Sécurité d'Horizon Client et d'Horizon Agent

Horizon Client 3.x/4.x et View Agent 6.2.x/Horizon Agent 7.0.x

Mars 2016

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

FR-001997-00

vmware®

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

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

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

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

docfeedback@vmware.com

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

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

Table des matières

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 de View*, 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 1

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 aborde les rubriques suivantes :

Comprendre les protocoles de communication d' View

Les composants View 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	Relie n'importe quel port TCP d'Horizon Client au port 4172 de l'application ou du poste de travail distant. PCoIP relie également le port UDP 50002 d'Horizon Client (ou le port UDP 55000 de PCoIP Secure Gateway) au port 4172 de l'application ou du poste de travail distant.
redirection USB	Port TCP 32111. Ce port est également utilisé pour la synchronisation de fuseau horaire.
VMware Blast Extreme	Relie n'importe quel port TCP ou UDP d'Horizon Client au port 22443 de l'application ou du poste de travail distant.
HTML Access	Pour HTML Access Gateway sur des Serveurs de connexion et des serveurs de sécurité, port TCP 8443 Pour les connexions de View Agent ou Horizon Agent, port TCP 22443

Règles de pare-feu pour Horizon Agent

Le programme d'installation d'Horizon Agent ouvre certains ports TCP sur le pare-feu. Les ports sont entrants sauf indication contraire.

Tableau 1-2. Ports TCP ouverts pendant l'installation de l'agent

Protocole	Ports
RDP	3389
redirection USB	32111 (Ce port est également utilisé pour la synchronisation de fuseau horaire.)
MMR (redirection multimédia) et CDR (redirection de lecteur client)	9427
PCoIP	4172 (TCP et UDP)
VMware Blast Extreme	22443 (TCP et UDP)
HTML Access	22443

Le programme d'installation de l'agent configure 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 modifiez le numéro du port RDP après l'installation, vous devez modifier les règles de pare-feu associées.

Si vous demandez au programme d'installation de l'agent de ne pas activer la prise en charge du Poste de travail à distance, il n'ouvre pas les ports 3389 et 32111 et vous devez ouvrir ces ports manuellement.

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.

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 View Server.

Lors de l'installation sur des clients Windows, des postes de travail distants et des hôtes RDS, le programme d'installation peut éventuellement configurer des règles de pare-feu Windows pour ouvrir les ports qui sont utilisés par défaut. 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 de View*.

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 View 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.

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

Source	Port	Cible	Port	Protocole	Description
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. **Remarque** Comme le port source varie, voir la note sous ce tableau.
Horizon Client	*	Horizon Agent	22443	TCP et UDP	VMware Blast Extreme si des connexions directes sont utilisées à la place de connexions par tunnel.
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 View ou dispositif Access Point	*	View Agent/Horizon Agent	3389	TCP	Trafic Microsoft RDP vers des postes de travail View quand des connexions par tunnel sont utilisées.
Serveur de sécurité, Serveur de connexion View ou dispositif Access Point	*	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 View ou dispositif Access Point	*	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 View ou dispositif Access Point	55000	View Agent/Horizon Agent	4172	UDP	PCoIP (pas SALSA20) si PCoIP Secure Gateway est utilisé.
Serveur de sécurité, Serveur de connexion View ou dispositif Access Point	*	View Agent/Horizon Agent	4172	TCP	PCoIP, si PCoIP Secure Gateway est utilisé.
Serveur de sécurité, Serveur de connexion View ou dispositif Access Point	*	Horizon Agent	22443	TCP	VMware Blast Extreme si Blast Secure Gateway est utilisé.
Serveur de sécurité, Serveur de connexion View ou dispositif Access Point	*	View Agent/Horizon Agent	22443	TCP	HTML Access si Blast Secure Gateway est utilisé.
View Agent/Horizon Agent	*	Serveur de connexion View	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. **Remarque** Comme le port cible varie, voir la note sous ce tableau.
View Agent/Horizon Agent	4172	Serveur de connexion View, serveur de sécurité ou dispositif Access Point	55000	UDP	PCoIP (pas SALSA20) si PCoIP Secure Gateway est utilisé.

Remarque 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 View, serveur de sécurité ou dispositif Access Point	443	TCP	HTTPS pour la connexion à View. (Ce port est également utilisé pour le tunnelling quand des connexions par tunnel sont utilisées.)
Horizon Client	*	View Agent/Horizon Agent	3389	TCP	Trafic Microsoft RDP vers des postes de travail View 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.
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. **Remarque** Comme le port source varie, voir la note sous ce tableau.
Horizon Client	*	Serveur de connexion View, serveur de sécurité ou dispositif Access Point	4172	TCP et UDP	PCoIP (pas SALSA20) si PCoIP Secure Gateway est utilisé. **Remarque** Comme le port source varie, voir la note sous ce tableau.

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

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

Remarque Le numéro de port UDP que les clients utilisent pour le protocole PCoIP est susceptible de changer. Si le port 50002 est utilisé, le client choisira 50003. Si le port 50003 est utilisé, le client choisira 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 aborde les rubriques suivantes :

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.
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.

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 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 d'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 fonction de redirection de scanner.
VMware Serial Com Client Service	Automatique	(Horizon Client 3.4 et versions ultérieures) Fournit des services pour la fonction 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	Fournit des services pour la fonction de redirection USB.

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	■ `vmware-usbarbitrator`, 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. ■ `vmware-view-used`, qui fournit des services pour la fonctionnalité de redirection USB. **Remarque** 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.
Client Mac	Horizon Client ne crée aucun démon.
Client Chrome	Horizon Client s'exécute dans un processus Android unique. Horizon Client ne crée aucun démon.
Client iOS	Horizon Client ne crée aucun démon.

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

Type	Service, processus ou démon
Client Android	Horizon Client s'exécute dans un processus Android unique. Horizon Client ne crée aucun démon.
Client Windows Store	Horizon Client ne crée ou ne déclenche aucun service système.
Poste de travail Linux	■ `StandaloneAgent`, qui s'exécute avec des privilèges root et est démarré lorsque le système Linux est activé et exécuté. `StandaloneAgent` communique avec le Serveur de connexion View 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 View). ■ `VMwareBlastServer`, qui est démarré par `StandaloneAgent` lorsqu'une demande `StartSession` est reçue de la part du Serveur de connexion View. Le démon `VMwareBlastServer` s'exécute avec le privilège `vmwblast` (un compte système créé lors de l'installation de l'agent Linux.) . Il communique avec `StandaloneAgent` via un canal `MKSControl` interne et communique avec Horizon Client à l'aide du protocole Blast.

Ressources à sécuriser 3

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

Ce chapitre aborde les rubriques suivantes :

Implémentation de meilleures pratiques pour sécuriser des systèmes client

Il vous est recommandé d'implémenter des 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	Lorsqu'Horizon Client démarre, des paramètres de configuration sont traités depuis plusieurs emplacements dans l'ordre suivant : 1 `/etc/vmware/view-default-config` 2 `~/.vmware/view-preferences` 3 `/etc/vmware/view-mandatory-config` 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).
Client Windows	Les paramètres d'utilisateur pouvant inclure des informations privées se trouvent dans le fichier suivant : `C:\Users\`*`user-name`*`\AppData\Roaming\VMware\VMware Horizon View Client\prefs.txt`

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

Type	Chemin du répertoire
Client Mac	Certains fichiers de configuration générés après le démarrage du client Mac. ■ `$HOME/Library/Preferences/com.vmware.horizon.plist` ■ `$HOME/Library/Preferences/com.vmware.vmrc.plist` ■ `$HOME/Library/Preferences/com.vmware.horizon.keyboard.plist` ■ `/Library/Preferences/com.vmware.horizon.plist`
Client Chrome	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.
Client iOS	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.
Client Android	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.
Client Windows Store	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.
View Agent ou Horizon Agent (poste de travail distant avec système d'exploitation Windows)	Les paramètres relatifs à la sécurité apparaissent uniquement dans le registre Windows.
Poste de travail Linux	Vous pouvez utiliser un éditeur de texte pour ouvrir le fichier de configuration suivant et pour spécifier les paramètres SSL. `/etc/vmware/viewagent-custom.conf`

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 View. Si un administrateur View doit vérifier l'expérience utilisateur, créez et autorisez un compte test séparé. Sur le poste de travail, les utilisateurs finaux View ne doivent pas être des membres de groupes privilégiés, tels que des administrateurs, car ils pourraient ensuite 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 OS X, lors du premier démarrage, l'utilisateur doit accorder un accès Administrateur local pour démarrer les services USB et 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 », page 41. 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 », page 33.

Ce chapitre aborde les rubriques suivantes :

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 les serveurs View 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 *Utilisation de VMware Horizon Client* pour le type de client spécifique. Les documents sont disponibles sur la page de documentation d'Horizon Client à l'adresse https://www.vmware.com/support/viewclients/doc/viewclients_pubs-archive.html. Ces documents contiennent également des informations sur l'utilisation des certificats auto-signés.

Paramètres liés à la sécurité dans le modèle de configuration de View Agent ou Horizon Agent

Les paramètres liés à la sécurité sont fournis dans le fichier de modèle ADM pour View Agent ou Horizon Agent(`vdm_agent.adm`). 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`	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 View via Horizon Client. Lorsque vous vous connectez à un poste de travail distant à partir d' Horizon Client pour Mac OS X, ne désactivez pas le paramètre `AllowDirectRDP`. Si ce paramètre est désactivé, la connexion échoue avec une erreur `Access is denied (Accès refusé)`. Par défaut, lorsqu'un utilisateur a ouvert une session de poste de travail View, vous pouvez utiliser RDP pour vous connecter à la machine virtuelle à l'extérieur de View. La connexion RDP met fin à la session du poste de travail View et les données et paramètres non enregistrés de l'utilisateur View risquent d'être perdus. L'utilisateur View 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`. **IMPORTANT** Pour que View fonctionne correctement, 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. Ce paramètre est activé par défaut. La valeur de Registre Windows équivalente est `AllowDirectRDP`.
`AllowSingleSignon`	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. Ce paramètre est activé par défaut. La valeur de Registre Windows équivalente est `AllowSingleSignon`.
`CommandsToRunOnConnect`	Spécifie une liste de commandes ou de scripts de commande à exécuter lorsqu'une session est connectée pour la première fois. Aucune liste n'est spécifiée par défaut. La valeur de Registre Windows équivalente est `CommandsToRunOnConnect`.
`CommandsToRunOnDisconnect`	Spécifie la liste des commandes ou des scripts de commande à exécuter lorsqu'une session est déconnectée. Aucune liste n'est spécifiée par défaut. La valeur de Registre Windows équivalente est `CommandsToRunOnReconnect`.
`CommandsToRunOnReconnect`	Spécifie une liste de commandes ou de scripts de commande à exécuter lorsqu'une session est reconnectée après une déconnexion. Aucune liste n'est spécifiée par défaut. La valeur de Registre Windows équivalente est `CommandsToRunOnDisconnect`.

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`	Spécifie la durée en secondes pendant laquelle le ticket de connexion View est valide. 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. La valeur de Registre Windows équivalente est `VdmConnectionTicketTimeout`.
`CredentialFilterExceptions`	Spécifie les fichiers exécutables qui ne sont pas autorisés à charger l'agent CredentialFilter. 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. Aucune liste n'est spécifiée par défaut. La valeur de Registre Windows équivalente est `CredentialFilterExceptions`.

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`.

Au cours de l'installation de View Agent ou d'Horizon Agent, le programme d'installation copie deux fichiers de modèle de configuration, `template_config` et `template_viewagent-custom.conf`, 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 `template-config` dans `config` et `template_viewagent-custom.conf` 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.

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`.

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

Option	Valeur	Valeur par défaut	Description
VVC.ScRedir.Enable	VRAI ou FAUX	VRAI	Définissez cette option pour 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.

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

Option	Valeur	Valeur par défaut	Description
Clipboard.Direction	0, 1, 2 ou 3	2	Cette option détermine la stratégie de redirection de Presse-papiers. ■ 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.
mksVNCServer.useXExtButtonMapping	VRAI ou FAUX	FAUX	Définissez cette option pour activer ou désactiver la prise en charge d'une souris pour gauchers sous SLED 11 SP3.

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
Sous-réseau	NULL ou adresse et masque de réseau au format d'adresse IP/CIDR	NULL	Utilisez cette option pour définir un sous-réseau avec lequel le Serveur de connexion View peut se connecter à la machine Agent s'il y a plusieurs adresses IP locales avec différents sous-réseaux. Vous devez spécifier la valeur au format d'adresse IP/CIDR. Par exemple, Sous-réseau=192.168.1.0/24. NULL implique que l'agent Linux sélectionne l'adresse IP de façon aléatoire.
SSOEnable	VRAI ou FAUX	VRAI	Définissez cette option pour désactiver l'authentification unique (SSO).
SSOUserFormat	Une chaîne de texte	[username]	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. Exemples de formats de nom de connexion : ■ SSOUserFormat=[domain]\\[username] ■ SSOUserFormat=[domain]+[username] ■ SSOUserFormat=[username]@[domain]
StartBlastServerTimeout	Un entier	20	Cette option détermine la durée, en secondes, allouée au processus VMwareBlastServer pour l'initialisation. Si le processus n'est pas prêt avant la fin de cette durée, la connexion de l'utilisateur échouera.
SSLCiphers	Une chaîne de texte	!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH	Utilisez cette option pour spécifier la liste de chiffrements. Vous devez utiliser le format défini dans https://www.openssl.org/docs/manmaster/apps/ciphers.html.
SSLProtocols	Une chaîne de texte	TLSv1_1:TLSv1_2	Utilisez cette option pour spécifier les protocoles de sécurité. Les protocoles pris en charge sont TLSv1.0, TLSv1.1 et TLSv1.2.

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

Option	Valeur	Valeur par défaut	Description
SSLCipherServerPreference	VRAI ou FAUX	VRAI	Utilisez cette option pour activer ou désactiver l'option SSL_OP_CIPHER_SERVER_PREFERENCE. Pour plus d'informations, reportez-vous à la section https://www.openssl.org/docs/manmaster/ssl/SSL_CTX_set_options.html.
LogoutAfterDisconnectTimeout	Un entier	2	Utilisez cette option pour définir la valeur de délai d'expiration en minutes pour `Automatically logoff after disconnect` si la connexion est en cours.
LogCnt	Un entier	-1	Utilisez cette option pour définir le nombre de fichiers journaux réservés dans `/tmp/vmware-root`. ■ -1 : tout conserver ■ 0 : tout supprimer ■ > 0 : nombre de journaux réservés.

Remarque 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

Des paramètres de stratégie de groupe pour HTML Access sont spécifiés dans le fichier de modèle `vdm_blast.adm`. Ce modèle est conçu pour le protocole d'affichage VMware Blast, qui est le seul utilisé par HTML Access.

Pour HTML Access 4.0 et Horizon 7.0, les paramètres de stratégie de groupe VMware Blast sont décrits dans la rubrique « Paramètres de stratégie de groupe VMware Blast » dans le document *Configuration de pools de postes de travail et d'applications dans View*.

Si vous disposez de HTML Access 3.5 ou version antérieure et d'Horizon 6.2.x ou version antérieure, le tableau suivant décrit des paramètres de stratégie de groupe qui s'appliquent à HTML Access. Notez qu'à partir d'Horizon 7.0, davantage de paramètres de stratégie de groupe VMware Blast sont disponibles.

Tableau 4-4. Paramètres de stratégie de groupe pour HTML Access 3.5 et versions antérieures

Paramètre	Description
Effacement d'écran	Permet de contrôler si la machine virtuelle distante peut être vue à l'extérieur d'View 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. Lorsque ce paramètre est activé ou non configuré, et quelqu'un tente d'accéder à la machine virtuelle distante de l'extérieur d'View pendant qu'une session HTML Access est active, la machine virtuelle distante affiche un écran vide.
Nettoyage de la mémoire de session	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. L'intervalle détermine la fréquence d'exécution du nettoyage de la mémoire. L'intervalle est défini en millisecondes. 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.

Tableau 4-4. Paramètres de stratégie de groupe pour HTML Access 3.5 et versions antérieures (suite)

Paramètre	Description
Configurer la redirection du Presse-papiers	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 : ■ **Activé du client vers le serveur seulement** (C'està-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.) Ce paramètre s'applique uniquement à View Agent ou Horizon Agent. Lorsque ce paramètre est désactivé ou n'est pas configuré, la valeur par défaut est **Activé du client vers le serveur seulement**.
Service HTTPS	Permet de changer le port TCP sécurisé (HTTPS) pour Blast Agent service. Le port par défaut est 22443. 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).

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 du fichier de modèle d'administration (ADM) d'Horizon Client (`vdm_client.adm`). 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.

Les paramètres de sécurité sont stockés dans le registre sur la machine hôte sous l'un des chemins d'accès suivants :

- Pour Windows 32 bits : `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`
- Pour Windows 64 bits : `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security`

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 de Serveur de connexion View qui acceptent l'identité et les informations d'identification d'utilisateur qui sont transmises quand un utilisateur coche la case **Log in as current user (Se connecter en tant qu'utilisateur actuel)**. Si vous ne spécifiez aucune instance de Serveur de connexion View, toutes les instances de Serveur de connexion View acceptent ces informations. Pour ajouter une instance de Serveur de connexion View, utilisez l'un des formats suivants : ■ **`domain\system$`** ■ **`system$@domain.com`** ■ Nom principal de service (SPN) du service Serveur de connexion View. La valeur de Registre Windows équivalente est `BrokersTrustedForDelegation`.

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

Paramètre	Description

`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 :
	■ `No Security`. View n'effectue pas la vérification de certificat.
	■ `Warn But Allow`. Lorsque les problèmes de certificat de serveur suivants se produisent, un avertissement s'affiche, mais l'utilisateur peut continuer à se connecter au Serveur de connexion View :
	  ■ Un certificat auto-signé est fourni par View. Dans ce cas, cela est acceptable si le nom de certificat ne correspond pas au nom du Serveur de connexion View fourni par l'utilisateur dans Horizon Client.
	  ■ Un certificat vérifiable qui a été configuré dans votre déploiement a expiré ou n'est pas encore valide.
	  Si une autre erreur de certificat se produit, View affiche une boîte de dialogue d'erreur et empêche l'utilisateur de se connecter au Serveur de connexion View.
	  `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 View. View affiche les erreurs de certificat à l'utilisateur.
	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.
	Lorsque ce paramètre n'est pas configuré ou est désactivé, les utilisateurs d'Horizon Client peuvent sélectionner un mode de vérification de certificat.
	Pour les clients Windows, si vous ne voulez pas configurer ce paramètre en tant que stratégie de groupe, vous pouvez également activer la vérification de certificat en ajoutant le nom de valeur `CertCheckMode` à l'une des clés de Registre suivantes sur l'ordinateur client :
	■ Pour Windows 32 bits : `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`
	■ Pour Windows 64 bits : `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security`
	Utilisez les valeurs suivantes dans la clé de registre :
	■ **`0`** implémente `No Security`.
	■ **`1`** implémente `Warn But Allow`.
	■ **`2`** implémente `Full Security`.
	Si vous configurez le paramètre de stratégie de groupe et le paramètre `CertCheckMode` dans la clé de Registre Windows, le paramètre de stratégie de groupe est prioritaire sur la valeur de la clé de registre.

`Default value of the 'Log in as current user' checkbox` (Paramètre de Configuration d'utilisateur et d'ordinateur)	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. Ce paramètre remplace la valeur par défaut spécifiée au cours de l'installation d'Horizon Client. Si un utilisateur exécute Horizon Client à partir de la ligne de commande et spécifie l'option `logInAsCurrentUser`, cette valeur remplace ce paramètre. 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 View, 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. Ce paramètre est désactivé par défaut. La valeur de Registre Windows équivalente est `LogInAsCurrentUser`.

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

Paramètre	Description
`Display option to Log in as current user` (Paramètre de Configuration d'utilisateur et d'ordinateur)	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. 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. 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 `Default value of the 'Log in as current user' checkbox`. Ce paramètre est activé par défaut. La valeur de Registre Windows équivalente est `LogInAsCurrentUser_Display`.
`Enable jump list integration` (Paramètre de Configuration d'ordinateur)	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 des raccourcis permet aux utilisateurs de se connecter à des instances récentes du Serveur de connexion View et à des postes de travail récemment utilisés. 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. Ce paramètre est activé par défaut. La valeur de Registre Windows équivalente est `EnableJumplist`.
`Enable SSL encrypted framework channel` (Paramètre de Configuration d'utilisateur et d'ordinateur)	Détermine si SSL doit être activé pour les postes de travail View 5.0 et versions antérieures. Avant View 5.0, les données envoyées au poste de travail via le port TCP 32111 n'étaient pas chiffrées. ■ **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. Par exemple, les postes de travail View 5.0 et versions antérieures ne prennent pas en charge SSL. **Activer** est le paramètre par défaut. ■ **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. La valeur de Registre Windows équivalente est `EnableTicketSSLAuth`.

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)	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. **Remarque** Toutes les chaînes de chiffrement sont sensibles à la casse. ■ Si cette fonction est activée, 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**. Cela signifie que 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.) 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.) Dans Horizon Client 3.2 et versions antérieures, SSL v3.0 est également activé. (SSL v2.0 et TLS v1.2 sont désactivés.) 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. Lien de référence pour la configuration : http://www.openssl.org/docs/apps/ciphers.html . La valeur de Registre Windows équivalente est `SSLCipherList`.
`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 View. Lorsque l'authentification unique est désactivée, Horizon Client n'affiche pas de boîte de dialogue de code PIN personnalisé. La valeur de Registre Windows équivalente est `EnableSmartCardSSO`.
`Ignore bad SSL certificate date received from the server` (Paramètre de Configuration d'ordinateur)	(View 4.6 et versions antérieures uniquement) Détermine si les erreurs associées aux dates des certificats de serveur non valides doivent être ignorées. Ces erreurs se produisent quand un serveur envoie un certificat avec une date passée. La valeur de Registre Windows équivalente est `IgnoreCertDateInvalid`.
`Ignore certificate revocation problems` (Paramètre de Configuration d'ordinateur)	(View 4.6 et versions antérieures uniquement) Détermine si les erreurs associées à un certificat de serveur révoqué doivent être ignorées. Ces erreurs se produisent lorsque le serveur envoie un certificat qui a été révoqué et lorsque le client ne peut pas vérifier l'état de révocation d'un certificat. Ce paramètre est désactivé par défaut. La valeur de Registre Windows équivalente est `IgnoreRevocation`.
`Ignore incorrect SSL certificate common name (host name field)` (Paramètre de Configuration d'ordinateur)	(View 4.6 et versions antérieures uniquement) Détermine si les erreurs associées aux noms communs de certificats de serveur incorrects doivent être ignorées. Ces erreurs se produisent quand le nom commun sur le certificat ne correspond pas au nom d'hôte du serveur qui l'envoie. La valeur de Registre Windows équivalente est `IgnoreCertCnInvalid`.

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

Paramètre	Description
`Ignore incorrect usage problems` (Paramètre de Configuration d'ordinateur)	(View 4.6 et versions antérieures uniquement) Détermine si les erreurs associées à une utilisation incorrecte d'un certificat de serveur doivent être ignorées. Ces erreurs se produisent lorsque le serveur envoie un certificat ayant un autre but que vérifier l'identité de l'expéditeur et crypter les communications du serveur. La valeur de Registre Windows équivalente est `IgnoreWrongUsage`.
`Ignore unknown certificate authority problems` (Paramètre de Configuration d'ordinateur)	(View 4.6 et versions antérieures uniquement) Détermine si les erreurs associées à une autorité de certification inconnue sur le certificat du serveur doivent être ignorées. Ces erreurs se produisent lorsque le serveur envoie un certificat signé par une autorité tierce non approuvée. La valeur de Registre Windows équivalente est `IgnoreUnknownCa`.

Les paramètres des définitions de script des périphériques USB sont stockés dans le registre sur la machine hôte sous l'un des chemins d'accès suivants :

- Pour Windows 32 bits : `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\USB`
- Pour Windows 64 bits : `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\USB`

Les paramètres des définitions de script pour le mot de passe sont stockés dans le registre sur la machine hôte sous `HKEY_CURRENT_USER\Software\VMware, Inc.\VMware VDM\Client\USB`.

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 `connectUSBOnStartup`.
`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 `connectUSBOnInsert`.
`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 matière de sécurité, consultez le document *Utilisation de VMware Horizon Client pour Windows*.

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 View Server.

Ce chapitre aborde les rubriques suivantes :

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 4.0 et 3.x sur des systèmes clients Windows, Linux, Mac OS X, iOS, Android et Chrome. Dans Horizon Client 3.1 (et versions ultérieures) pour Windows, Linux et Mac OS X, 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 4.0

Tableau 5-1. 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	■ 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)
■ TLS 1.1	■ 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)

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

Horizon Client 3.5

Tableau 5-2. 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	■ 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)
■ TLS 1.1 ■ TLS 1.0	■ 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)

Horizon Client 3.3 et 3.4

Tableau 5-3. 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
■ TLS 1.1 ■ TLS 1.0	■ 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)

Remarque 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 5-2 sont prises en charge.

Horizon Client 3.0, 3.1 et 3.2

Tableau 5-4. 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
■ TLS 1.1 ■ TLS 1.0 ■ SSL 3.0 (activé sur les clients Windows uniquement)	■ 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)

Remarque 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 5-2 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. Pour plus d'informations, consultez le document *Utilisation d'Horizon Client pour Windows*.
- Sur les systèmes clients Linux, vous pouvez utiliser des propriétés de fichier de configuration ou des options de ligne de commande. Pour plus d'informations, consultez le document *Utilisation d'Horizon Client pour Linux*.
- Sur les systèmes clients Mac OS X, vous pouvez utiliser un paramètre Préférence dans Horizon Client. Pour plus d'informations, consultez le document *Utilisation d'Horizon Client pour Mac OS X*.
- Sur les systèmes clients iOS, Android et Chrome, vous pouvez utiliser un paramètre Options SSL avancées dans les paramètres d'Horizon Client. Pour plus d'informations, consultez le document applicable : *Utilisation d'Horizon Client pour iOS*, *Utilisation d'Horizon Client pour Android* ou *Utilisation d'Horizon Client pour Chrome*.

Les documents sont disponibles sur la page de documentation d'Horizon Client à l'adresse https://www.vmware.com/support/viewclients/doc/viewclients_pubs-archive.html.

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 http://openssl.org/docs/manmaster/apps/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 View

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

Assurez-vous que le Serveur de connexion View 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 View.

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 aborde les rubriques suivantes :

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` **Remarque** Vous pouvez utiliser un GPO pour configurer le niveau de journalisation, entre 0 et 3 (le plus détaillé). Utilisez le fichier de modèle ADM des variables de session de client View PCoIP (`pcoip.adm`). Le paramètre s'appelle **Configurer le niveau de détails du journal des événements PCoIP**.

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

Type de journaux	Chemin du répertoire	Nom de fichier
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` **Remarque** Vous pouvez utiliser un GPO pour configurer l'emplacement du journal. Utilisez le fichier de modèle ADM de configuration commune de View (`vdm_common.adm`).
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-vdpServiceClient-XXXXXX.log`
Service WSNM Du processus `wsnm.exe`	`C:\ProgramData\VMware\VDM\logs`	`debug-yyyy-mm-dd-XXXXXX.txt` **Remarque** Vous pouvez utiliser un GPO pour configurer l'emplacement du journal. Utilisez le fichier de modèle ADM de configuration commune de View (`vdm_common.adm`).
redirection USB Du processus `vmware-view-usbd.exe`	`C:\ProgramData\VMware\VDM\logs`	`debug-yyyy-mm-dd-XXXXXX.txt` **Remarque** Vous pouvez utiliser un GPO pour configurer l'emplacement du journal. Utilisez le fichier de modèle ADM de configuration commune de View (`vdm_common.adm`).
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 ADM des variables de session de client View PCoIP (`pcoip.adm`). 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 ADM de configuration commune de View (`vdm_common.adm`).
- 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 ADM de configuration commune de View (`vdm_common.adm`).
- 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 ADM de configuration commune de View (`vdm_common.adm`).

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 OS X

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 OS X

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	`/tmp/vmware-root/`	`.vmware-installer-pid.log` `vmware-vmis-pid.log`
Interface utilisateur d'Horizon Client	`/tmp/vmware-`*`username`*`/`	`vmware-horizon-client-pid.log`
Client PCoIP	`/tmp/teradici-`*`username`*`/`	`pcoip_client_`*`YYYY_MM_DD_XXXXXX`*`.log`
Audio/Vidéo en temps réel	`/tmp/vmware-`*`username`*`/`	`vmware-RTAV-pid.log`
redirection USB	`/tmp/vmware-root/`	`vmware-usbarb-pid.log` `vmware-view-usbd-pid.log`
VChan	`/tmp/vmware-`*`username`*`/`	`VChan-Client.log` **Remarque** Ce journal est créé lorsque vous activez les journaux RDPVCBridge en définissant « `export VMW_RDPVC_BRIDGE_LOG_ENABLED=1` ».

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 suivant : `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

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

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 suivant : `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 du client et en utilisant 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 View Agent ou 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`
		Remarque Vous pouvez utiliser un GPO pour configurer l'emplacement du journal. Utilisez le fichier de modèle ADM de configuration commune de View (`vdm_common.adm`).

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 ADM de configuration commune de View (`vdm_common.adm`).
- 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 de View*.

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	`/tmp/vmware-root`
View Agent (pour Horizon 6) ou Horizon Agent (pour Horizon 7)	`/var/log/vmware`
View Agent (pour Horizon 6) ou Horizon Agent (pour Horizon 7)	`/usr/lib/vmware/viewagent/viewagent-debug.log`

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 View suivants : View Composer, Serveur de connexion View, View Agent ou Horizon Agent et divers clients. Les composants de correctif que vous devez appliquer dépendent des correctifs de bogue dont votre déploiement d'View a besoin.

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

1 View Composer

2 Serveur de connexion View

3 View Agent (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 de View*.

Ce chapitre aborde les rubriques suivantes :

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.

Prérequis

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

Procédure

1 Sur 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.

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

   Remarque Avec Horizon 6 version 6.2 et ultérieures, il n'est plus nécessaire de 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'instructions 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.

   Remarque Avec Horizon Client pour Windows 3.5 et versions ultérieures, il n'est plus nécessaire de désinstaller la version précédente avant d'installer le correctif sur les clients Windows.

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.

Index

V