redirection USB.

Services installés sur le client Windows

Le fonctionnement d'Horizon Client dépend de plusieurs services Windows.

Tableau 2-2. Services d'Horizon Client

Nom du service	Type de démarrage	Description
VMware Horizon Client	Automatique	Fournit des services Horizon Client.
VMware Netlink Supervisor Service	Automatique	Pour prendre en charge les fonctions de redirection de scanner et de port série, fournit des services de surveillance pour le transfert d'informations entre les processus de noyau et d'espace utilisateur.
VMware Scanner Redirection Client Service	Automatique	(Horizon Client 3.2 et versions ultérieures) Fournit des services pour la fonctionnalité de redirection de scanner.
VMware Serial Com Client Service	Automatique	(Horizon Client 3.4 et versions ultérieures) Fournit des services pour la fonctionnalité de redirection de port série.
VMware USB Arbitration Service	Automatique	Compte les divers périphériques USB connectés au client et détermine les périphériques à connecter au client et ceux à connecter au poste de travail distant.
VMware View USB	Automatique	(Horizon Client 4.3 et versions antérieures) Fournit des services pour la fonctionnalité de redirection USB.
		Note Dans Horizon Client 4.4 et versions ultérieures, ce service est supprimé et le service USBD est déplacé dans le processus <code>vmware-remotemks.exe</code> .

Démons installés dans d'autres clients et le poste de travail Linux

Pour des raisons de sécurité, il est important de savoir si des démons ou des processus sont installés par Horizon Client.

Tableau 2-3. Services, processus ou démons installés par Horizon Client , par type de client

Type	Service, processus ou démon
Client Linux	<ul style="list-style-type: none"> ■ <code>vmware-usbarbitrator</code>, qui compte les divers périphériques USB connectés au client et détermine les périphériques à connecter au client et ceux à connecter au poste de travail distant. ■ <code>vmware-view-used</code>, qui fournit des services pour la fonctionnalité de redirection USB. <p>Note Ces démons démarrent automatiquement si vous cochez la case Enregistrer et démarrer le ou les services après l'installation lors de l'installation. Ces processus s'exécutent en tant que root.</p>
Client Mac	Horizon Client ne crée aucun démon.
Client Chrome OS	Horizon Client s'exécute dans un processus Android. Horizon Client ne crée aucun démon.
Client iOS	Horizon Client ne crée aucun démon.
Client Android	Horizon Client s'exécute dans un processus Android. Horizon Client ne crée aucun démon.
Client Windows 10 UWP	Horizon Client ne crée ou ne déclenche aucun service système.
Client Windows Store	Horizon Client ne crée ou ne déclenche aucun service système.
Poste de travail Linux	<ul style="list-style-type: none"> ■ <code>StandaloneAgent</code>, qui s'exécute avec des privilèges root et est démarré lorsque le système Linux est activé et exécuté. <code>StandaloneAgent</code> communique avec le Serveur de connexion pour réaliser la gestion de session de poste de travail distant (configure/détruit la session, en mettant à jour l'état du poste de travail distant sur le broker dans le Serveur de connexion). ■ <code>VMwareBlastServer</code>, qui est démarré par <code>StandaloneAgent</code> lorsqu'une demande <code>StartSession</code> est reçue de la part du Serveur de connexion. Le démon <code>VMwareBlastServer</code> s'exécute avec le privilège <code>vmwblast</code> (un compte système créé lors de l'installation de l'agent Linux.) . Il communique avec <code>StandaloneAgent</code> via un canal <code>MKSControl</code> interne et communique avec Horizon Client en utilisant le protocole d'affichage VMware Blast.

Ressources à sécuriser

Ces ressources incluent des fichiers de configuration, des mots de passe et des contrôles d'accès pertinents.

Ce chapitre contient les rubriques suivantes :

- [Implémentation de meilleures pratiques pour sécuriser des systèmes client](#)
- [Emplacements des fichiers de configuration](#)
- [Comptes](#)

Implémentation de meilleures pratiques pour sécuriser des systèmes client

Implémentez les meilleures pratiques pour sécuriser des systèmes client.

- Assurez-vous que les systèmes client sont configurés pour passer en veille après une période d'inactivité et que les utilisateurs doivent saisir un mot de passe avant de réveiller l'ordinateur.
- Les utilisateurs doivent saisir un nom d'utilisateur et un mot de passe lors du démarrage des systèmes client. Ne configurez pas les systèmes client pour qu'ils autorisent les ouvertures de session automatiques.
- Pour les systèmes client Mac, pensez à définir différents mots de passe pour la chaîne de clé et le compte d'utilisateur. Lorsque les mots de passe sont différents, les utilisateurs sont invités avant que le système n'entre des mots de passe en leur nom. Pensez également à activer la protection FileVault.

Emplacements des fichiers de configuration

Les ressources à protéger incluent les fichiers de configuration relatifs à la sécurité.

Tableau 3-1. Emplacement des fichiers de configuration, par type de client

Type	Chemin du répertoire
Client Linux	<p>Lorsque Horizon Client démarre, des paramètres de configuration sont traités depuis divers emplacements dans l'ordre suivant :</p> <ol style="list-style-type: none"> 1 /etc/vmware/view-default-config 2 ~/.vmware/view-preferences 3 /etc/vmware/view-mandatory-config <p>Si un paramètre est défini dans plusieurs emplacements, la valeur utilisée est la valeur du dernier fichier ou de la dernière option de ligne de commande lu(e).</p>
Client Windows	<p>Les paramètres d'utilisateur pouvant inclure des informations privées se trouvent dans le fichier suivant :</p> <p>C:\Users\user-name\AppData\Roaming\VMware\VMware Horizon View Client\prefs.txt</p>
Client Mac	<p>Certains fichiers de configuration générés après le démarrage du client Mac.</p> <ul style="list-style-type: none"> ■ \$HOME/Library/Preferences/com.vmware.horizon.plist ■ \$HOME/Library/Preferences/com.vmware.vmr.plist ■ \$HOME/Library/Preferences/com.vmware.horizon.keyboard.plist ■ /Library/Preferences/com.vmware.horizon.plist
Client Chrome OS	<p>Les paramètres relatifs à la sécurité apparaissent dans l'interface utilisateur plutôt que dans les fichiers de configuration. Les utilisateurs ne peuvent pas voir les fichiers de configuration.</p>
Client iOS	<p>Les paramètres relatifs à la sécurité apparaissent dans l'interface utilisateur plutôt que dans les fichiers de configuration. Les utilisateurs ne peuvent pas voir les fichiers de configuration.</p>
Client Android	<p>Les paramètres relatifs à la sécurité apparaissent dans l'interface utilisateur plutôt que dans les fichiers de configuration. Les utilisateurs ne peuvent pas voir les fichiers de configuration.</p>
Client Windows 10 UWP	<p>Les paramètres relatifs à la sécurité apparaissent dans l'interface utilisateur plutôt que dans les fichiers de configuration. Les utilisateurs ne peuvent pas voir les fichiers de configuration.</p>
Client Windows Store	<p>Les paramètres relatifs à la sécurité apparaissent dans l'interface utilisateur plutôt que dans les fichiers de configuration. Les utilisateurs ne peuvent pas voir les fichiers de configuration.</p>
View Agent ou Horizon Agent (poste de travail distant avec système d'exploitation Windows)	<p>Les paramètres relatifs à la sécurité apparaissent uniquement dans le registre Windows.</p>
Poste de travail Linux	<p>Vous pouvez utiliser un éditeur de texte pour ouvrir le fichier de configuration suivant et pour spécifier les paramètres SSL.</p> <p>/etc/vmware/viewagent-custom.conf</p>

Comptes

Les utilisateurs clients doivent disposer d'un compte dans Active Directory.

Comptes d'utilisateur Horizon Client

Configurez des comptes d'utilisateurs dans Active Directory pour les utilisateurs qui ont accès à des applications et à des postes de travail distants. Les comptes d'utilisateur doivent être des membres du groupe Utilisateurs du Bureau à distance si vous prévoyez d'utiliser le protocole RDP.

Normalement, les utilisateurs finaux ne doivent pas être des administrateurs Horizon. Si un administrateur Horizon doit vérifier l'expérience utilisateur, créez et autorisez un compte test séparé. Sur le poste de travail, les utilisateurs finaux Horizon ne doivent pas être des membres de groupes privilégiés, tels que des administrateurs, car ils pourraient alors modifier des fichiers de configuration verrouillés et le registre Windows.

Comptes système créés au cours de l'installation

Aucun compte d'utilisateur de service n'est créé sur un type de client par l'application Horizon Client. Pour les services créés par Horizon Client pour Windows, l'ID de connexion est Système local.

Sur le client Mac, lors du premier démarrage, l'utilisateur doit accorder un accès Administrateur local pour démarrer les services USB et d'impression virtuelle (ThinPrint). Une fois ces services démarrés pour la première fois, l'utilisateur standard dispose d'un accès d'exécution pour eux. De la même façon, sur le client Linux, les démons `vmware-usbarbitrator` et `vmware-view-used` démarrent automatiquement si vous cochez la case **Enregistrer et démarrer le ou les services après l'installation** pendant l'installation. Ces processus s'exécutent en tant que root.

Aucun compte d'utilisateur de service n'est créé par View Agent ou Horizon Agent sur les postes de travail Windows. Sur les postes de travail Linux, un compte système, `vmwblast`, est créé. Sur les postes de travail Linux, le démon `StandaloneAgent` s'exécute avec des privilèges root et le démon `VmwareBlastServer` s'exécute avec des privilèges `vmwblast`.

Paramètres de sécurité pour le client et l'agent

4

Plusieurs paramètres de client et d'agent sont disponibles pour ajuster la sécurité de la configuration. Vous pouvez accéder aux paramètres pour le poste de travail distant et les clients Windows en utilisant des objets de stratégie de groupe ou en modifiant les paramètres de registre Windows.

Pour les paramètres de configuration liés à la collecte des journaux, reportez-vous à la section [Chapitre 6 Emplacements des fichiers journaux du client et de l'agent](#). Pour les paramètres de configuration liés aux protocoles de sécurité et aux suites de chiffrement, reportez-vous à la section [Chapitre 5 Configuration des protocoles de sécurité et des suites de chiffrement](#).

Ce chapitre contient les rubriques suivantes :

- [Configuration de la vérification des certificats](#)
- [Paramètres liés à la sécurité dans les modèles de configuration de View Agent et Horizon Agent](#)
- [Définir des options dans des fichiers de configuration sur un poste de travail Linux](#)
- [Paramètres de stratégie de groupe pour HTML Access](#)
- [Paramètres de sécurité des modèles de configuration d'Horizon Client](#)
- [Configuration du mode de vérification de certificat d'Horizon Client](#)
- [Configuration de la protection LSA](#)

Configuration de la vérification des certificats

Les administrateurs peuvent configurer le mode de vérification des certificats afin que, par exemple, une vérification complète soit toujours effectuée. Les administrateurs peuvent également configurer si les utilisateurs finaux sont autorisés à choisir si les connexions clientes sont rejetées quand une ou plusieurs vérifications des certificats de serveur échouent.

La vérification des certificats se produit pour les connexions SSL/TLS entre des instances du Serveur de connexion et Horizon Client. Les administrateurs peuvent configurer le mode de vérification pour utiliser l'une des stratégies suivantes :

- Les utilisateurs finaux sont autorisés à choisir le mode de vérification. Le reste de cette liste décrit les trois modes de vérification.
- (Pas de vérification) Aucune vérification de certificat n'est effectuée.

- (Avertir) Les utilisateurs sont avertis si un certificat auto-signé est présenté par le serveur. Les utilisateurs peuvent choisir d'autoriser ou pas ce type de connexion.
- (Sécurité complète) Une vérification complète est effectuée et les connexions qui ne passent pas de vérification complète sont rejetées.

La vérification de certificat inclut les vérifications suivantes :

- Le certificat a-t-il été révoqué ?
- Le certificat a-t-il un autre but que de vérifier l'identité de l'expéditeur et de chiffrer les communications du serveur ? Autrement dit, s'agit-il du bon type de certificat ?
- Le certificat a-t-il expiré, ou est-il valide uniquement dans le futur ? Autrement dit, le certificat est-il valide en fonction de l'horloge de l'ordinateur ?
- Le nom commun sur le certificat correspond-il au nom d'hôte du serveur qui l'envoie ? Une incompatibilité peut se produire si l'équilibrage de charge redirige Horizon Client vers un serveur disposant d'un certificat qui ne correspond pas au nom d'hôte entré dans Horizon Client. Une incompatibilité peut également se produire si vous entrez une adresse IP plutôt qu'un nom d'hôte dans le client.
- Le certificat est-il signé par une autorité de certification inconnue ou non approuvée ? Les certificats auto-signés sont un type d'autorité de certification non approuvée.

Pour que cette vérification aboutisse, la chaîne d'approbation du certificat doit être associée à une racine dans le magasin de certificats local.

Pour plus d'informations sur la configuration de la vérification des certificats sur un type de client spécifique, consultez le document Horizon Client pour le type de client spécifique. Ces documents contiennent également des informations sur l'utilisation des certificats auto-signés.

Paramètres liés à la sécurité dans les modèles de configuration de View Agent et Horizon Agent

Des paramètres liés à la sécurité sont fournis dans les fichiers de modèle d'administration ADM et ADMX pour View Agent et Horizon Agent. Les fichiers de modèle d'administration ADM et ADMX sont nommés `vdm_agent.adm` et `vdm_agent.admx`. Sauf indication contraire, les paramètres comprennent uniquement un paramètre Configuration ordinateur.

Les paramètres de sécurité sont stockés dans le registre sur la machine invitée sous `HKLM\Software\VMware, Inc.\VMware VDM\Agent\Configuration`.

Tableau 4-1. Paramètres liés à la sécurité dans le modèle de configuration de View Agent (pour Horizon 6) ou Horizon Agent (pour Horizon 7)

Paramètre	Description
AllowDirectRDP	<p>Détermine si les clients qui ne sont pas des périphériques Horizon Client peuvent se connecter directement à des postes de travail distants avec RDP. Lorsque ce paramètre est désactivé, l'agent autorise uniquement les connexions gérées par Horizon via Horizon Client.</p> <p>Lorsque vous vous connectez à un poste de travail distant à partir d'Horizon Client pour Mac, ne désactivez pas le paramètre AllowDirectRDP. Si ce paramètre est désactivé, la connexion échoue avec une erreur Access is denied (Accès refusé).</p> <p>Par défaut, lorsqu'un utilisateur a ouvert une session de poste de travail distant, vous pouvez utiliser RDP pour vous connecter à la machine virtuelle. La connexion RDP met fin à la session de poste de travail distant et les données et paramètres non enregistrés de l'utilisateur risquent d'être perdus. L'utilisateur ne peut pas se connecter au poste de travail tant que la connexion RDP externe est fermée. Pour éviter cette situation, désactivez le paramètre AllowDirectRDP.</p> <hr/> <p>Important Les services Bureau à distance doivent s'exécuter sur le système d'exploitation invité de chaque poste de travail. Vous pouvez utiliser ce paramètre pour empêcher les utilisateurs de faire des connexions RDP directes sur leurs postes de travail.</p> <hr/> <p>Ce paramètre est activé par défaut. La valeur de Registre Windows équivalente est AllowDirectRDP.</p>
AllowSingleSignon	<p>Détermine si l'authentification unique (Single Sign-On, SSO) est utilisée pour connecter les utilisateurs aux postes de travail et aux applications. Lorsque ce paramètre est activé, les utilisateurs doivent entrer leurs informations d'identification une seule fois, lorsqu'ils se connectent au serveur. Lorsqu'il est désactivé, les utilisateurs doivent s'authentifier de nouveau lorsque la connexion à distance est effectuée.</p> <p>Ce paramètre est activé par défaut. La valeur de Registre Windows équivalente est AllowSingleSignon.</p>
CommandsToRunOnConnect	<p>Spécifie une liste de commandes ou de scripts de commande à exécuter lorsqu'une session est connectée pour la première fois.</p> <p>Aucune liste n'est spécifiée par défaut. La valeur de Registre Windows équivalente est CommandsToRunOnConnect.</p>
CommandsToRunOnDisconnect	<p>Spécifie la liste des commandes ou des scripts de commande à exécuter lorsqu'une session est déconnectée.</p> <p>Aucune liste n'est spécifiée par défaut. La valeur de Registre Windows équivalente est CommandsToRunOnReconnect.</p>
CommandsToRunOnReconnect	<p>Spécifie une liste de commandes ou de scripts de commande à exécuter lorsqu'une session est reconnectée après une déconnexion.</p> <p>Aucune liste n'est spécifiée par défaut. La valeur de Registre Windows équivalente est CommandsToRunOnDisconnect.</p>

Tableau 4-1. Paramètres liés à la sécurité dans le modèle de configuration de View Agent (pour Horizon 6) ou Horizon Agent (pour Horizon 7) (Suite)

Paramètre	Description
ConnectionTicketTimeout	<p>Spécifie la durée en secondes pendant laquelle le ticket de connexion Horizon est valide.</p> <p>Les périphériques Horizon Client utilisent un ticket de connexion pour la vérification et l'authentification unique lorsqu'ils se connectent à l'agent. Pour des raisons de sécurité, un ticket de connexion est valide pendant une durée limitée. Lorsqu'un utilisateur se connecte à un poste de travail distant, l'authentification doit avoir lieu pendant le délai d'expiration du ticket de connexion sinon la session expire. Si ce paramètre n'est pas configuré, le délai d'expiration par défaut est de 900 secondes.</p> <p>La valeur de Registre Windows équivalente est <code>VdmConnectionTicketTimeout</code>.</p>
CredentialFilterExceptions	<p>Spécifie les fichiers exécutables qui ne sont pas autorisés à charger l'agent <code>CredentialFilter</code>. Les noms de fichier ne doivent pas contenir de chemin d'accès ou de suffixe. Utilisez un point-virgule pour séparer plusieurs noms de fichier.</p> <p>Aucune liste n'est spécifiée par défaut.</p> <p>La valeur de Registre Windows équivalente est <code>CredentialFilterExceptions</code>.</p>

Pour plus d'informations sur ces paramètres et leurs implications en termes de sécurité, reportez-vous au document *Administration de View*.

Définir des options dans des fichiers de configuration sur un poste de travail Linux

Vous pouvez configurer certaines options en ajoutant des entrées aux fichiers `/etc/vmware/config` ou `/etc/vmware/viewagent-custom.conf`.

Lors de l'installation d'Horizon Agent, le programme d'installation copie deux fichiers de modèle de configuration, `config.template` et `viewagent-custom.conf.template`, dans `/etc/vmware`. De plus, si les fichiers `/etc/vmware/config` et `/etc/vmware/viewagent-custom.conf` n'existent pas, le programme d'installation copie `config.template` dans `config` et `viewagent-custom.conf.template` dans `viewagent-custom.conf`. Dans les fichiers de modèle, toutes les options de configuration sont répertoriées et documentées. Pour définir une option, supprimez simplement le commentaire et modifiez la valeur si nécessaire.

Par exemple, la ligne suivante dans `/etc/vmware/config` configure le build sur le mode PNG sans perte.

```
RemoteDisplay.buildToPNG=TRUE
```

Après avoir modifié la configuration, redémarrez Linux pour que les modifications prennent effet.

Options de configuration dans `/etc/vmware/config`

VMwareBlastServer et ses plug-ins liés utilisent le fichier de configuration `/etc/vmware/config`.

Note Le tableau suivant décrit chaque paramètre de stratégie appliqué par agent pour USB dans le fichier de configuration d'Horizon Agent. Horizon Agent utilise les paramètres pour décider si un périphérique USB peut être transmis à la machine hôte. Horizon Agent transmet également les paramètres à Horizon Client pour qu'il les interprète et les applique. L'application est effectuée selon que vous spécifiez le modificateur de fusion (**m**) pour appliquer les paramètres de stratégie de filtre Horizon Agent et Horizon Client ou le modificateur de remplacement (**o**) pour utiliser le paramètre de stratégie de filtre Horizon Agent au lieu du paramètre de stratégie de filtre Horizon Client.

Tableau 4-2. Options de configuration dans `/etc/vmware/config`

Option	Valeur/Format	Valeur par défaut	Description
Clipboard.Direction	0, 1, 2, ou 3	2	Utilisez cette option pour spécifier la stratégie de redirection du Presse-papiers. Les valeurs valides sont les suivantes : <ul style="list-style-type: none"> 0 - Désactivez la redirection de Presse-papiers. 1 - Activez la redirection de Presse-papiers dans les deux sens. 2 - Activez la redirection de Presse-papiers uniquement depuis le client vers le poste de travail distant. 3 - Activez la redirection de Presse-papiers uniquement depuis le poste de travail vers le client.
RemoteDisplay.allowAudio	true ou false	true	Définissez cette option pour activer/désactiver la sortie audio.
RemoteDisplay.allowH264	true ou false	true	Définissez cette option pour activer ou désactiver le codage H.264.
RemoteDisplay.buildToPNG	true ou false	false	Les applications graphiques, en particulier les applications de conception graphique, requièrent un rendu exact des pixels d'images dans l'affichage client d'un poste de travail Linux. Vous pouvez configurer le build sur le mode PNG sans perte pour la lecture des images et des vidéos qui sont générées sur un poste de travail et rendues sur le périphérique client. Cette fonctionnalité utilise de la bande passante supplémentaire entre le client et l'hôte ESXi. L'activation de cette option désactive le codage H.264.
RemoteDisplay.enableNetworkContinuity	true ou false	true	Définissez cette option pour activer ou désactiver la fonctionnalité Network Continuity dans Horizon Agent for Linux.

Tableau 4-2. Options de configuration dans /etc/vmware/config (Suite)

Option	Valeur/Format	Valeur par défaut	Description
RemoteDisplay.enableNetworkIntelligence	true ou false	true	Définissez cette option pour activer ou désactiver la fonctionnalité Network Intelligence dans Horizon Agent for Linux.
RemoteDisplay.enableStats	true ou false	false	Active ou désactive les statistiques du protocole d'affichage VMware Blast dans le journal mks, telles que la bande passante, FPS, RTT, etc.
RemoteDisplay.enableUDP	true ou false	true	Définissez cette option pour activer ou désactiver la prise en charge du protocole UDP dans Horizon Agent for Linux.
RemoteDisplay.maxBandwidthKbps	Un entier	4096000	Spécifie la bande passante maximale, en kilobits par seconde (Kbit/s), pour une session VMware Blast. La bande passante inclut la création d'images, le son, le canal virtuel et le trafic de contrôle VMware Blast. La valeur maximale est de 4 Gbit/s (4096000).
RemoteDisplay.maxFPS	Un entier	60	Spécifie le nombre maximal d'actualisations d'écran. Utilisez ce paramètre pour gérer la bande passante moyenne que les utilisateurs consomment. La valeur valide doit être comprise entre 3 et 60. La valeur par défaut est de 60 actualisations par seconde.
RemoteDisplay.maxQualityJPEG	Plage de valeurs disponible : 1 à 100	90	Spécifie la qualité d'image de l'écran de poste de travail pour le codage JPEG/PNG. Les paramètres de qualité élevée sont destinés aux zones de l'écran qui sont plus statiques, ce qui se traduit par une meilleure qualité d'image.
RemoteDisplay.midQualityJPEG	Plage de valeurs disponible : 1 à 100	35	Spécifie la qualité d'image de l'écran de poste de travail pour le codage JPEG/PNG. Utilisez cette option pour définir les paramètres de qualité moyenne de l'écran de poste de travail.
RemoteDisplay.minQualityJPEG	Plage de valeurs disponible : 1 à 100	25	Spécifie la qualité d'image de l'écran de poste de travail pour le codage JPEG/PNG. Les paramètres de qualité faible sont destinés aux zones de l'écran qui changent souvent, par exemple, lors du défilement.
RemoteDisplay.qpmaxH264	Plage de valeurs disponible : 0 à 51	36	Utilisez cette option pour définir le paramètre de quantification H264minQP, qui spécifie la meilleure qualité d'image pour l'écran distant configuré pour utiliser le codage H.264. Définissez une valeur supérieure à celle définie pour RemoteDisplay.qpminH264.
RemoteDisplay.qpminH264	Plage de valeurs disponible : 0 à 51	10	Utilisez cette option pour définir le paramètre de quantification H264maxQP, qui spécifie la plus faible qualité d'image pour l'écran distant configuré pour utiliser le codage H.264. Définissez une valeur inférieure à celle définie pour RemoteDisplay.qpmaxH264.

Tableau 4-2. Options de configuration dans /etc/vmware/config (Suite)

Option	Valeur/Format	Valeur par défaut	Description
UsbRedirPlugin.log.logLevel	error, warn, info, debug, trace ou verbose	info	Utilisez cette option pour définir le niveau de journalisation du plug-in de redirection USB.
UsbRedirServer.log.logLevel	error, warn, info, debug, trace ou verbose	info	Utilisez cette option pour définir le niveau de journalisation du serveur de redirection USB.
VMWPkcs11Plugin.log.enable	true ou false	false	Définissez cette option afin d'activer ou de désactiver le mode de journalisation pour la fonctionnalité d'authentification unique réelle.
VMWPkcs11Plugin.log.logLevel	error, warn, info, debug, trace ou verbose	info	Utilisez cette option afin de définir le niveau de journalisation pour la fonctionnalité d'authentification unique réelle.
VVC.RTAV.Enable	true ou false	true	Définissez cette option pour activer/désactiver l'entrée audio.
VVC.ScRedir.Enable	true ou false	true	Définissez cette option pour activer/désactiver la redirection de carte à puce.
VVC.logLevel	fatal error, warn, info, debug ou trace	info	Utilisez cette option pour définir le niveau de journalisation du nœud de proxy VVC.
cdrserver.cacheEnable	true ou false	true	Définissez cette option pour activer ou désactiver la fonctionnalité de cache en écriture de l'agent vers le client.
cdrserver.forcedByAdmin	true ou false	false	Définissez cette option pour contrôler si le client peut partager des dossiers supplémentaires qui ne sont pas spécifiés avec l'option <code>cdrserver.shareFolders</code> .
cdrserver.logLevel	error, warn, info, debug, trace ou verbose	info	Utilisez cette option pour définir le niveau de journalisation pour le fichier <code>vmware-CDRserver.log</code> .

Tableau 4-2. Options de configuration dans /etc/vmware/config (Suite)

Option	Valeur/Format	Valeur par défaut	Description
cdrserver.permissions	R	RW	<p>Utilisez cette option pour appliquer des autorisations en lecture/écriture supplémentaires dont dispose Horizon Agent sur les dossiers partagés par Horizon Client. Par exemple :</p> <ul style="list-style-type: none"> ■ Si le dossier partagé par Horizon Client dispose des autorisations <code>read</code> et <code>write</code> et que vous définissez <code>cdrserver.permissions=R</code>, Horizon Agent ne dispose que d'autorisations d'accès <code>read</code>. ■ Si le dossier partagé par Horizon Client ne dispose que d'autorisations <code>read</code> et que vous définissez <code>cdrserver.permissions=RW</code>, Horizon Agent ne dispose toujours que de droits d'accès <code>read</code>. Horizon Agent ne peut pas modifier l'attribut <code>read</code> seul qui a été défini par Horizon Client. Horizon Agent ne peut supprimer que les droits d'accès en écriture. <p>Voici les utilisations classiques :</p> <ul style="list-style-type: none"> ■ <code>cdrserver.permissions=R</code> ■ <code>#cdrserver.permissions=R</code> (par exemple, commenter ou supprimer l'entrée)
cdrserver.sharedFolders	<code>file_path1,R;file_path2,;file_path3,R; . . .</code>	non défini	<p>Spécifiez un ou plusieurs chemins de fichier vers les dossiers que le client peut partager avec le poste de travail Linux. Par exemple :</p> <ul style="list-style-type: none"> ■ Pour un client Windows : <code>C:\spreadsheets,;D:\ebooks,R</code> ■ Pour un client non-Windows : <code>/tmp/spreadsheets;/tmp/ebooks,;/home/finance,R</code>
collaboration.logLevel	<code>error, info ou debug</code>	<code>info</code>	<p>Utilisez cette option pour définir le niveau de journalisation utilisé pour la session de collaboration. Si le niveau de journalisation est <code>debug</code>, tous les appels effectués aux fonctions <code>collabui</code> et le contenu de la liste <code>collabor</code> sont journalisés.</p>
collaboration.maxCollabors	Un entier inférieur à 10	5	Spécifie le nombre maximal de collaborateurs que vous pouvez inviter à rejoindre une session.
collaboration.enableEmail	<code>true</code> ou <code>false</code>	<code>true</code>	Définissez cette option pour activer ou désactiver l'envoi d'invitations de collaboration à l'aide d'une application de messagerie installée. Lorsqu'elle est désactivée, vous ne pouvez pas utiliser un e-mail pour inviter des collaborateurs, même si une application de messagerie est installée.
collaboration.serverUrl	[URL]	non défini	Spécifie les URL de serveur à inclure dans les invitations de collaboration.

Tableau 4-2. Options de configuration dans /etc/vmware/config (Suite)

Option	Valeur/Format	Valeur par défaut	Description
collaboration.enableControlPassing	true ou false	true	Définissez cette option pour autoriser ou empêcher les collaborateurs d'avoir le contrôle du poste de travail Linux. Pour spécifier une session de collaboration en lecture seule, définissez cette option sur false .
mksVNCServer.useUInputButtonMapping	true ou false	false	Définissez cette option pour activer la prise en charge d'une souris pour gauchers sous Ubuntu ou RHEL 7. CentOS et RHEL 6 prennent en charge les souris pour gauchers et vous n'avez pas besoin de définir cette option.
mksVNCServer.useXExtButtonMapping	true ou false	false	Définissez cette option pour activer ou désactiver la prise en charge d'une souris pour gauchers sous SLED 11 SP3.
mksvhan.clipboardSize	Un entier	1024	Utilisez cette option pour spécifier la taille maximale du Presse-papiers pour copier et coller.
vdpService.log.logLevel	fatal error, warn, info, debug ou trace	info	Utilisez cette option pour définir le niveau de journalisation de vdpService.
viewusb.AllowAudioIn	{m o}: {true false}	non défini, ce qui équivaut à true	Utilisez cette option pour autoriser ou interdire les périphériques d'entrée audio à rediriger. Exemple : o:false
viewusb.AllowAudioOut	{m o}: {true false}	non défini, ce qui équivaut à false	Définissez cette option pour autoriser ou interdire la redirection de périphériques de sortie audio.
viewusb.AllowAutoDeviceSplitting	{m o}: {true false}	non défini, ce qui équivaut à false	Définissez cette option pour autoriser ou interdire le fractionnement automatique de périphériques USB composites. Exemple : m:true
viewusb.AllowDevDescFailsafe	{m o}: {true false}	non défini, ce qui équivaut à false	Définissez cette option pour autoriser ou interdire les périphériques à rediriger même si Horizon Client ne parvient pas à obtenir les descripteurs de configuration ou de périphérique. Pour autoriser un périphérique même s'il ne parvient pas à obtenir les descripteurs de configuration ou de périphérique, incluez-le dans les filtres Inclure, tels que IncludeVidPid ou IncludePath .
viewusb.AllowHIDBootable	{m o}: {true false}	non défini, ce qui équivaut à true	Utilisez cette option pour autoriser ou interdire la redirection de périphériques d'entrée, autres que des claviers et des souris, qui sont disponibles lors du démarrage, également connus sous le nom de périphériques de démarrage HID.
viewusb.AllowKeyboardMouse	{m o}: {true false}	non défini, ce qui équivaut à false	Utilisez cette option pour autoriser ou interdire la redirection de claviers avec des périphériques de pointage intégrés (souris, trackball ou pavé tactile).

Tableau 4-2. Options de configuration dans /etc/vmware/config (Suite)

Option	Valeur/Format	Valeur par défaut	Description
viewusb.AllowSmartcard	{m o} : {true false}	non défini, ce qui équivaut à false	Définissez cette option pour autoriser ou interdire les périphériques de carte à puce à rediriger.
viewusb.AllowVideo	{m o} : {true false}	non défini, ce qui équivaut à true	Utilisez cette option pour autoriser ou interdire les périphériques vidéo à rediriger.
viewusb.DisableRemoteConfig	{m o} : {true false}	non défini, ce qui équivaut à false	Définissez cette option pour désactiver ou activer l'utilisation des paramètres d'Horizon Agent lors du filtrage des périphériques USB.
viewusb.ExcludeAllDevices	{true false}	non défini, ce qui équivaut à false	Utilisez cette option pour exclure ou inclure tous les périphériques USB de la redirection. Si ce paramètre est défini sur true , vous pouvez utiliser d'autres paramètres de règle pour autoriser la redirection de périphériques spécifiques ou de familles de périphériques. Si ce paramètre est défini sur false , vous pouvez utiliser d'autres paramètres de règle pour empêcher la redirection de périphériques spécifiques ou de familles de périphériques. Si vous définissez la valeur de ExcludeAllDevices sur true sur Horizon Agent, et si ce paramètre est transmis à Horizon Client, le paramètre d'Horizon Agent remplace celui d'Horizon Client.
viewusb.ExcludeFamily	{m o} : <i>family_name_1</i> ; <i>family_name_2</i> ; ...	non défini	Utilisez cette option pour exclure des familles de périphériques de la redirection. Par exemple : m:bluetooth;smart-card Si vous avez activé le fractionnement automatique de périphérique, Horizon examine la famille de périphériques de chaque interface d'un périphérique USB composite pour décider quelles interfaces doivent être exclues. Si vous avez désactivé le fractionnement automatique de périphérique, Horizon examine la famille de périphérique de l'ensemble du périphérique USB composite. Note Les souris et les claviers sont exclus de la redirection par défaut et il n'est pas nécessaire de les exclure avec ce paramètre.
viewusb.ExcludePath	{m o} : <i>bus-x1[/y1].../port-z1</i> ; <i>bus-x2[/y2].../port-z2</i> ; ...	non défini	Utilisez cette option pour exclure des périphériques dans des chemins de concentrateur ou de port spécifiés de la redirection. Vous devez spécifier des numéros de bus et de port au format hexadécimal. Vous ne pouvez pas utiliser le caractère générique dans les chemins. Par exemple : m:bus-1/2/3_port-02;bus-1/1/1/4_port-ff

Tableau 4-2. Options de configuration dans /etc/vmware/config (Suite)

Option	Valeur/Format	Valeur par défaut	Description
viewusb.ExcludeVidPid	{m o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]	non défini	Définissez cette option pour exclure des périphériques avec des ID de fournisseur et de produit spécifiés de la redirection. Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (*) à la place de chiffres dans un ID. Par exemple : o:vid-0781_pid-****;vid-0561_pid-554c
viewusb.IncludeFamily	{m o}:family_name_1[;family_name_2]...	non défini	Définissez cette option pour inclure des familles de périphériques pouvant être redirigées. Par exemple : o:storage; smart-card
viewusb.IncludePath	{m o}:bus-x1[/y1].../port-z1[;bus-x2[/y2].../port-z2;...]	non défini	Utilisez cette option pour inclure des périphériques dans des chemins de concentrateur ou de port spécifiés pour être redirigés. Vous devez spécifier des numéros de bus et de port au format hexadécimal. Vous ne pouvez pas utiliser le caractère générique dans les chemins. Par exemple : m:bus-1/2_port-02;bus-1/7/1/4_port-0f
viewusb.IncludeVidPid	{m o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]	non défini	Définissez cette option pour inclure des périphériques avec des ID de fournisseur et de produit spécifiés pouvant être redirigés. Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (*) à la place de chiffres dans un ID. Par exemple : o:vid-***_pid-0001;vid-0561_pid-554c

Tableau 4-2. Options de configuration dans /etc/vmware/config (Suite)

Option	Valeur/Format	Valeur par défaut	Description
viewusb.SplitExcludeVidPid	{m o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]	non défini	Utilisez cette option pour exclure ou inclure un périphérique USB composite spécifié du fractionnement par ID de fournisseur et par ID de produit. Le format du paramètre est vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...] . Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (*) à la place de chiffres dans un ID. Exemple : m:vid-0f0f_pid-55**
viewusb.SplitVidPid	{m o}: vid-xxxx_pid-yyyy([exintf:zz[;exintf:ww]])[;...]	non défini	Définissez cette option pour traiter les composants d'un périphérique USB composite spécifiés par des ID de fournisseur et de produit en tant que périphériques séparés. Le format du paramètre est vid-xxxx_pid-yyyy(exintf:zz[;exintf:ww]) . Vous pouvez utiliser le mot-clé exintf pour exclure des composants de la redirection en spécifiant leur numéro d'interface. Vous devez spécifier les numéros d'ID au format hexadécimal et les numéros d'interface au format décimal en incluant les zéros à gauche. Vous pouvez utiliser le caractère générique (*) à la place de chiffres dans un ID. Exemple : o:vid-0f0f_pid-***(exintf-01);vid-0781_pid-554c(exintf:01;exintf:02)

Note Horizon n'inclut pas automatiquement les composants que vous n'avez pas explicitement exclus. Vous devez spécifier une stratégie de filtre telle que **Inclure un périphérique VidPid** pour inclure ces composants.

Options de configuration dans /etc/vmware/viewagent-custom.conf

Java Standalone Agent utilise le fichier de configuration /etc/vmware/viewagent-custom.conf.

Tableau 4-3. Options de configuration dans /etc/vmware/viewagent-custom.conf

Option	Valeur	Valeur par défaut	Description
CDREnable	true ou false	true	Utilisez cette option pour activer ou désactiver la fonctionnalité de redirection du lecteur client.
CollaborationEnable	true ou false	true	Utilisez cette option pour activer ou désactiver la fonctionnalité de session de collaboration sur les postes de travail Linux.

Tableau 4-3. Options de configuration dans /etc/vmware/viewagent-custom.conf (Suite)

Option	Valeur	Valeur par défaut	Description
EndpointVPNEnable	true ou false	false	Définissez cette option pour spécifier si l'adresse IP de la carte de réseau physique du client ou l'adresse IP VPN doit être utilisée lors de l'évaluation de l'adresse IP du point de terminaison par rapport à la plage d'adresses IP du point de terminaison utilisée dans la Console User Environment Manager. Si l'option est définie sur false, l'adresse IP de carte de réseau physique du client est utilisée. Dans le cas contraire, l'adresse IP VPN est utilisée.
HelpDeskEnable	true ou false	true	Définissez cette option pour activer ou désactiver la fonctionnalité de l'outil Service d'assistance.
KeyboardLayoutSync	true ou false	true	Utilisez cette option pour spécifier s'il faut synchroniser ou non la liste de paramètres régionaux système et la disposition de clavier actuelle d'un client avec des postes de travail Horizon Agent pour Linux. Lorsque ce paramètre est activé ou qu'il n'est pas configuré, la synchronisation est autorisée. Lorsque ce paramètre est désactivé, la synchronisation n'est pas autorisée. Cette fonctionnalité est prise en charge uniquement pour Horizon Client pour Windows et dans les langues suivantes : anglais, français, allemand, japonais, coréen, espagnol, chinois simplifié et chinois traditionnel.
LogCnt	Un entier	-1	Utilisez cette option pour définir le nombre de fichiers journaux réservés dans /tmp/vmware-root. <ul style="list-style-type: none"> ■ -1 : tout conserver ■ 0 : tout supprimer ■ > 0 : nombre de journaux réservés.
NetbiosDomain	Une chaîne de texte en lettres majuscules		Lorsque vous configurez l'authentification unique réelle, utilisez cette option pour définir le nom NetBIOS du domaine de votre organisation.
OfflineJoinDomain	pbis ou samba	pbis	Utilisez cette option pour définir la jonction de domaine hors connexion Instant Clone. Les méthodes disponibles pour exécuter une jonction de domaine hors ligne sont l'authentification PBISO (PowerBroker Identity Services Open) et la jonction de domaine hors ligne Samba. Si cette propriété a une valeur autre que pbis ou samba, la jonction de domaine hors ligne est ignorée.

Tableau 4-3. Options de configuration dans /etc/vmware/viewagent-custom.conf (Suite)

Option	Valeur	Valeur par défaut	Description
RunOnceScript			<p>Utilisez cette option pour joindre la machine virtuelle clonée à Active Directory.</p> <p>Définissez l'option RunOnceScript après avoir modifié le nom d'hôte. Le script spécifié est exécuté une seule fois après le changement du premier nom d'hôte. Le script est exécuté avec l'autorisation racine lorsque le service de l'agent démarre et que le nom d'hôte a été modifié après l'installation de l'agent.</p> <p>Par exemple, pour la solution winbind, vous devez joindre la machine virtuelle de base à Active Directory avec winbind, puis définir cette option sur un chemin de script. Cela doit contenir la commande de jonction de domaine /usr/bin/net ads join -U <ADUserName> %<ADUserPassword>. Après le clone de machine virtuelle, la personnalisation du système d'exploitation modifie le nom d'hôte. Lorsque le service de l'agent démarre, le script est exécuté pour joindre la machine virtuelle clonée à Active Directory.</p>
RunOnceScriptTimeout		120	<p>Utilisez cette option pour définir le délai d'expiration en secondes de l'option RunOnceScript.</p> <p>Par exemple, définissez RunOnceScriptTimeout=120</p>
SSLCiphers	Une chaîne de texte	!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES	<p>Utilisez cette option pour spécifier la liste de chiffrements. Vous devez utiliser le format défini dans https://www.openssl.org/docs/manmaster/man1/ciphers.html.</p>
SSLProtocols	Une chaîne de texte	TLSv1_1:TLSv1_2	<p>Utilisez cette option pour spécifier les protocoles de sécurité. Les protocoles pris en charge sont TLSv1.0, TLSv1.1 et TLSv1.2.</p>

Tableau 4-3. Options de configuration dans /etc/vmware/viewagent-custom.conf (Suite)

Option	Valeur	Valeur par défaut	Description
SSODesktopType	UseGnomeClassic ou UseGnomeFlashback ou UseGnomeUbuntu ou UseMATE ou UseKdePlasma ou		<p>Cette option spécifie l'environnement de poste de travail à utiliser, au lieu de l'environnement de poste de travail par défaut, lorsque l'authentification unique est activée.</p> <p>Vous devez d'abord vérifier que l'environnement de poste de travail choisi est installé sur votre poste de travail avant de spécifier son utilisation. Lorsque cette option est définie sur un poste de travail Ubuntu 14.04/16.04/18.04, elle s'applique, que la fonctionnalité d'authentification unique soit activée ou non. Si cette option est spécifiée dans un poste de travail RHEL/CentOS 7.x, l'environnement de poste de travail choisi est utilisé uniquement si l'authentification unique est activée.</p> <p>Note Cette option n'est pas prise en charge sur les postes de travail RHEL/CentOS 6 et SLED 11. Reportez-vous au document <i>Configuration des postes de travail Horizon 7 for Linux</i> pour obtenir plus d'informations sur la configuration de KDE comme environnement de poste de travail par défaut lorsque l'authentification unique est activée sur ces postes de travail.</p>
SSOEnable	true ou false	true	Définissez cette option pour activer/désactiver l'authentification unique (SSO).
SSOUserFormat	Une chaîne de texte	[username]	<p>Utilisez cette option pour spécifier le format du nom de connexion pour l'authentification unique. La valeur par défaut est le nom d'utilisateur uniquement. Définissez cette option si le nom de domaine est également requis. En général, le nom de connexion est le nom de domaine plus un caractère spécial suivi du nom d'utilisateur. Si le caractère spécial est une barre oblique inverse, vous devez l'échapper avec une autre barre oblique inverse. Voici des exemples de formats de nom de connexion :</p> <ul style="list-style-type: none"> ■ SSOUserFormat=[domain]\\[username] ■ SSOUserFormat=[domain]+[username] ■ SSOUserFormat=[username]@[domain]
Sous-réseau	Une valeur au format d'adresse IP CIDR	[subnet]	Définissez cette option sur un sous-réseau que d'autres machines peuvent utiliser pour se connecter à Horizon Agent for Linux. S'il existe plusieurs adresses IP locales avec différents sous-réseaux, l'adresse IP locale dans le sous-réseau configuré sera utilisée pour la connexion à Horizon Agent for Linux. Vous devez spécifier la valeur au format d'adresse IP CIDR. Par exemple, Subnet=123.456.7.8/24.

Tableau 4-3. Options de configuration dans /etc/vmware/viewagent-custom.conf (Suite)

Option	Valeur	Valeur par défaut	Description
UEMEnable	true ou false	false	Définissez cette option pour activer ou désactiver les stratégies de carte à puce User Environment Manager. Si l'option est définie sur Activer, et que la condition dans la stratégie de carte à puce User Environment Manager est remplie, les stratégies sont appliquées.
UEMNetworkPath	Une chaîne de texte		Cette option doit être définie sur le chemin de réseau qui est défini dans la Console d'User Environment Manager. Le chemin d'accès doit suivre le format //10.111.22.333/view/LinuxAgent/UEMConfig.

Note Les trois options de sécurité, SSLCiphers, SSLProtocols et SSLCipherServerPreference, sont conçues pour le processus VMwareBlastServer. Lorsque le processus VMwareBlastServer démarre, Java Standalone Agent transmet ces options sous forme de paramètres. Lorsque Blast Secure Gateway (BSG) est activé, ces options affectent la connexion entre BSG et le poste de travail Linux. Lorsque BSG est désactivé, ces options affectent la connexion entre le client et le poste de travail Linux.

Paramètres de stratégie de groupe pour HTML Access

Les paramètres de stratégie de groupe pour HTML Access sont spécifiés dans les fichiers de modèle d'administration ADM et ADMX nommés vdm_blast.adm et vdm_blast.admx. Les modèles sont conçus pour le protocole d'affichage VMware Blast, qui est le seul utilisé par HTML Access.

Pour HTML Access 4.0 et versions ultérieures et Horizon 7 version 7.x, les paramètres de stratégie de groupe VMware Blast sont décrits dans la section « Paramètres de stratégie VMware Blast » dans le document *Configuration des fonctionnalités de poste de travail distant dans Horizon 7*.

Si vous disposez de HTML Access 3.5 ou version antérieure et d'Horizon 6 version 6.2.x ou version antérieure, le tableau suivant décrit des paramètres de stratégie de groupe qui s'appliquent à HTML Access. Dans Horizon 7 version 7.x et versions ultérieures, davantage de paramètres de stratégie de groupe VMware Blast sont disponibles.

Tableau 4-4. Paramètres de stratégie de groupe pour HTML Access 3.5 ou version antérieure et Horizon 6 version 6.2.x ou version antérieure

Paramètre	Description
Effacement d'écran	<p>Permet de contrôler si la machine virtuelle distante peut être vue à l'extérieur d'Horizon 6 pendant une session HTML Access. Par exemple, un administrateur peut utiliser vSphere Web Client pour ouvrir une console sur la machine virtuelle pendant qu'un utilisateur est connecté au poste de travail via HTML Access.</p> <p>Lorsque ce paramètre est activé ou non configuré, et que quelqu'un tente d'accéder à la machine virtuelle distante de l'extérieur d'Horizon 6 pendant qu'une session HTML Access est active, la machine virtuelle distante affiche un écran vide.</p>
Nettoyage de la mémoire de session	<p>Permet de contrôler le nettoyage de la mémoire des sessions distantes abandonnées. Lorsque ce paramètre est activé, vous pouvez définir l'intervalle et le seuil de nettoyage de la mémoire.</p> <p>L'intervalle détermine la fréquence d'exécution du nettoyage de la mémoire. L'intervalle est défini en millisecondes.</p> <p>Le seuil détermine le temps qui doit s'écouler après qu'une session est abandonnée avant qu'elle ne devienne un candidat pour la suppression. Le seuil est défini en millisecondes.</p>
Configurer la redirection du Presse-papiers	<p>Détermine le sens dans lequel la redirection du Presse-papiers est autorisée. Il n'est possible de copier et de coller que du texte. Vous pouvez sélectionner l'une des valeurs suivantes :</p> <ul style="list-style-type: none"> ■ Activé du client vers le serveur seulement (C'est-à-dire autoriser le copier/coller uniquement du client vers le poste de travail distant.) ■ Désactivé dans les deux sens ■ Activé dans les deux sens ■ Activé du serveur vers le client seulement (C'est-à-dire autoriser uniquement le copier/coller du poste de travail distant vers le système client.) <p>Ce paramètre s'applique uniquement à View Agent ou Horizon Agent.</p> <p>Lorsque ce paramètre est désactivé ou n'est pas configuré, la valeur par défaut est Activé du client vers le serveur seulement.</p>
Service HTTP	<p>Permet de changer le port TCP sécurisé (HTTPS) pour Blast Agent service. Le port par défaut est 22443.</p> <p>Activez ce paramètre pour pouvoir changer le numéro de port. Si vous modifiez ce paramètre, vous devez aussi mettre à jour les paramètres du pare-feu correspondant aux postes de travail à distance affectés (sur lesquels View Agent ou Horizon Agent est installé).</p>

Paramètres de sécurité des modèles de configuration d'Horizon Client

Les paramètres liés à la sécurité sont fournis dans les sections Sécurité et Définitions de script des fichiers de modèle d'administration ADM et ADMX d'Horizon Client. Le fichier de modèle d'administration ADM se nomme `vdm_client.adm` et le fichier de modèle d'administration ADMX se nomme `vdm_client.admx`. Sauf indication contraire, les paramètres comprennent uniquement un paramètre Configuration ordinateur. Si un paramètre Configuration utilisateur est disponible et si vous lui définissez une valeur, il remplace le paramètre Configuration ordinateur équivalent.

Le tableau suivant décrit les paramètres figurant dans la section Sécurité des fichiers de modèle d'administration ADM et ADMX.

Tableau 4-5. Modèle de configuration d' Horizon Client : paramètres de sécurité

Paramètre	Description
Allow command line credentials (Paramètre de Configuration d'ordinateur)	Détermine si les informations d'identification d'utilisateur peuvent être fournies avec des options de ligne de commande d'Horizon Client. Si ce paramètre est désactivé, les options smartCardPIN et password ne sont pas disponibles lorsque les utilisateurs exécutent Horizon Client à partir de la ligne de commande. Ce paramètre est activé par défaut. La valeur de Registre Windows équivalente est AllowCmdLineCredentials.
Servers Trusted For Delegation (Paramètre de Configuration d'ordinateur)	Spécifie les instances du Serveur de connexion qui acceptent l'identité et les informations d'identification d'utilisateur qui sont transmises quand un utilisateur coche la case Se connecter en tant qu'utilisateur actuel . Si vous ne spécifiez aucune instance de Serveur de connexion, toutes les instances de Serveur de connexion acceptent ces informations. Pour ajouter une instance de Serveur de connexion, utilisez l'un des formats suivants : <ul style="list-style-type: none"> ■ <code>domain\system\$</code> ■ <code>system\$@domain.com</code> ■ Nom principal de service (SPN) du service Serveur de connexion. La valeur de Registre Windows équivalente est BrokersTrustedForDelegation.
Certificate verification mode (Paramètre de Configuration d'ordinateur)	Configure le niveau de la vérification de certificat exécutée par Horizon Client. Vous pouvez sélectionner l'un de ces modes : <ul style="list-style-type: none"> ■ No Security. Aucune vérification des certificats. ■ Warn But Allow. Un avertissement s'affiche si l'hôte du Serveur de connexion présente un certificat auto-signé, mais l'utilisateur peut continuer à se connecter au Serveur de connexion. Il n'est pas nécessaire que le nom du certificat corresponde au nom du Serveur de connexion fourni par l'utilisateur dans Horizon Client. Si une autre erreur de certificat se produit, une boîte de dialogue d'erreur s'affiche et empêche l'utilisateur de se connecter au Serveur de connexion. Warn But Allow est la valeur par défaut. ■ Full Security. Si une erreur de type de certificat se produit, l'utilisateur ne peut pas se connecter au Serveur de connexion. L'utilisateur voit les erreurs de certificat. <p>Lorsque ce paramètre de stratégie de groupe est configuré, les utilisateurs peuvent voir le mode de vérification de certificat sélectionné dans Horizon Client, mais ils ne peuvent pas configurer le paramètre. La boîte de dialogue de configuration SSL informe les utilisateurs que l'administrateur a verrouillé le paramètre.</p> <p>Lorsque ce paramètre n'est pas configuré ou est désactivé, les utilisateurs d'Horizon Client peuvent sélectionner un mode de vérification de certificat.</p> <p>Si vous ne souhaitez pas configurer le paramètre de vérification des certificats en tant que stratégie de groupe, vous pouvez également activer la vérification des certificats en modifiant les paramètres de registre Windows.</p>

Tableau 4-5. Modèle de configuration d' Horizon Client : paramètres de sécurité (Suite)

Paramètre	Description
Default value of the 'Log in as current user' checkbox (Paramètre de Configuration d'utilisateur et d'ordinateur)	<p>Spécifie la valeur par défaut de la case à cocher Se connecter en tant qu'utilisateur actuel dans la boîte de dialogue de connexion d'Horizon Client.</p> <p>Ce paramètre remplace la valeur par défaut spécifiée au cours de l'installation d'Horizon Client.</p> <p>Si un utilisateur exécute Horizon Client à partir de la ligne de commande et spécifie l'option <code>LogInAsCurrentUser</code>, cette valeur remplace ce paramètre.</p> <p>Lorsque la case Se connecter en tant qu'utilisateur actuel est cochée, l'identité et les informations d'identification que l'utilisateur a fournies lors de la connexion au système client sont transmises à l'instance du Serveur de connexion, puis au poste de travail distant. Lorsque la case n'est pas cochée, les utilisateurs doivent fournir leur identité et leurs informations d'identification plusieurs fois avant de pouvoir accéder à un poste de travail distant.</p> <p>Ce paramètre est désactivé par défaut.</p> <p>La valeur de Registre Windows équivalente est <code>LogInAsCurrentUser</code>.</p>
Display option to Log in as current user (Paramètre de Configuration d'utilisateur et d'ordinateur)	<p>Détermine si la case à cocher Se connecter en tant qu'utilisateur actuel doit être visible dans la boîte de dialogue de connexion d'Horizon Client.</p> <p>Lorsque la case est visible, les utilisateurs peuvent la cocher ou la décocher et remplacer sa valeur par défaut. Lorsque la case est masquée, les utilisateurs ne peuvent pas remplacer sa valeur par défaut dans la boîte de dialogue de connexion d'Horizon Client.</p> <p>Vous pouvez spécifier la valeur par défaut de la case Log in as current user (Se connecter en tant qu'utilisateur actuel) en utilisant le paramètre de règle <code>Default value of the 'Log in as current user' checkbox</code>.</p> <p>Ce paramètre est activé par défaut.</p> <p>La valeur de Registre Windows équivalente est <code>LogInAsCurrentUser_Display</code>.</p>
Enable jump list integration (Paramètre de Configuration d'ordinateur)	<p>Détermine si une liste de raccourcis doit s'afficher dans l'icône Horizon Client sur la barre des tâches des systèmes Windows 7 ou versions ultérieures. La liste de raccourcis permet aux utilisateurs de se connecter à des instances du Serveur de connexion et des postes de travail récents.</p> <p>Si Horizon Client est partagé, vous pouvez ne pas souhaiter que les utilisateurs voient les noms des postes de travail récemment utilisés. Vous pouvez désactiver la liste de raccourcis en désactivant ce paramètre.</p> <p>Ce paramètre est activé par défaut.</p> <p>La valeur de Registre Windows équivalente est <code>EnableJumpList</code>.</p>
Enable SSL encrypted framework channel (Paramètre de Configuration d'utilisateur et d'ordinateur)	<p>Détermine s'il faut activer le canal d'infrastructure chiffré SSL.</p> <ul style="list-style-type: none"> ■ Activer : active SSL, mais autorise le retour à la connexion non chiffrée précédente si le poste de travail distant ne prend pas en charge SSL. ■ Désactiver : désactive SSL. Ce paramètre n'est pas recommandé, mais peut toutefois être utile pour le débogage ou si le canal n'est pas configuré en tunnel et peut par la suite faire l'objet d'une optimisation par un produit accélérateur WAN. ■ Appliquer : active SSL et refuse les connexions aux postes de travail qui ne prennent pas en charge SSL. <p>La valeur de Registre Windows équivalente est <code>EnableTicketSSLAuth</code>.</p>

Tableau 4-5. Modèle de configuration d' Horizon Client : paramètres de sécurité (Suite)

Paramètre	Description
Configures SSL protocols and cryptographic algorithms (Paramètre de Configuration d'utilisateur et d'ordinateur)	<p>Configure la liste de chiffrements afin de limiter l'utilisation de certains protocoles et algorithmes de chiffrement avant l'établissement d'une connexion SSL chiffrée. La liste de chiffrements est composée d'une ou de plusieurs chaînes de chiffrement séparées par deux points.</p> <hr/> <p>Note Toutes les chaînes de chiffrement sont sensibles à la casse.</p> <ul style="list-style-type: none"> ■ La valeur par défaut d'Horizon Client 4.10 et versions ultérieures est TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES. ■ La valeur par défaut d'Horizon Client 4.2 et versions ultérieures est TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES. ■ La valeur par défaut d'Horizon Client 4.0.1 et 4.1 est TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH. ■ La valeur par défaut d'Horizon Client 4.0 est TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH. ■ La valeur par défaut d'Horizon Client 3.5 est TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH. ■ La valeur par défaut d'Horizon Client 3.3 et 3.4 est TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH. ■ La valeur dans Horizon Client 3.2 et versions antérieures est SSLv3:TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH. <hr/> <p>À partir d'Horizon Client 4.10, TLS v1.0 est définitivement désactivé, il n'est donc plus pris en charge.</p> <p>Dans Horizon Client 4.0.1 à 4.9, TLS v1.0, TLS v1.1 et TLS v1.2 sont activés. (SSL v2.0 et v3.0 sont supprimés.) Vous pouvez désactiver TLS v1.0 si la compatibilité TLS v1.0 avec le serveur n'est pas requise.</p> <p>Dans Horizon Client 4.0, TLS v1.1 et TLS v1.2 sont activés. (TLS v1.0 est désactivé. SSL v2.0 et v3.0 sont supprimés.)</p> <p>Dans Horizon Client 3.5, TLS v1.0, TLS v1.1 et TLS v1.2 sont activés. (SSL v2.0 et v3.0 sont désactivés.) Dans Horizon Client 3.3 et 3.4, TLS v1.0 et TLS v1.1 sont activés. (SSL v2.0, SSL v3.0 et TLS v1.2 sont désactivés.)</p> <p>Dans Horizon Client 3.2 et versions antérieures, SSL v3.0 est également activé. (SSL v2.0 et TLS v1.2 sont désactivés.)</p> <p>Les suites de chiffrement utilisent la spécification AES 128 ou 256 bits, suppriment les algorithmes DH anonymes, puis trient la liste de chiffrements actuels par longueur de clé de chiffrement.</p> <p>Lien de référence pour la configuration : http://www.openssl.org/docs/apps/ciphers.html .</p> <p>La valeur de Registre Windows équivalente est SSLCipherList.</p> <p>Si vous ne souhaitez pas configurer ce paramètre en tant que stratégie de groupe, vous pouvez également l'activer en ajoutant le nom de valeur SSLCipherList à l'une des clés de registre suivantes sur l'ordinateur client :</p> <ul style="list-style-type: none"> ■ Pour Windows 32 bits : HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security

Tableau 4-5. Modèle de configuration d' Horizon Client : paramètres de sécurité (Suite)

Paramètre	Description
	<ul style="list-style-type: none"> Pour Windows 64 bits : HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security
Enable Single Sign-On for smart card authentication (Paramètre de Configuration d'ordinateur)	Détermine si l'authentification unique est activée pour l'authentification par carte à puce. Lorsque l'authentification unique est activée, Horizon Client stocke le code PIN de carte à puce chiffré dans la mémoire temporaire avant de l'envoyer au Serveur de connexion. Lorsque l'authentification unique (Single Sign-On) est désactivée, Horizon Client n'affiche pas de boîte de dialogue de code PIN personnalisée. La valeur de Registre Windows équivalente est EnableSmartCardSSO.

Le tableau suivant décrit les paramètres figurant dans la section Définitions de script des fichiers de modèle d'administration ADM et ADMX.

Tableau 4-6. Paramètres liés à la sécurité dans la section Définitions de script

Paramètre	Description
Connect all USB devices to the desktop on launch	Détermine si tous les périphériques USB disponibles sur le système client sont connectés au poste de travail lorsque ce dernier est lancé. Ce paramètre est désactivé par défaut. La valeur de Registre Windows équivalente est connectUSB0nStartup.
Connect all USB devices to the desktop when they are plugged in	Détermine si les périphériques USB sont connectés au poste de travail lorsqu'ils sont branchés sur le système client. Ce paramètre est désactivé par défaut. La valeur de Registre Windows équivalente est connectUSB0nInsert.
Logon Password	Spécifie le mot de passe utilisé par Horizon Client lors de la connexion. Active Directory stocke ce mot de passe en texte brut. Ce paramètre n'est pas défini par défaut. La valeur de Registre Windows équivalente est Password.

Pour plus d'informations sur ces paramètres et leurs implications en termes de sécurité, consultez la documentation d'Horizon Client pour Windows.

Configuration du mode de vérification de certificat d' Horizon Client

Vous pouvez configurer le mode de vérification de certificat d'Horizon Client en ajoutant le nom de valeur CertCheckMode à une clé de registre sur l'ordinateur client.

Sur les systèmes Windows 32 bits, la clé de registre est : HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security. Sur les systèmes Windows 64 bits, la clé de registre est : HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security.

Utilisez une des valeurs suivantes dans la clé de registre :

- 0 : implémente l'option **Ne pas vérifier les certificats d'identité des serveurs.**
- 1 : implémente l'option **Avertir avant de se connecter à des serveurs non approuvés.**

- 2 : implémente l'option **Ne jamais se connecter aux serveurs non approuvés**.

Vous pouvez également configurer le mode de vérification de certificat d'Horizon Client en configurant le paramètre de stratégie de groupe `Mode de vérification des certificats`. Si vous configurez le paramètre de stratégie de groupe et le paramètre `CertCheckMode` dans la clé de registre, le paramètre de stratégie de groupe est prioritaire sur la valeur de la clé de registre.

Lorsque le paramètre de stratégie de groupe ou le paramètre de registre est configuré, les utilisateurs peuvent voir le mode de vérification de certificat sélectionné dans Horizon Client, mais ils ne peuvent pas configurer le paramètre.

Pour plus d'informations sur la configuration du paramètre de stratégie de groupe `Mode de vérification des certificats`, consultez [Paramètres de sécurité des modèles de configuration d'Horizon Client](#).

Configuration de la protection LSA

Horizon Agent et Horizon Client prennent en charge la protection LSA (Local Security Authority). La protection LSA empêche les utilisateurs ayant des informations d'identification non protégées de lire la mémoire et d'injecter du code.

Pour plus d'informations sur la configuration de la protection LSA, lisez la documentation de Microsoft Windows Server.

La fonctionnalité suivante échoue lorsque la protection LSA est configurée pour Horizon Client 4.4 et versions antérieures :

- Se connecter en tant qu'utilisateur actuel

Les fonctions suivantes échouent lorsque la protection LSA est configurée pour les versions d'Horizon Agent antérieures à Horizon 7 version 7.2 :

- Authentification par carte à puce
- authentification unique réelle

Configuration des protocoles de sécurité et des suites de chiffrement

5

Vous pouvez configurer les protocoles de sécurité et les suites de chiffrement qui sont acceptés et proposés entre les composants d'Horizon Client, de View Agent/Horizon Agent et du serveur.

Ce chapitre contient les rubriques suivantes :

- [Stratégies par défaut pour les protocoles de sécurité et les suites de chiffrement](#)
- [Configuration des protocoles de sécurité et des suites de chiffrement pour des types de client spécifiques](#)
- [Désactiver des chiffrements faibles dans les protocoles SSL/TLS](#)
- [Configurer des protocoles de sécurité et des suites de chiffrement pour l'agent HTML Access](#)
- [Configurer des stratégies de proposition sur des postes de travail distants](#)

Stratégies par défaut pour les protocoles de sécurité et les suites de chiffrement

Les stratégies d'acceptation et de proposition générales activent certains protocoles de sécurité et certaines suites de chiffrement par défaut.

Les tableaux suivants répertorient les protocoles et les suites de chiffrement qui sont activés par défaut pour Horizon Client. Dans Horizon Client 3.1 et versions ultérieures pour Windows, Linux et Mac, ces suites de chiffrement et ces protocoles sont également utilisés pour chiffrer le canal USB (communication entre le démon de service USB et View Agent ou Horizon Agent). Pour les versions d'Horizon Client antérieures à la version 4.0, le démon de service USB ajoute RC4 (:RC4-SHA: +RC4) à la fin de la chaîne de commande de chiffrement lorsqu'il se connecte à un poste de travail distant. RC4 n'est plus ajouté à partir d'Horizon Client 4.0.

Horizon Client 4.2 et versions ultérieures

Tableau 5-1. Protocoles de sécurité et suites de chiffrement activés par défaut dans Horizon Client 4.2 et versions ultérieures

Protocoles de sécurité par défaut	Suites de chiffrement par défaut
TLS 1.2	<ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
<ul style="list-style-type: none"> ■ TLS 1.1 ■ TLS 1.0 	<ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)

Note À partir d'Horizon Client 4.10, TLS v1.0 est définitivement désactivé, il n'est donc plus pris en charge.

Tableau 5-1. Protocoles de sécurité et suites de chiffrement activés par défaut dans Horizon Client 4.2 et versions ultérieures (Suite)

Protocoles de sécurité par défaut	Suites de chiffrement par défaut
	<ul style="list-style-type: none"> ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

À partir d'Horizon Client 4.10, TLS v1.0 est définitivement désactivé, il n'est donc plus pris en charge.

Dans Horizon Client 4.2 à 4.9, TLS v1.0 est activé par défaut pour garantir que, par défaut, Horizon Client peut se connecter à des serveurs Horizon Cloud avec infrastructure hébergée. La chaîne de chiffrement par défaut est !aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES. Vous pouvez désactiver TLS v1.0 si la compatibilité TLS v1.0 avec le serveur n'est pas requise.

Horizon Client 4.0.1 et 4.1

Tableau 5-2. Protocoles de sécurité et suites de chiffrement activés par défaut dans Horizon Client 4.0.1 et 4.1

Protocoles de sécurité par défaut	Suites de chiffrement par défaut
TLS 1.2	<ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
<ul style="list-style-type: none"> ■ TLS 1.1 ■ TLS 1.0 	<ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)

Tableau 5-2. Protocoles de sécurité et suites de chiffrement activés par défaut dans Horizon Client 4.0.1 et 4.1 (Suite)

Protocoles de sécurité par défaut	Suites de chiffrement par défaut
	<ul style="list-style-type: none">■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

TLS 1.0 est activé par défaut pour garantir que, par défaut, Horizon Client peut se connecter à des serveurs Horizon Cloud avec infrastructure hébergée. La chaîne de chiffrement par défaut est TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH. Vous pouvez désactiver TLS 1.0 si la compatibilité TLS 1.0 avec le serveur n'est pas requise.

Horizon Client 4.0

Tableau 5-3. Protocoles de sécurité et suites de chiffrement activés par défaut dans Horizon Client 4.0

Protocoles de sécurité par défaut	Suites de chiffrement par défaut
TLS 1.2	<ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
<ul style="list-style-type: none"> ■ TLS 1.1 	<ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)

Tableau 5-3. Protocoles de sécurité et suites de chiffrement activés par défaut dans Horizon Client 4.0 (Suite)

Protocoles de sécurité par défaut	Suites de chiffrement par défaut
	<ul style="list-style-type: none"><li data-bbox="625 296 1423 327">■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)<li data-bbox="625 331 1423 363">■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Important TLS 1.0 est désactivé par défaut. SSL 3.0 a été supprimé.

Horizon Client 3.5

Tableau 5-4. Protocoles de sécurité et suites de chiffrement activés par défaut dans Horizon Client 3.5

Protocoles de sécurité par défaut	Suites de chiffrement par défaut
TLS 1.2	<ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032) ■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) ■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031) ■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) ■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)
<ul style="list-style-type: none"> ■ TLS 1.1 ■ TLS 1.0 	<ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)

Tableau 5-4. Protocoles de sécurité et suites de chiffrement activés par défaut dans Horizon Client 3.5 (Suite)

Protocoles de sécurité par défaut	Suites de chiffrement par défaut
	<ul style="list-style-type: none"> ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Horizon Client 3.3 et 3.4

Tableau 5-5. Protocoles de sécurité et suites de chiffrement activés par défaut dans Horizon Client 3.3 et 3.4

Protocoles de sécurité par défaut	Suites de chiffrement par défaut
<ul style="list-style-type: none"> ■ TLS 1.1 ■ TLS 1.0 	<ul style="list-style-type: none"> ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Note TLS 1.2 est également pris en charge, mais il n'est pas activé par défaut. Pour activer TLS 1.2, suivez les instructions dans [l'article 2121183 de la base de connaissances de VMware](#), après lequel les suites de chiffrement répertoriées dans [Tableau 5-4](#) sont prises en charge.

Horizon Client 3.0, 3.1 et 3.2

Tableau 5-6. Protocoles de sécurité et suites de chiffrement activés par défaut dans Horizon Client 3.0, 3.1 et 3.2

Protocoles de sécurité par défaut	Suites de chiffrement par défaut
<ul style="list-style-type: none"> ■ TLS 1.1 ■ TLS 1.0 ■ SSL 3.0 (activé sur les clients Windows uniquement) 	<ul style="list-style-type: none"> ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) ■ TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA (0xc022) ■ TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA (0xc021) ■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f) ■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005) ■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) ■ TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA (0xc01f) ■ TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA (0xc01e) ■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e) ■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004) ■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) ■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Note TLS 1.2 est également pris en charge, mais il n'est pas activé par défaut. Pour activer TLS 1.2, suivez les instructions dans [l'article 2121183 de la base de connaissances de VMware](#), après lequel les suites de chiffrement répertoriées dans [Tableau 5-4](#) sont prises en charge.

Configuration des protocoles de sécurité et des suites de chiffrement pour des types de client spécifiques

Chaque type de client dispose de sa propre méthode de configuration des protocoles et des suites de chiffrement utilisés.

Vous devez modifier les protocoles de sécurité dans Horizon Client uniquement si votre serveur View Server ne prend pas en charge les paramètres actuels. Si vous configurez un protocole de sécurité pour Horizon Client qui n'est pas activé sur le serveur View Server auquel le client se connecte, une erreur TLS/SSL se produit et la connexion échoue.

Pour modifier les valeurs par défaut des protocoles et des chiffrements, utilisez le mécanisme spécifique au client :

- Sur les systèmes clients Windows, vous pouvez utiliser un paramètre de stratégie de groupe ou un paramètre de registre Windows.
- Sur les systèmes clients Windows 10 UWP, vous pouvez utiliser le paramètre Options SSL dans les options d'Horizon Client.
- Sur les systèmes clients Linux, vous pouvez utiliser des propriétés de fichier de configuration ou des options de ligne de commande.

- Sur les systèmes clients Mac, vous pouvez utiliser un paramètre Préférence dans Horizon Client.
- Sur les systèmes clients iOS, Android et Chrome OS, vous pouvez utiliser un paramètre Options SSL avancées dans les paramètres d'Horizon Client.

Pour plus d'informations, consultez la documentation Horizon Client.

Désactiver des chiffrements faibles dans les protocoles SSL/TLS

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

Procédure

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

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

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

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

Configurer des protocoles de sécurité et des suites de chiffrement pour l'agent HTML Access

À partir de View Agent 6.2, vous pouvez configurer les suites de chiffrement que l'agent HTML Access utilise en modifiant le registre Windows. À partir de View Agent 6.2.1, vous pouvez également configurer les protocoles de sécurité utilisés. Vous pouvez également spécifier les configurations dans un objet de stratégie de groupe (GPO).

Avec View Agent 6.2.1 et versions ultérieures, par défaut, l'agent HTML Access utilise uniquement TLS 1.1 et TLS 1.2. Les protocoles autorisés sont, du plus faible au plus élevé, TLS 1.0, TLS 1.1 et TLS 1.2. Les protocoles plus anciens, tels que SSLv3 et version antérieure, ne sont jamais autorisés. Deux valeurs de registre, `SslProtocolLow` et `SslProtocolHigh`, déterminent la plage de protocoles que l'agent HTML Access acceptera. Par exemple, les paramètres `SslProtocolLow=tls_1.0` et `SslProtocolHigh=tls_1.2` forceront l'agent HTML Access à accepter TLS 1.0, TLS 1.1 et TLS 1.2. Les paramètres par défaut sont `SslProtocolLow=tls_1.1` et `SslProtocolHigh=tls_1.2`.

Vous devez spécifier la liste de chiffrements utilisant le format défini dans <https://www.openssl.org/docs/manmaster/man1/ciphers.html>, sous la section CIPHER LIST FORMAT (Format de liste de chiffrements). La liste de chiffrements suivante est celle par défaut :

```
ECDHE-RSA-AES256-SHA:AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
```

Procédure

- 1 Démarrez l'éditeur du Registre Windows.
- 2 Accédez à la clé de registre `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config`.
- 3 Ajoutez deux nouvelles valeurs de chaîne (REG_SZ), `SslProtocolLow` et `SslProtocolHigh`, pour spécifier la plage de protocoles.

Les données des valeurs de registre doivent être `tls_1.0`, `tls_1.1` ou `tls_1.2`. Pour activer un seul protocole, spécifiez le même protocole pour les deux valeurs de registre. Si l'une des valeurs de registre n'existe pas ou si ses données ne sont pas définies sur l'un des trois protocoles, les protocoles par défaut seront utilisés.

- 4 Ajoutez une nouvelle valeur de chaîne (REG_SZ), `SslCiphers`, pour spécifier une liste de suites de chiffrement.

Saisissez ou collez la liste de suites de chiffrement dans le champ de données de la valeur de registre. Par exemple,

```
ECDHE-RSA-AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
```

- 5 Redémarrez VMware Blast de service Windows.

Pour reprendre l'utilisation de la liste de chiffrements par défaut, supprimez la valeur de registre `SslCiphers` et redémarrez VMware Blast de service Windows. Ne supprimez pas simplement la partie données de la valeur, car l'agent HTML Access traitera alors tous les chiffrements comme étant inacceptables, conformément à la définition de format de la liste de chiffrements OpenSSL.

Lorsque l'agent HTML Access démarre, il écrit les informations sur le protocole et le chiffrement dans son fichier journal. Vous pouvez examiner le fichier journal pour voir les valeurs qui sont appliquées.

Les protocoles et les suites de chiffrement par défaut pourront changer à l'avenir en fonction de l'évolution des meilleures pratiques de VMware concernant la sécurité du réseau.

Configurer des stratégies de proposition sur des postes de travail distants

Vous pouvez contrôler la sécurité des connexions Bus de messages à un Serveur de connexion en configurant les stratégies de proposition sur des postes de travail distants qui exécutent Windows.

Assurez-vous que le Serveur de connexion est configuré pour accepter les mêmes stratégies afin d'éviter un échec de connexion.

Procédure

- 1 Lancez l'éditeur du Registre Windows sur le poste de travail distant.
- 2 Accédez à la clé de registre `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration`.
- 3 Ajoutez une nouvelle valeur de chaîne (REG_SZ), `ClientSSLSecureProtocols`.
- 4 Définissez la valeur sur une liste de suites de chiffrement au format `\LIST:protocol_1,protocol_2,...`
Répertoriez les protocoles avec le dernier protocole en premier. Par exemple :

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

- 5 Ajoutez une nouvelle valeur de chaîne (REG_SZ), `ClientSSLCipherSuites`.
- 6 Définissez la valeur sur une liste de suites de chiffrement au format `\LIST:cipher_suite_1,cipher_suite_2,...`

La liste doit être dans l'ordre de préférence, avec la suite de chiffrement préférée en premier. Par exemple :

```
\LIST:TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

Emplacements des fichiers journaux du client et de l'agent

6

Les clients et l'agent créent des fichiers journaux qui enregistrent l'installation et le fonctionnement de leurs composants.

Ce chapitre contient les rubriques suivantes :

- [Journaux d'Horizon Client pour Windows](#)
- [Journaux d'Horizon Client pour Mac](#)
- [Journaux d'Horizon Client pour Linux](#)
- [Journaux d'Horizon Client sur des périphériques mobiles](#)
- [Journaux d'Horizon Agent de machines Windows](#)
- [Journaux de poste de travail Linux](#)

Journaux d'Horizon Client pour Windows

Les fichiers journaux peuvent permettre de résoudre des problèmes liés à l'installation, au protocole d'affichage et divers composants de fonctionnalité. Vous pouvez utiliser des paramètres de stratégie de groupe pour configurer l'emplacement, le niveau de détail et la période de conservation de certains fichiers journaux.

Emplacement du journal

Pour les noms de fichier dans le tableau suivant, *YYYY* représente l'année, *MM* le mois, *DD* le jour et *XXXXXX* un nombre.

Tableau 6-1. Fichiers journaux d'Horizon Client pour Windows

Type de journaux	Chemin du répertoire	Nom de fichier
Installation	C:\Users\%username%\AppData\Local\Temp	vminst.log_XXXXXX_XXXXXX.txt vmmsi.log_XXXXXX_XXXXXX.txt
Client PCoIP Du processus vmware-remotemks.exe	C:\Users\%username%\AppData\Local\Temp	pcoip_client_YYYY_MM_DD_XXXXXX.txt Note Vous pouvez utiliser un GPO pour configurer le niveau de journalisation, entre 0 et 3 (le plus détaillé). Utilisez le fichier de modèle ADMX des variables de session de client View PCoIP (pcoip.admx). Le paramètre s'appelle Configurer le niveau de détails du journal des événements PCoIP .
Interface utilisateur d'Horizon Client Du processus vmware-view.exe	C:\Users\%username%\AppData\Local\VMware\VDM\Logs	vmware-horizon-viewclient-YYYY-MM-DD-XXXXXX.txt Note Vous pouvez utiliser un GPO pour configurer l'emplacement du journal. Utilisez le fichier de modèle ADMX de configuration commune de View sur le fichier vdm_common.admx.
Journaux d'Horizon Client Du processus vmware-view.exe	C:\Users\%username%\AppData\Local\Temp\vmware-username-XXXXXX	vmware-crtbora-XXXXXX.log
Cadre de message	C:\Users\%username%\AppData\Local\VMware\VDM\Logs	log-YYYY-MM-DD-XXXXXX.txt debug-YYYY-MM-DD-XXXXXX.txt
Journaux MKS (souris-clavier-écran) distants Du processus vmware-remotemks.exe	C:\Users\%username%\AppData\Local\Temp\vmware-username	ViewMP-Client-XXXXXX.log vmware-mks-XXXXXX.log vmware-rdeSvc-XXXXXX.log vmware-vvaClient-XXXXXX.log
Client Tsdr Du processus vmware-remotemks.exe	C:\Users\%username%\AppData\Local\Temp\vmware-username	vmware-ViewTsdr-Client-XXXXXX.log
Client Tsmmr Du processus vmware-remotemks.exe	C:\Users\%username%\AppData\Local\Temp\vmware-username	vmware-ViewTsmmr-Client-XXXXXX.log
Client VdpService Du processus vmware-remotemks.exe	C:\Users\%username%\AppData\Local\Temp\vmware-username	vmware-udpServiceClient-XXXXXX.log
Service WSNM Du processus wsnm.exe	C:\ProgramData\VMware\VDM\logs	debug-yyyy-mm-dd-XXXXXX.txt Note Vous pouvez utiliser un GPO pour configurer l'emplacement du journal. Utilisez le fichier de modèle ADMX de configuration commune de View sur le fichier vdm_common.admx.

Tableau 6-1. Fichiers journaux d'Horizon Client pour Windows (Suite)

Type de journaux	Chemin du répertoire	Nom de fichier
redirection USB À partir du processus vmware-view-usbd.exe ou vmware-remotemks.exe	C:\ProgramData\VMware\VDM\Logs	debug-yyyy-mm-dd-XXXXXX.txt Dans Horizon Client 4.4 et versions ultérieures, le processus vmware-view-usbd.exe est supprimé et le processus USB D est déplacé vers le processus vmware-remotemks.exe.
		Note Vous pouvez utiliser un GPO pour configurer l'emplacement du journal. Utilisez le fichier de modèle ADMX de configuration commune de View sur le fichier vdm_common.admx.
Redirection de port série Du processus vmwsprrdpwks.exe	C:\ProgramData\VMware\VDM\Logs	Serial*.txt Netlink*.txt
Redirection de scanner Du processus ftscanmgr.exe	C:\ProgramData\VMware\VDM\Logs	Scanner*.txt Netlink*.txt

Configuration du journal

Vous pouvez utiliser des paramètres de stratégie de groupe pour apporter des modifications à la configuration :

- Pour les journaux de client PCoIP, vous pouvez configurer le niveau de journalisation, entre 0 et 3 (le plus détaillé). Utilisez le fichier de modèle ADMX des variables de session de client View PCoIP (pcoip.admx). Le paramètre s'appelle **Configurer le niveau de détails du journal des événements PCoIP**.
- Pour les journaux d'interface utilisateur du client, configurez l'emplacement du journal, le niveau de détail et la stratégie de conservation. Utilisez le fichier de modèle ADMX de configuration commune de View sur le fichier vdm_common.admx.
- Pour les journaux de redirection USB, configurez l'emplacement du journal, le niveau de détail et la stratégie de conservation. Utilisez le fichier de modèle ADMX de configuration commune de View sur le fichier vdm_common.admx.
- Pour les journaux de service WSNM, configurez l'emplacement du journal, le niveau de détail et la stratégie de conservation. Utilisez le fichier de modèle ADMX de configuration commune de View sur le fichier vdm_common.admx.

Vous pouvez également utiliser une commande de ligne de commande pour définir un niveau de détail. Accédez au répertoire C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT et entrez la commande suivante :

```
support.bat loglevels
```

Une nouvelle fenêtre d'invite de commande s'affiche et vous êtes invité à sélectionner un niveau de détail.

Collecte d'un bundle de journaux

Vous pouvez utiliser l'interface utilisateur du client ou une commande de ligne de commande pour collecter des journaux dans un fichier .zip que vous pouvez envoyer au support technique de VMware.

- Dans la fenêtre **Horizon Client**, dans le menu Options, sélectionnez **Informations de support** et, dans la boîte de dialogue qui s'affiche, cliquez sur **Collecter des données de support**.
- À partir de la ligne de commande, accédez au répertoire C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT et entrez la commande suivante :
support.bat.

Journaux d'Horizon Client pour Mac

Les fichiers journaux peuvent permettre de résoudre des problèmes liés à l'installation, au protocole d'affichage et divers composants de fonctionnalité. Vous pouvez créer un fichier de configuration pour configurer le niveau de détail.

Emplacement du journal

Tableau 6-2. Fichiers journaux d'Horizon Client pour Mac

Type de journaux	Chemin du répertoire	Nom de fichier
Interface utilisateur d'Horizon Client	~/Library/Logs/VMware Horizon Client	
Client PCoIP	~/Library/Logs/VMware Horizon Client	
Audio/Vidéo en temps réel	~/Library/Logs/VMware	vmware-RTAV-pid.log
redirection USB	~/Library/Logs/VMware	
VChan	~/Library/Logs/VMware Horizon Client	
Journaux MKS (souris-clavier-écran) distants	~/Library/Logs/VMware	
Crtbora	~/Library/Logs/VMware	

Configuration du journal

Dans Horizon Client 3.1 et version ultérieure, Horizon Client génère des fichiers journaux dans le répertoire `~/Library/Logs/VMware Horizon Client` du client Mac. Les administrateurs peuvent configurer le nombre maximal de fichiers journaux et le nombre maximal de jours de conservation des fichiers journaux en définissant des clés dans le fichier `/Library/Preferences/com.vmware.horizon.plist` sur un client Mac.

Tableau 6-3. Clés plist pour la collecte de fichiers journaux

Clé	Description
MaxDebugLogs	Nombre maximal de fichiers journaux. La valeur maximale est de 100.
MaxDaysToKeepLogs	Nombre maximal de jours de conservation des fichiers journaux. Cette valeur n'a pas de limite.

Les fichiers qui ne correspondent pas à ces critères sont supprimés lorsque vous lancez Horizon Client.

Si les clés `MaxDebugLogs` ou `MaxDaysToKeepLogs` ne sont pas définies dans le fichier `com.vmware.horizon.plist`, le nombre par défaut de fichiers journaux est de 5 et les fichiers sont conservés 7 jours par défaut.

Journaux d'Horizon Client pour Linux

Les fichiers journaux peuvent permettre de résoudre des problèmes liés à l'installation, au protocole d'affichage et divers composants de fonctionnalité. Vous pouvez créer un fichier de configuration pour configurer le niveau de détail.

Emplacement du journal

Tableau 6-4. Fichiers journaux d'Horizon Client pour Linux

Type de journaux	Chemin du répertoire	Nom de fichier
Installation	<code>/tmp/vmware-root/</code>	<code>.vmware-installer-pid.log</code> <code>vmware-vmis-pid.log</code>
Interface utilisateur d'Horizon Client	<code>/tmp/vmware-username/</code>	<code>vmware-horizon-client-pid.log</code>
Client PCoIP	<code>/tmp/teradici-username/</code>	<code>pcoip_client_YYYY_MM_DD_XXXXXX.log</code>
Audio/Vidéo en temps réel	<code>/tmp/vmware-username/</code>	<code>vmware-RTAV-pid.log</code>
redirection USB	<code>/tmp/vmware-root/</code>	<code>vmware-usbarb-pid.log</code> <code>vmware-view-usbd-pid.log</code>
VChan	<code>/tmp/vmware-username/</code>	<code>VChan-Client.log</code>

Note Ce journal est créé lorsque vous activez les journaux RDPVCBridge en définissant « `export VMW_RDPVC_BRIDGE_LOG_ENABLED=1` ».

Tableau 6-4. Fichiers journaux d'Horizon Client pour Linux (Suite)

Type de journaux	Chemin du répertoire	Nom de fichier
Journaux MKS (souris-clavier-écran) distants	/tmp/vmware-username/	vmware-mks-pid.log vmware-MKSVchanClient-pid.log vmware-rdeSvc-pid.log
Client VdpService	/tmp/vmware-username/	vmware-vdpServiceClient-pid.log
Client Tsdr	/tmp/vmware-username/	vmware-ViewTsdr-Client-pid.log

Configuration du journal

Vous pouvez utiliser une propriété de configuration (`view.defaultLogLevel`) pour définir le niveau de détail des journaux clients, qui va de 0 (collecter tous les événements) à 6 (collecter uniquement les événements critiques).

Pour les journaux USB, vous pouvez utiliser les commandes de ligne de commande suivantes :

```
vmware-usbarbitrator --verbose
vmware-view-usbd -o log:trace
```

Collecte d'un bundle de journaux

Le collecteur de journaux se trouve à l'emplacement `/usr/bin/vmware-view-log-collector`. Pour utiliser le collecteur de journaux, vous devez disposer d'autorisations d'exécution. Vous pouvez définir des autorisations à partir de la ligne de commande Linux en entrant la commande suivante :

```
chmod +x /usr/bin/vmware-view-log-collector
```

Vous pouvez exécuter le collecteur de journaux à partir d'une ligne de commande Linux en entrant la commande suivante :

```
/usr/bin/vmware-view-log-collector
```

Journaux d'Horizon Client sur des périphériques mobiles

Sur des périphériques mobiles, vous pouvez avoir besoin d'installer un programme tiers afin d'accéder au répertoire où sont stockés les fichiers journaux. Les clients mobiles disposent de paramètres de configuration pour envoyer des bundles de journaux à VMware. Comme la journalisation peut affecter les performances, vous devez activer la journalisation uniquement lorsque vous avez besoin de résoudre un problème.

Journaux de client iOS

Pour les clients iOS, les fichiers journaux se trouvent dans les répertoires `tmp` et `Documents` sous `User Programs/Horizon/`. Pour accéder à ces répertoires, vous devez d'abord installer une application tierce comme `iFunbox`.

Vous pouvez activer la journalisation en activant le paramètre **Journalisation** dans les paramètres d'Horizon Client. Avec ce paramètre activé, si le client se ferme de manière inattendue ou si vous fermez le client et que vous le relancez, les fichiers journaux sont fusionnés et compressés dans un fichier GZ unique. Vous pouvez ensuite envoyer le bundle à VMware par e-mail. Si votre périphérique est connecté à un PC ou à un Mac, vous pouvez également utiliser iTunes pour extraire les fichiers journaux.

Journaux de client Android

Pour les clients Android, les fichiers journaux se trouvent dans le répertoire `Android/data/com.vmware.view.client.android/files/`. Pour accéder à ce répertoire, vous devez d'abord installer une application tierce comme File Explorer ou My Files.

Par défaut, les journaux sont créés uniquement lorsque l'application se ferme de manière inattendue. Vous pouvez modifier cette valeur par défaut en activant le paramètre **Activer le journal** dans les paramètres d'Horizon Client. Pour envoyer un bundle de journaux à VMware par e-mail, vous pouvez utiliser le paramètre **Envoyer le journal** dans les paramètres généraux du client.

Journaux de client Chrome OS

Pour les clients Chrome OS, les journaux sont disponibles uniquement via la console JavaScript.

Journaux de client Windows 10 UWP

Pour les clients Windows 10 UWP, les journaux se trouvent dans le répertoire `C:\Windows\Users\%username%\AppData\Local\VMware\VDM\Logs`.

Vous pouvez activer la journalisation en activant l'option **Activer la journalisation avancée** dans la section Journalisation des options d'Horizon Client et en cliquant sur le bouton **Collecte des informations de support**. Vous êtes invité à sélectionner un dossier pour les journaux, et vous pouvez compresser le dossier comme vous le feriez pour tout autre dossier.

Journaux de client Windows Store

Pour les clients Windows Store sur lesquels Horizon Client pour Windows Store est installé, au lieu d'Horizon Client pour Windows, les fichiers journaux se trouvent dans le répertoire `C:\Users\%username%\AppData\Local\Packages\VMwareInc.VMwareViewClient_23chmsjxv380w\LocalState\logs`.

Vous pouvez activer la journalisation en activant le paramètre **Activer la journalisation avancée** dans les paramètres généraux d'Horizon Client, puis en cliquant sur le bouton **Collecte des informations de support**. Vous êtes invité à sélectionner un dossier pour les journaux, et vous pouvez compresser le dossier comme vous le feriez pour tout autre dossier.

Journaux d' Horizon Agent de machines Windows

Les fichiers journaux peuvent permettre de résoudre des problèmes liés à l'installation, au protocole d'affichage et divers composants de fonctionnalité. Vous pouvez utiliser des paramètres de stratégie de groupe pour configurer l'emplacement, le niveau de détail et la période de conservation de certains fichiers journaux.

Emplacement du journal

Pour les noms de fichier dans le tableau suivant, *YYYY* représente l'année, *MM* le mois, *DD* le jour et *XXXXXX* un nombre.

Tableau 6-5. Fichiers journaux d'Horizon Client pour Windows

Type de journaux	Chemin du répertoire	Nom de fichier
Installation	C:\Users\%username%\AppData\Local\Temp	vminst.log_XXXXXX_XXXXXX.txt vmmsi.log_XXXXXX_XXXXXX.txt
View Agent (pour Horizon 6) ou Horizon Agent (pour Horizon 7)	<Drive Letter>:\ProgramData\VMware\VDM\logs	pcoip_agent_YYYY_MM_DD_XXXXXX.txt pcoip_agent_YYYY_MM_DD_XXXXXX.txt vmware-vdpServiceServer-XXXXXX.log Serial*.txt Scanner*.txt Netlink*.txt debug-yyyy-mm-dd-XXXXXX.txt

Note Vous pouvez utiliser un GPO pour configurer l'emplacement du journal. Utilisez le fichier de modèle ADMX de configuration commune de View sur le fichier `vdm_common.admx`.

Configuration du journal

Il existe plusieurs méthodes pour configurer des options de journalisation.

- Vous pouvez utiliser des paramètres de stratégie de groupe pour configurer l'emplacement du journal, le niveau de détail et la stratégie de conservation. Utilisez le fichier de modèle ADMX de configuration commune de View sur le fichier `vdm_common.admx`.
- Vous pouvez utiliser une commande de ligne de commande pour définir un niveau de détail. Accédez au répertoire `C:\Program Files\VMware\VMware View\Agent\DCT` et entrez la commande suivante : `support.bat loglevels`. Une nouvelle fenêtre d'invite de commande s'affiche et vous êtes invité à sélectionner un niveau de détail.
- Vous pouvez utiliser la commande `vdmadmin` avec l'option `-A` pour configurer la journalisation par View Agent ou Horizon Agent. Pour obtenir des instructions, reportez-vous au document *Administration d'Horizon 7*.

Collecte d'un bundle de journaux

Vous pouvez utiliser une commande de ligne de commande pour collecter des journaux dans un fichier .zip que vous pouvez envoyer au support technique de VMware. À partir de la ligne de commande, accédez au répertoire `C:\Program Files\VMware\VMware View\Agent\DCT` et entrez la commande suivante : `support.bat`.

Journaux de poste de travail Linux

Les fichiers journaux peuvent permettre de résoudre des problèmes liés à l'installation, au protocole d'affichage et divers composants de fonctionnalité. Vous pouvez créer un fichier de configuration pour configurer le niveau de détail.

Emplacement du journal

Tableau 6-6. Fichiers journaux de poste de travail Linux

Type de journaux	Chemin du répertoire
Installation	<code>/tmp/vmware-root</code>
View Agent (pour Horizon 6) ou Horizon Agent (pour Horizon 7)	<code>/var/log/vmware</code>
View Agent (pour Horizon 6) ou Horizon Agent (pour Horizon 7)	<code>/usr/lib/vmware/viewagent/viewagent-debug.log</code>

Configuration du journal

Modifiez le fichier `/etc/vmware/config` pour configurer la journalisation.

Collecte d'un bundle de journaux

Vous pouvez créer un bundle DCT (Data Collection Tool) qui rassemble les informations de configuration de la machine et se connecte à une archive compressée. Ouvrez une invite de commande dans le poste de travail Linux et exécutez le script `dct-debug.sh`.

```
sudo /usr/lib/vmware/viewagent/bin/dct-debug.sh
```

L'archive est générée dans le répertoire depuis lequel le script était exécuté (le répertoire de travail actuel). Le nom de fichier inclut le système d'exploitation, l'horodatage et d'autres informations ; par exemple : `ubuntu-12-vdm-sdct-20150201-0606-agent.tgz`

Cette commande collecte des fichiers journaux depuis les répertoires `/tmp/vmware-root` et `/var/log/vmware`. Elle collecte également les fichiers journaux système et les fichiers de configuration suivants :

- `/var/log/messages*`
- `/var/log/syslog*`

- /var/log/boot*.log
- /proc/cpuinfo, /proc/meminfo, /proc/vmstat, /proc/loadavg
- /var/log/audit/auth.log*
- /etc/hosts
- /etc/resolv.conf
- /etc/nsswitch.conf
- /var/log/Xorg*
- /etc/X11/xorg.conf
- Les fichiers noyaux dans /usr/lib/vmware/viewagent
- Les fichiers de blocage dans /var/crash/_usr_lib_vmware_viewagent*

Application de correctifs de sécurité

7

Les versions de correctif peuvent inclure des fichiers de programme d'installation pour les composants d'Horizon 6 ou d'Horizon 7 suivants : View Composer, Serveur de connexion, View Agent ou Horizon Agent et divers clients. Les composants de correctif que vous devez appliquer dépendent des correctifs de bogue dont votre déploiement a besoin.

En fonction des correctifs de bogue dont vous avez besoin, installez les composants d'Horizon 6 ou d'Horizon 7 applicables dans l'ordre suivant :

- 1 View Composer
- 2 Serveur de connexion
- 3 View Agent (pour Horizon 6) ou Horizon Agent (pour Horizon 7)
- 4 Horizon Client

Pour obtenir des instructions sur l'application de correctifs pour les composants de serveur, consultez le document *Mises à niveau d'Horizon 7*.

Ce chapitre contient les rubriques suivantes :

- [Appliquer un correctif pour View Agent ou Horizon Agent](#)
- [Appliquer un correctif à Horizon Client](#)

Appliquer un correctif pour View Agent ou Horizon Agent

L'application d'un correctif nécessite le téléchargement et l'exécution du programme d'installation pour la version du correctif.

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

Conditions préalables

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

Procédure

- 1 Sur l'ensemble des machines virtuelles parentes, machines virtuelles utilisées pour les modèles de clone complet, clones complets dans un pool et machines virtuelles individuelles ajoutées manuellement, téléchargez le fichier du programme d'installation pour la version de correctif de View Agent (pour Horizon 6) ou Horizon Agent (pour Horizon 7).

Votre contact chez VMware vous fournira des instructions sur ce téléchargement.

- 2 Exécutez le programme d'installation que vous avez téléchargé pour la version de correctif de View Agent ou Horizon Agent.

Note Dans la version 6.2 et les versions ultérieures d'Horizon 6, vous n'avez pas à désinstaller la version précédente avant d'installer le correctif.

- 3 Si vous désactivez l'approvisionnement de nouvelles machines virtuelles en préparation pour l'application d'un correctif à View Composer, activez de nouveau l'approvisionnement.
- 4 Pour les machines virtuelles parentes qui seront utilisées pour créer des pools de postes de travail de clone lié, prenez un snapshot de la machine virtuelle.

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

Appliquer un correctif à Horizon Client

L'application d'un correctif sur un poste de travail client nécessite le téléchargement et l'exécution du programme d'installation pour la version du correctif. Sur les clients mobiles, l'application d'un correctif implique l'installation de la mise à jour auprès d'un site Web qui vend des applications, tel que Google Play, Windows Store ou l'App Store d'Apple.

Procédure

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

Votre contact chez VMware vous fournira des instructions sur ce téléchargement. Vous pouvez également accéder à la page de téléchargement du client à l'adresse <http://www.vmware.com/go/viewclients>. Comme mentionné précédemment, pour certains clients, vous pouvez obtenir la version du correctif auprès d'un App Store.

- 2 Si le périphérique client est un poste de travail ou un ordinateur portable Mac ou Linux, supprimez la version actuelle du logiciel client de votre périphérique.

Utilisez la méthode spécifique du périphérique habituelle pour supprimer des applications.

Note Avec la version 3.5 et les versions ultérieures d'Horizon Client pour Windows, vous n'avez pas à désinstaller la version précédente avant d'installer le correctif sur les clients Windows. Avec la version 4.1 et les versions ultérieures d'Horizon Client pour Windows, vous pouvez activer la fonctionnalité Mise à niveau d'Horizon Client en ligne afin de mettre à niveau Horizon Client en ligne sur les clients Windows. Avec Horizon Client pour Mac 4.4 et versions ultérieures, vous pouvez activer la fonctionnalité Mise à niveau d'Horizon Client en ligne afin de mettre à niveau Horizon Client en ligne sur des clients Mac.

- 3 Le cas échéant, exécutez le programme d'installation que vous avez téléchargé pour la version de correctif d'Horizon Client.

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

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