Sécurité d'Horizon

VMware Horizon 2111

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

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

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

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

Table des matières

Sécurité de VMware Horizon

Sécurité d'Horizon fournit une référence succincte aux fonctionnalités de sécurité de VMware Horizon.

- Comptes de connexion requis au système et à la base de données.
- 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.
- Interfaces, ports et services externes qui doivent être ouverts ou activés pour le bon fonctionnement de VMware Horizon.

Public cible

Ces informations sont destinées aux décideurs, aux architectes, aux administrateurs informatiques et aux autres personnes qui doivent se familiariser avec les composants de sécurité de VMware Horizon.

Comptes, ressources et fichiers journaux d'VMware Horizon

1

Le fait de posséder des comptes différents pour des composants spécifiques permet de ne pas donner aux utilisateurs un accès et des autorisations dont ils n'ont pas besoin. Connaître l'emplacement des fichiers de configuration et des fichiers avec des données sensibles permet de configurer la sécurité pour divers systèmes hôtes.

Ce chapitre contient les rubriques suivantes :

Comptes VMware Horizon

Vous devez configurer des comptes système et des comptes de base de données pour administrer les composants de VMware Horizon.

Tableau 1-1. Comptes système VMware Horizon

Composant Horizon	Comptes requis
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, mais les comptes ne requièrent pas de privilèges d'administrateur Horizon.
vCenter Server	Configurez dans Active Directory un compte d'utilisateur autorisé à effectuer dans vCenter Server les opérations nécessaires à la prise en charge de VMware Horizon. Pour plus d'informations sur les privilèges requis, consultez le document *Installation d'Horizon*.
Serveur de connexion	Lorsque vous installez VMware Horizon, vous pouvez spécifier un utilisateur de domaine spécifique, le groupe d'administrateurs local ou un groupe d'utilisateurs de domaine spécifique en tant qu'administrateurs Horizon. Nous vous recommandons de créer un groupe d'utilisateurs de domaine dédié d'administrateurs Horizon. L'utilisateur par défaut est l'utilisateur de domaine actuellement connecté. Dans Horizon Console, vous pouvez utiliser **Paramètres > Administrateurs** pour modifier la liste des administrateurs Horizon. Pour plus d'informations sur les privilèges requis, consultez le document *Administration d'Horizon*.

Tableau 1-2. Comptes de base de données Horizon

Composant Horizon	Comptes requis
Base de données des événements utilisée par l'Horizon Connection Server	Une base de données Microsoft SQL Server, Oracle ou PostgreSQL stocke des données d'événement Horizon. Vous pouvez créer un compte d'administration pour la base de données qu'Horizon Console peut utiliser afin d'accéder aux données d'événements.

Pour réduire le risque de vulnérabilités de sécurité, effectuez les actions suivantes :

- Configurez les bases de données VMware Horizon sur des serveurs distincts des autres serveurs de base de données que votre entreprise utilise.
- Ne permettez pas à un compte d'utilisateur d'accéder à plusieurs bases de données.
- Configurez un compte distinct pour l'accès à la base de données des événements.

Ressources d'VMware Horizon

VMware Horizon inclut plusieurs fichiers de configuration et des ressources similaires qui doivent être protégés.

Tableau 1-3. Ressources du Serveur de connexion Horizon

Resource (Ressource)	Emplacement	Protection
Paramètres LDAP	Non applicable.	Les données LDAP sont protégées automatiquement dans le cadre du contrôle d'accès basé sur des rôles.
Fichiers de sauvegarde LDAP	`%ProgramData%\VMWare\VDM\backups`	Protégé par un contrôle d'accès.
`locked.properties` (fichier de configuration de Secure Gateway)	*`install_directory`*`\VMware\VMware View\Server\sslgateway\conf`	Assurez-vous que ce fichier est protégé contre l'accès par des utilisateurs qui ne sont pas des administrateurs Horizon.
`absg.properties` (fichier de configuration de Blast Secure Gateway)	*`install_directory`*`\VMware\VMware View\Server\appblastgateway`	Assurez-vous que ce fichier est protégé contre l'accès par des utilisateurs qui ne sont pas des administrateurs Horizon.
Fichiers journaux	Reportez-vous à la section Fichiers journaux d'VMware Horizon.	Protégé par un contrôle d'accès.
`web.xml` (Fichier de configuration Tomcat)	*`install_directory`*`\VMware View\Server\broker\web apps\ROOT\Web INF`	Protégé par un contrôle d'accès.

Fichiers journaux d'VMware Horizon

VMware Horizon crée des fichiers journaux qui enregistrent l'installation et le fonctionnement de ses composants.

Note Les fichiers journaux d'VMware Horizon sont destinés à être utilisés par le support VMware. VMware vous recommande de configurer et d'utiliser la base de données des événements pour contrôler VMware Horizon. Pour plus d'informations, consultez les documents *Installation d'Horizon* et *Administration d'Horizon*.

Tableau 1-4. Fichiers journaux d'VMware Horizon

Composant Horizon	Chemin d'accès au fichier et autres informations
Tous les composants (journaux d'installation)	*%TEMP%*\vminst.log_*date_timestamp* *%TEMP%*\vmmsi.log_*date_timestamp*
Horizon Agent	*<Drive Letter>*:\ProgramData\VMware\VDM\logs Pour accéder aux fichiers journaux d'VMware Horizon stockés dans *<Lettre de lecteur>*:\ProgramData\VMware\VDM\logs, vous devez ouvrir les journaux à partir d'un programme disposant de privilèges administrateur élevés. Cliquez avec le bouton droit sur le fichier du programme et sélectionnez **Exécuter en tant qu'administrateur**. Si un disque de données utilisateur (User Data Disk, UDD) est configuré, *<Drive Letter* peut correspondre à l'UDD. Les journaux pour PCoIP sont nommés pcoip_agent*.log et pcoip_server*.log.
Fonctionnalités de poste de travail distant	Vous pouvez définir des niveaux de journal et générer des fichiers journaux dans un bundle DCT (Data collection Tool) pour les fonctionnalités de poste de travail distant sur l'agent et le client Windows, le client Mac et le client Linux. Agent Windows : C:\Program Files\VMware\VMware View\Agent\DCT\support.bat Client Windows : C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT\support.bat Client Mac : /Applications/VMware Horizon Client.app/Contents/Library/dct/HorizonCollector.sh Client Linux : /usr/bin/vmware-view-log-collector
Applications publiées	Base de données des événements Horizon configurée sur un serveur de base de données Microsoft SQL Server, Oracle ou PostgreSQL. Journaux d'événements d'application Windows. Désactivé par défaut.

Tableau 1-4. Fichiers journaux d'VMware Horizon (suite)

Composant Horizon	Chemin d'accès au fichier et autres informations
Serveur de connexion	*<Lettre de lecteur>*:\ProgramData\VMware\log\ConnectionServer. **Note** Ce chemin d'accès au fichier est un lien symbolique qui redirige vers l'emplacement réel des fichiers journaux, à savoir *<Lettre de lecteur>*:\ProgramData\VMware\VDM\logs. Le répertoire des journaux est configurable dans les paramètres de configuration de journal du fichier de modèle d'administration ADMX pour la configuration commune (vdm_common.admx). Les journaux PCoIP Secure Gateway sont rédigés dans des fichiers nommés SecurityGateway_*.log dans le sous-répertoire PCoIP Secure Gateway. Les journaux Blast Secure Gateway sont rédigés dans des fichiers nommés absg*.log dans le sous-répertoire Blast Secure Gateway.
Services Horizon	Base de données des événements Horizon configurée sur un serveur de base de données Microsoft SQL Server, Oracle ou PostgreSQL. Journaux d'événements de système Windows.

Paramètres de sécurité de VMware Horizon

2

VMware Horizon inclut plusieurs paramètres que vous pouvez utiliser pour régler la sécurité de la configuration. Vous pouvez accéder aux paramètres en utilisant Horizon Console ou l'utilitaire ADSI Edit, si nécessaire.

Note Pour plus d'informations sur les paramètres de sécurité pour Horizon Client et Horizon Agent, consultez le document *Sécurité d'Horizon Client et d'Horizon Agent*.

Ce chapitre contient les rubriques suivantes :

Paramètres généraux liés à la sécurité dans Horizon Console

Vous pouvez accéder aux paramètres globaux liés à la sécurité pour les sessions et les connexions clientes sous **Paramètres > Paramètres globaux > Paramètres de sécurité** ou sous **Paramètres > Paramètres globaux > Paramètres généraux** dans Horizon Console.

Tableau 2-1. Paramètres généraux liés à la sécurité

Paramètre	Description
Modifier le mot de passe de récupération de données	Le mot de passe est requis lorsque vous restaurez la configuration d'Horizon LDAP à partir d'une sauvegarde chiffrée. Lorsque vous installez le Serveur de connexion, fournissez un mot de passe de récupération de données. Après l'installation, vous pouvez modifier ce mot de passe dans Horizon Console. Lorsque vous sauvegardez le Serveur de connexion, la configuration d'Horizon LDAP est exportée sous forme de données LDIF chiffrées. Pour restaurer la sauvegarde cryptée avec l'utilitaire `vdmimport`, vous devez fournir le mot de passe de récupération de données. Le mot de passe doit contenir entre 1 et 128 caractères. Suivez les meilleures pratiques de votre entreprise concernant la génération de mots de passe sécurisés.
Mode de sécurité des messages	Détermine le mécanisme de sécurité utilisé lorsque des messages JMS sont transmis entre composants VMware Horizon. ■ Si le paramètre est réglé sur **Désactivé**, le mode de sécurité des messages est désactivé. ■ S'il est défini sur **Activé**, la signature des messages hérités et la vérification des messages JMS sont effectuées. Les composants VMware Horizon rejettent les messages non signés. Ce mode prend en charge une combinaison de connexions TLS et JMS en texte brut. ■ S'il est défini sur **Amélioré**, TLS est utilisé pour toutes les connexions JMS, pour chiffrer tous les messages. Le contrôle d'accès est également activé pour restreindre les rubriques JMS avec lesquelles les composants VMware Horizon peuvent échanger des messages. ■ Si le paramètre est défini sur **Mélangé**, le mode de sécurité des messages est activé, mais pas appliqué pour les composants de VMware Horizon. Le paramètre par défaut est **Amélioré** pour les nouvelles installations. Si vous procédez à une mise à niveau à partir d'une version précédente, le paramètre utilisé dans la version précédente est conservé. **Important** VMware recommande vivement de définir le mode de sécurité des messages sur **Amélioré** après la mise à niveau de toutes les instances du Serveur de connexion et des postes de travail VMware Horizon vers cette version. Le réglage **Amélioré** apporte de nombreuses améliorations importantes à la sécurité et des mises à jour à la file d'attente des messages (MQ).
État de sécurité amélioré (lecture seule)	Champ en lecture seule qui s'affiche lorsque **Mode de sécurité des messages** est modifié de **Activé** à **Amélioré**. Comme la modification est effectuée par phases, ce champ montre la progression de l'opération : ■ **En attente du redémarrage du bus de message** est la première phase. Cet état s'affiche jusqu'à ce que vous redémarriez manuellement toutes les instances du Serveur de connexion de l'espace ou le service Composant du bus de message VMware Horizon sur tous les hôtes de Serveur de connexion de l'espace. ■ **Amélioré en attente** est l'état suivant. Dès que tous les services Composant du bus de messages Horizon ont été redémarrés, le système commence à modifier le mode de sécurité des messages sur **Amélioré** pour tous les postes de travail. ■ **Amélioré** est l'état final, indiquant que tous les composants utilisent maintenant le mode de sécurité des messages **Amélioré**.

Tableau 2-1. Paramètres généraux liés à la sécurité (suite)

Paramètre	Description
Authentifier à nouveau les connexions par tunnel sécurisé après une interruption de réseau	Détermine si les informations d'identification nécessitent une nouvelle authentification après une interruption réseau lorsque des clients Horizon Client se connectent à des postes de travail et des applications VMware Horizon à l'aide d'un tunnel sécurisé. Ce paramètre offre une sécurité améliorée. Par exemple, si un ordinateur portable qui a été volé se connecte à un autre réseau, l'utilisateur ne peut pas accéder automatiquement aux postes de travail et aux applications VMware Horizon, car la connexion réseau a été temporairement interrompue. Ce paramètre est désactivé par défaut.
Forcer la déconnexion des utilisateurs	Déconnecte tous les postes de travail et toutes les applications après que le nombre de minutes spécifié s'est écoulé depuis que l'utilisateur s'est connecté à VMware Horizon. Tous les postes de travail et toutes les applications seront déconnectés en même temps, quel que soit le moment auquel l'utilisateur les a ouverts. La valeur par défaut est de 600 minutes.
Pour les clients prenant en charge les applications. **Si l'utilisateur cesse d'utiliser le clavier et la souris, déconnecter ses applications et supprimer les informations d'identification SSO**	Protège les sessions d'application en l'absence d'activité de clavier ou de souris sur le périphérique client. Si ce paramètre est défini sur **Après ... minutes**, VMware Horizon, View déconnecte toutes les applications et ignore les informations d'identification SSO au terme du nombre spécifié de minutes sans activité de l'utilisateur. Les sessions de postes de travail sont déconnectées. L'utilisateur doit ouvrir une nouvelle session pour se reconnecter aux applications déconnectées ou lancer un nouveau poste de travail ou une nouvelle application. Si ce paramètre est défini sur **Jamais**, VMware Horizon ne déconnecte jamais les applications et n'ignore jamais les informations d'identification SSO suite à l'inactivité de l'utilisateur. La valeur par défaut est **Jamais**.
Autres clients. **Supprimer les informations d'identification SSO**	Ignore les informations d'identification SSO au bout d'un certain temps. Ce paramètre concerne les clients qui ne prennent pas en charge l'accès à distance aux applications. Si ce paramètre est défini sur **Après ... minutes**, l'utilisateur doit ouvrir une nouvelle session pour se connecter à un poste de travail une fois que le nombre spécifié de minutes s'est écoulé depuis qu'il s'est connecté à VMware Horizon, quelle que soit son activité sur le périphérique client. La valeur par défaut est **Après 15 minutes**.
Délai d'expiration de la session de View Administrator	Détermine la durée pendant laquelle une session Horizon Console inactive continue avant d'expirer. **Important** Définir le délai d'expiration de la session Horizon Console sur un nombre de minutes élevé augmente le risque d'utilisation non autorisée de Horizon Console. Soyez prudent lorsque vous autorisez une session inactive à durer longtemps. Par défaut, le délai d'expiration de la session Horizon Console est de 30 minutes. Vous pouvez définir un délai d'expiration de session compris entre 1 et 4 320 minutes.

Note TLS est requis pour toutes les connexions d'Horizon Client et d'Horizon Console à VMware Horizon. Si votre déploiement de VMware Horizon utilise des équilibrages de charge ou d'autres serveurs intermédiaires orientés clients, vous pouvez décharger TLS sur ceux-ci et configurer des connexions non-TLS sur des instances individuelles du Serveur de connexion. Reportez-vous à la section « Décharger des connexions TLS sur des serveurs intermédiaires » dans le document *Administration d'Horizon*.

Modifier le mot de passe de récupération de données

Vous fournissez un mot de passe de récupération de données lorsque vous installez le Serveur de connexion. Après l'installation, vous pouvez modifier ce mot de passe dans Horizon Console. Le mot de passe est requis lorsque vous restaurez la configuration d'Horizon LDAP à partir d'une sauvegarde.

Lorsque vous sauvegardez le Serveur de connexion, la configuration d'Horizon LDAP est exportée sous forme de données LDIF chiffrées. Pour restaurer la configuration VMware Horizon de sauvegarde cryptée, vous devez fournir le mot de passe de récupération de données.

Le mot de passe doit contenir entre 1 et 128 caractères. Suivez les meilleures pratiques de votre entreprise concernant la génération de mots de passe sécurisés.

Procédure

1. Dans Horizon Console, sélectionnez **Paramètres > Paramètres généraux**.
2. Dans l'onglet **Paramètres de sécurité**, cliquez sur **Modifier le mot de passe de récupération des données**.
3. Tapez et retapez le nouveau mot de passe.
4. (Facultatif) Tapez un rappel de mot de passe.

Résultats

Note Vous pouvez également modifier le mot de passe de récupération de données lorsque vous planifiez la sauvegarde de vos données de configuration VMware Horizon. Reportez-vous à la section « Planifier des sauvegardes de la configuration d'Horizon » dans le document *Administration d'Horizon*.

Étape suivante

Lorsque vous employez l'utilitaire `vdmimport` pour restaurer une configuration VMware Horizon de sauvegarde, fournissez le nouveau mot de passe.

Mode de sécurité des messages pour les composants Horizon

Vous pouvez définir le mode de sécurité des messages pour spécifier le mécanisme de sécurité utilisé lorsque des messages JMS sont échangés entre des composants VMware Horizon.

Le tableau suivant affiche les options que vous pouvez sélectionner pour configurer le mode de sécurité des messages. Pour définir une option, sélectionnez-la dans la liste **Mode de sécurité des messages** dans l'onglet **Paramètres de sécurité** de la page **Paramètres généraux**.

Tableau 2-2. Options du mode de sécurité des messages

Option	Description
Désactivé	Le mode de sécurité des messages est désactivé.
Mélangé	Le mode de sécurité des messages est activé mais pas appliqué. Vous pouvez utiliser ce mode pour détecter d'anciens composants dans votre environnement VMware Horizon. Les fichiers journaux générés par le Serveur de connexion contiennent des références à ces composants. Ce paramètre n'est pas recommandé. Utilisez ce paramètre uniquement pour découvrir les composants devant être mis à niveau.
Activé	Le mode de sécurité des messages est activé, utilisation d'une combinaison de signature et de chiffrement des messages. Les messages JMS sont rejetés si la signature est manquante ou non valide, ou si un message a été modifié après avoir été signé. Certains messages JMS sont chiffrés, car ils comportent des informations sensibles telles que les informations d'identification de l'utilisateur. Si vous utilisez le paramètre **Activé**, vous pouvez également utiliser IPSec pour chiffrer tous les messages JMS entre les instances du Serveur de connexion, et entre les instances du Serveur de connexion et les dispositifs Unified Access Gateway.
Amélioré	SSL est utilisé pour toutes les connexions JMS. Le contrôle d'accès JMS est également activé afin que les postes de travail et les instances du Serveur de connexion puissent envoyer et recevoir uniquement des messages JMS sur certaines rubriques.

La première fois que vous installez VMware Horizon sur un système, le mode de sécurité des messages est défini sur **Activé**. Si vous effectuez la mise à niveau d'VMware Horizon à partir d'une version précédente, le mode de sécurité des messages reste le même.

Important Si vous prévoyez de modifier un environnement VMware Horizon mis à niveau depuis **Activé** vers **Amélioré**, vous devez d'abord mettre à niveau toutes les instances du Serveur de connexion et les postes de travail VMware Horizon. Dès que vous avez défini le paramètre sur **Amélioré**, le nouveau paramètre entre en vigueur par étapes.

1. Vous devez redémarrer manuellement le service Composant du bus de message VMware Horizon sur tous les hôtes du Serveur de connexion de l'espace ou redémarrer les instances du Serveur de connexion.
2. Dès que les services ont redémarré, les instances du Serveur de connexion reconfigurent le mode de sécurité des messages sur tous les postes de travail en passant ce mode à **Amélioré**.
3. Pour surveiller l'avancement dans Horizon Console, accédez à **Paramètres > Paramètres généraux**.

   Dans l'onglet **Paramètres de sécurité**, l'élément **État de sécurité amélioré** affiche **Amélioré** lorsque tous les composants sont passés au mode Amélioré.

   Sinon, vous pouvez employer l'utilitaire de ligne de commande `vdmutil` pour surveiller l'avancement. Reportez-vous à la rubrique Utilisation de l'utilitaire vdmutil pour configurer le mode de sécurité des messages JMS.

Si vous prévoyez de modifier un environnement VMware Horizon actif de **Désactivé** à **Activé**, ou de **Activé** à **Désactivé**, passez en mode **Mélangé** pendant une courte période avant de faire la modification finale. Par exemple, si votre mode actuel est **Désactivé**, passez en mode **Mélangé** pendant une journée, puis passez à **Activé**. En mode **Mélangé**, les signatures sont jointes aux messages mais ne sont pas vérifiées, ce qui permet de propager la modification du mode des messages dans l'environnement.

Utilisation de l'utilitaire vdmutil pour configurer le mode de sécurité des messages JMS

Vous pouvez utiliser l'interface de ligne de commande `vdmutil` pour configurer et gérer le mécanisme de sécurité utilisé lorsque des messages JMS sont transmis entre des composants VMware Horizon.

Syntaxe et emplacement de l'utilitaire

La commande `vdmutil` peut effectuer les mêmes opérations que la commande `lmvutil` qui était incluse avec les versions antérieures d'VMware Horizon. En outre, la commande `vdmutil` dispose d'options permettant de déterminer le mode de sécurité des messages utilisés et de surveiller l'avancement du passage de tous les composants VMware Horizon en mode Amélioré. Utilisez la forme suivante de la commande `vdmutil` à partir d'une invite de commande Windows.

```
vdmutil command_option [additional_option argument] ...
```

Les options supplémentaires que vous pouvez utiliser dépendent de l'option de commande. Cette rubrique met l'accent sur les options du mode de sécurité des messages. Pour les autres options, liées à Architecture Cloud Pod, reportez-vous au document *Administration d'Architecture Cloud Pod dans Horizon*.

Par défaut, le chemin d'accès au fichier exécutable de la commande `vdmutil` est `C:\Program Files\VMware\VMware View\Server\tools\bin`. Pour éviter d'entrer le chemin d'accès sur la ligne de commande, ajoutez-le à la variable d'environnement PATH.

Authentification

Vous devez exécuter la commande en tant qu'utilisateur disposant du rôle Administrateurs. Vous pouvez utiliser Horizon Console pour affecter le rôle Administrateurs à un utilisateur. Reportez-vous à la section « Configuration de l'administration déléguée basée sur des rôles » du document *Administration d'Horizon*.

La commande `vdmutil` inclut des options pour spécifier le nom d'utilisateur, le domaine et le mot de passe à utiliser pour l'authentification.

Tableau 2-3. options d'authentification de la commande vdmutil

Option	Description
`--authAs`	Nom d'un utilisateur administrateur Horizon. N'utilisez ni le format *domain**username* ni le format de nom principal d'utilisateur (UPN).
`--authDomain`	Nom de domaine complet de l'utilisateur administrateur Horizon spécifié dans l'option `--authAs`.
`--authPassword`	Mot de passe de l'utilisateur administrateur Horizon spécifié dans l'option `--authAs`. Si vous entrez « `*` » plutôt qu'un mot de passe, la commande `vdmutil` affiche une invite de mot de passe et ne conserve pas les mots de passe sensibles dans l'historique des commandes sur la ligne de commande.

Vous devez utiliser les options d'authentification avec toutes les options de la commande `vdmutil`, à l'exception de `--help` et de `--verbose`.

Options spécifiques aux modes de sécurité des messages JMS

Le tableau suivant répertorie uniquement les options de ligne de commande `vdmutil` qui concernent l'affichage, la configuration ou la surveillance du mode de sécurité des messages JMS. Pour consulter la liste des arguments que vous pouvez utiliser avec une option spécifique, utilisez l'option de ligne de commande `--help`.

La commande `vdmutil` renvoie 0 lorsqu'une opération réussit et un code différent de zéro spécifique d'un échec lorsqu'une opération échoue. La commande `vdmutil` écrit des messages d'erreur en format d'erreur standard. Lorsqu'une opération produit une sortie ou lorsque la journalisation détaillée est activée à l'aide de l'option `--verbose`, la commande `vdmutil` écrit la sortie en format de sortie standard, en anglais américain.

Tableau 2-4. Options de la commande vdmutil

Option	Description
`--activatePendingConnectionServerCertificates`	Active un certificat de sécurité en attente pour une instance du Serveur de connexion dans l'espace local.
`--countPendingMsgSecStatus`	Compte le nombre de machines empêchant une transition vers ou depuis le mode Amélioré.
`--createPendingConnectionServerCertificates`	Crée un certificat de sécurité en attente pour une instance du Serveur de connexion dans l'espace local.
`--getMsgSecLevel`	Obtient l'état de sécurité des messages amélioré pour l'espace local. Cet état concerne le processus de modification du mode de sécurité des messages JMS permettant de passer d'**Activé** à **Amélioré** pour tous les composants d'un environnement VMware Horizon.
`--getMsgSecMode`	Obtient le mode de sécurité des messages pour l'espace local.
`--help`	Répertorie les options de la commande `vdmutil`. Vous pouvez également utiliser `--help` sur une commande particulière, comme `--setMsgSecMode --help`.
`--listMsgBusSecStatus`	Répertorie l'état de sécurité du bus de message pour tous les serveurs de connexion de l'espace local.

Tableau 2-4. Options de la commande vdmutil (suite)

Option	Description
`--listPendingMsgSecStatus`	Répertorie les machines empêchant une transition vers ou depuis le mode Amélioré. Limité à 25 entrées par défaut.
`--setMsgSecMode`	Définit le mode de sécurité des messages de l'espace local.
`--verbose`	Active la journalisation détaillée. Vous pouvez ajouter cette option à n'importe quelle autre option pour obtenir une sortie de commande détaillée. La commande `vdmutil` écrit dans la sortie standard.

Paramètres de serveur liés à la sécurité dans Horizon Console

Les paramètres de serveur liés à la sécurité sont accessibles sous **Paramètres > Serveurs** dans Horizon Console.

Tableau 2-5. Paramètres de serveur liés à la sécurité

Paramètre	Description
Utiliser PCoIP Secure Gateway pour les connexions PCoIP à la machine	Détermine si Horizon Client établit une connexion plus sécurisée à l'hôte du Serveur de connexion lorsque des utilisateurs se connectent à des postes de travail et à des applications VMware Horizon avec le protocole d'affichage PCoIP. Si ce paramètre est désactivé, la session de poste de travail ou d'application est établie directement entre le client et le poste de travail VMware Horizon ou l'hôte des services Bureau à distance (RDS), contournant ainsi l'hôte du Serveur de connexion. Ce paramètre est désactivé par défaut.
Utiliser une connexion par tunnel sécurisé à la machine	Détermine si Horizon Client établit une autre connexion HTTPS à l'hôte du Serveur de connexion lorsque des utilisateurs se connectent à un poste de travail ou à une application VMware Horizon. Si ce paramètre est désactivé, la session de poste de travail ou d'application est établie directement entre le client et le poste de travail VMware Horizon ou l'hôte des services Bureau à distance (RDS), contournant ainsi l'hôte du Serveur de connexion. Ce paramètre est activé par défaut.
Utiliser Blast Secure Gateway pour les connexions Blast à la machine	Détermine si les clients qui accèdent à des postes de travail à l'aide d'un navigateur Web ou du protocole d'affichage Blast Extreme utilisent Blast Secure Gateway pour établir un tunnel sécurisé avec le Serveur de connexion. Si le paramètre n'est pas activé, les clients utilisant une session Blast Extreme et des navigateurs Web établissent des connexions directes aux postes de travail VMware Horizon, en contournant le Serveur de connexion. Ce paramètre est désactivé par défaut.

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

Paramètres liés à la sécurité dans Horizon LDAP

Les paramètres liés à la sécurité sont fournis dans Horizon LDAP sous le chemin d'accès d'objet `cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int`. Vous pouvez utiliser l'utilitaire Éditeur ADSI pour modifier la valeur de ces paramètres sur une instance du Serveur de connexion. La modification se propage automatiquement à toutes les autres instances du Serveur de connexion dans un groupe.

Tableau 2-6. Paramètres liés à la sécurité dans Horizon LDAP

Paire nom/valeur	Description
cs-allowunencryptedstartsession	L'attribut est `pae-NameValuePair`. Cet attribut contrôle si un canal sécurisé est requis entre une instance du Serveur de connexion et un poste de travail lorsqu'une session d'utilisateur distante est démarrée. Lorsque Horizon Agent est installé sur un ordinateur de poste de travail, cet attribut n'a aucun effet et un canal sécurisé est toujours requis. Dans tous les cas, les informations d'identification d'utilisateur et les tickets d'autorisation sont protégés par une clé statique. Un canal sécurisé fournit une garantie supplémentaire de confidentialité à l'aide de clés dynamiques. Si elle est définie sur **0**, une session d'utilisateur distante ne démarre pas si un canal sécurisé ne peut pas être établi. Ce paramètre est approprié si tous les postes de travail se trouvent dans des domaines approuvés ou si Horizon Agent est installé sur tous les postes de travail. Si elle est définie sur **1**, une session d'utilisateur distante peut être démarrée même si un canal sécurisé ne peut pas être établi. Ce paramètre est approprié si des agents Horizon Agent antérieurs sont installés sur certains postes de travail et s'ils se ne trouvent pas dans des domaines approuvés. Le paramètre par défaut est **1**.
keysize	L'attribut est `pae-MSGSecOptions`. Lorsque le mode de sécurité des messages est défini sur **Amélioré**, TLS est utilisé pour sécuriser les connexions JMS plutôt que d'utiliser un chiffrement par message. En mode de sécurité des messages amélioré, la validation s'applique à un seul type de message. Pour le mode des messages amélioré, VMware recommande d'augmenter la taille de la clé à 2 048 bits. Si vous n'utilisez pas le mode de sécurité des messages amélioré, VMware recommande de ne pas modifier la valeur par défaut de 512 bits, car l'augmentation de la taille de la clé affecte les performances et l'évolutivité. Si vous souhaitez que toutes les clés soient de 2 048 bits, la taille de clé DSA doit être modifiée immédiatement après l'installation de la première instance du Serveur de connexion et avant la création de serveurs et de postes de travail supplémentaires.

Renouveler automatiquement les certificats auto-signés

Vous pouvez renouveler automatiquement les certificats auto-signés avec l'attribut `pae-managedCertificateAdvanceRollOver`.

Spécifiez une valeur pour remplacer le certificat auto-signé par un certificat futur ou en attente dans le nombre de jours spécifié avant l'expiration du certificat actuel.

Par défaut. Cette valeur n'est pas définie. La plage valide est comprise entre 1 et 90.

Paramètres de serveur liés à la sécurité pour l'authentification utilisateur

Les paramètres de serveur liés à la sécurité pour l'authentification utilisateur sont accessibles sous **Paramètres > Paramètres généraux > Paramètres généraux** ou **Paramètres > Serveur** dans Horizon Console. Ces paramètres de sécurité déterminent comment Horizon Client peut se connecter au Serveur de connexion.

- Pour permettre à l'instance du Serveur de connexion d'accepter l'identité de l'utilisateur et les informations d'identification transmises lorsque les utilisateurs sélectionnent **Se connecter en tant qu'utilisateur actuel** dans le menu **Options** dans Horizon Client, activez le paramètre **Autoriser l'ouverture de session en tant qu'utilisateur actuel** pour l'instance du Serveur de connexion. Ce paramètre est disponible pour Horizon Client pour Windows. Pour plus d'informations, reportez-vous au document *Administration d'Horizon*.
- Pour masquer l'URL du serveur dans Horizon Client, activez le paramètre global **Masquer les informations de serveur dans l'interface utilisateur client**. Pour plus d'informations, reportez-vous à la section « Paramètres généraux pour les sessions client » dans le document *Administration d'Horizon*.
- Pour masquer le menu déroulant **Domaine** dans Horizon Client, activez le paramètre global **Masquer la liste de domaines dans l'interface utilisateur client**. Pour plus d'informations, reportez-vous à la section « Paramètres généraux pour les sessions client » dans le document *Administration d'Horizon*.
- Pour envoyer la liste de domaines à Horizon Client, activez-le paramètre global **Envoyer la liste de domaines** dans Horizon Console. Pour plus d'informations, reportez-vous à la section « Paramètres généraux pour les sessions client » dans le document *Administration d'Horizon*.

Note Tous les paramètres ne s'appliquent pas à tous les clients Horizon Client. Pour voir les paramètres d'authentification utilisateur d'un client Horizon Client particulier, consultez la documentation d'Horizon Client à l'adresse https://docs.vmware.com/fr/VMware-Horizon-Client/index.html.

Fourniture de détails du serveur

Pour que la fonctionnalité Se connecter en tant qu'utilisateur actuel fonctionne, VMware Horizon doit fournir le Nom du principal du serveur (identité Windows) du Serveur de connexion pour les clients qui se connectent avant l'authentification des utilisateurs.

Cette information est retirée par défaut, mais peut être fournie en activant le paramètre **Autoriser l'ouverture de session en tant qu'utilisateur actuel** dans Horizon Console. Ce choix est effectué individuellement pour chaque serveur. Si le paramètre n'est pas activé pour un serveur donné, les utilisateurs qui se connectent à ce serveur à partir d'Horizon Client pour Windows doivent entrer les informations d'identification, même s'ils ont activé le paramètre **Se connecter**

en tant qu'utilisateur actuel. Lorsque vous décidez d'activer ou non le paramètre **Autoriser l'ouverture de session en tant qu'utilisateur actuel** pour un serveur, déterminez si les clients qui se connectent se trouvent sur un réseau interne, donc un peu sous votre contrôle, ou sur un réseau externe, donc non contrôlés.

Le paramètre **Masquer les informations de serveur dans l'interface utilisateur client** affecte uniquement l'interface utilisateur du client. Il ne modifie pas les informations que le serveur fournit au client. Ce paramètre est désactivé par défaut.

Fourniture d'informations de domaine

La liste des domaines d'utilisateur disponibles peut être fournie aux clients qui se connectent avant l'authentification utilisateur et, si elle est fournie, elle peut apparaître dans un menu déroulant.

Cette information est masquée par défaut, mais peut être fournie en activant le paramètre général **Envoyer la liste de domaines** dans Horizon Console.

Il est recommandé de fournir la liste de domaines aux clients s'ils se connectent à l'environnement via un dispositif Unified Access Gateway qui est configuré pour effectuer l'authentification préalable à deux facteurs. La liste de domaines n'est pas envoyée à un client tant que l'authentification préalable n'a pas réussi. Pour plus d'informations sur la configuration de l'authentification à deux facteurs pour un dispositif Unified Access Gateway, consultez la documentation de Unified Access Gateway à l'adresse https://docs.vmware.com/fr/Unified-Access-Gateway/index.html.

Le paramètre **Masquer la liste de domaines dans l'interface utilisateur client** affecte uniquement l'interface utilisateur du client. Il ne modifie pas les informations que le serveur fournit au client. Ce paramètre est désactivé par défaut.

Lorsque les utilisateurs se connectent à un serveur, si l'option **Envoyer la liste de domaines** est désactivée et si l'option **Masquer la liste de domaines dans l'interface utilisateur client** est activée, le menu déroulant **Domaine** dans Horizon Client affiche `*DefaultDomain*` et les utilisateurs peuvent être amenés à entrer un domaine, par exemple, nomutilisateur@domaine, dans la zone de texte **Nom d'utilisateur**. Si les utilisateurs n'entrent pas manuellement le domaine et si plusieurs domaines sont configurés, ils peuvent échouer à se connecter au serveur.

Le tableau suivant montre comment les paramètres globaux **Envoyer la liste de domaines** et **Masquer la liste de domaines dans l'interface utilisateur client** déterminent le mode de connexion des utilisateurs au serveur.

Paramètre Envoyer la liste de domaines	Paramètre Masquer la liste de domaines dans l'interface utilisateur client	Mode de connexion des utilisateurs
Désactivé (par défaut)	Activé	Le menu déroulant **Domaine** est masqué. Les utilisateurs doivent entrer l'une des valeurs suivantes dans la zone de texte **Nom d'utilisateur**. ■ Nom d'utilisateur (non autorisé pour plusieurs domaines) ■ ***domain\username*** ■ ***username@domain.com***
Désactivé (par défaut)	Désactivé	Si un domaine par défaut est configuré sur le client, il s'affiche dans le menu déroulant **Domaine**. Si le client ne connaît pas un domaine par défaut, `*DefaultDomain*` s'affiche dans le menu déroulant **Domaine**. Les utilisateurs doivent entrer l'une des valeurs suivantes dans la zone de texte **Nom d'utilisateur**. ■ Nom d'utilisateur (non autorisé pour plusieurs domaines) ■ ***domain\username*** ■ ***username@domain.com***
Activé	Activé	Le menu déroulant **Domaine** est masqué. Les utilisateurs doivent entrer l'une des valeurs suivantes dans la zone de texte **Nom d'utilisateur**. ■ Nom d'utilisateur (non autorisé pour plusieurs domaines) ■ ***domain\username*** ■ ***username@domain.com***
Activé	Désactivé	Les utilisateurs peuvent entrer un nom d'utilisateur dans la zone de texte **Nom d'utilisateur** et sélectionner un domaine dans le menu déroulant **Domaine**. Ils peuvent également entrer l'une des valeurs suivantes dans la zone de texte **Nom d'utilisateur**. ■ ***domain\username*** ■ ***username@domain.com***

Ports et services

3

Certains ports UDP et TCP doivent être ouverts pour que les composants VMware Horizon puissent communiquer entre eux. Savoir quels services Windows sont exécutés sur chaque type de serveur VMware Horizon permet d'identifier les services qui ne se trouvent pas sur le serveur.

Ce chapitre contient les rubriques suivantes :

Ports TCP et UDP d'VMware Horizon

VMware Horizon utilise des ports TCP et UDP pour l'accès réseau entre ses composants.

Lors de l'installation, VMware Horizon peut configurer facultativement des règles de pare-feu Windows pour ouvrir les ports utilisés par défaut. Si vous modifiez les ports par défaut après l'installation, vous devez reconfigurer manuellement les règles de pare-feu Windows pour autoriser l'accès sur les ports mis à jour. Reportez-vous à la section « Remplacement des ports par défaut pour les services VMware Horizon » dans le document *Installation d'Horizon*.

Pour obtenir une liste de ports qu'VMware Horizon utilise pour une connexion de certificat associée à la solution TrueSSO, reportez-vous à la section Ports TrueSSO d'VMware Horizon.

Tableau 3-1. Ports TCP et UDP utilisés par VMware Horizon

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

Tableau 3-1. Ports TCP et UDP utilisés par VMware Horizon (suite)

Source	Port	Cible	Port	Protocole	Description
Serveur de connexion ou dispositif Unified Access Gateway	*	Horizon Agent	3389	TCP	Trafic Microsoft RDP vers des postes de travail VMware Horizon quand des connexions par tunnel sont utilisées.
Serveur de connexion ou dispositif Unified Access Gateway	*	Horizon Agent	9427	TCP	Redirection multimédia Windows, redirection du lecteur client, optimisation de Microsoft Teams, redirection multimédia HTML5, redirection de l'imprimante VMware et redirection USB lors de l'utilisation de connexions par tunnel.
Serveur de connexion ou dispositif Unified Access Gateway	*	Horizon Agent	32111	TCP	Redirection USB et synchronisation de fuseau horaire quand des connexions par tunnel sont utilisées.
Serveur de connexion ou dispositif Unified Access Gateway	*	Horizon Agent	4172	TCP	PCoIP, si PCoIP Secure Gateway est utilisé.
Serveur de connexion ou dispositif Unified Access Gateway	*	Horizon Agent	22443	TCP	VMware Blast Extreme si Blast Secure Gateway est utilisé.
Serveur de connexion ou dispositif Unified Access Gateway	*	Horizon Agent	22443	TCP	HTML Access si Blast Secure Gateway est utilisé.
Horizon Agent	4172	Horizon Client	*	UDP	PCoIP, si PCoIP Secure Gateway n'est pas utilisé. **Note** Comme le port cible varie, voir la note sous ce tableau.
Horizon Agent	4172	Serveur de connexion ou dispositif Unified Access Gateway	55000	UDP	PCoIP (pas SALSA20) si PCoIP Secure Gateway est utilisé.
Horizon Agent	4172	Dispositif Unified Access Gateway	*	UDP	PCoIP. Des applications et des postes de travail VMware Horizon renvoient des données PCoIP à un dispositif Unified Access Gateway à partir du port UDP 4172. Le port UDP de destination sera le port source des paquets UDP reçus. Comme ces paquets sont des données de réponse, il est normalement inutile d'ajouter une règle de pare-feu explicite pour cela.

Tableau 3-1. Ports TCP et UDP utilisés par VMware Horizon (suite)

Source	Port	Cible	Port	Protocole	Description
Horizon Agent (non géré)	*	Instance du Serveur de connexion	389	TCP	Accès AD LDS lors de l'installation de l'agent non géré. **Note** Pour d'autres utilisations de ce port, consultez la note au-dessous de ce tableau.
Horizon Client	*	Serveur de connexion ou dispositif Unified Access Gateway	80	TCP	TLS (accès HTTPS) est activé par défaut pour les connexions client, mais le port 80 (accès HTTP) peut être utilisé dans certains cas. Reportez-vous à la section Redirection HTTP dans VMware Horizon.
Horizon Client	*	Serveur de connexion ou dispositif Unified Access Gateway	443	TCP	HTTPS pour la connexion à VMware Horizon. (Ce port est également utilisé pour le tunnelling quand des connexions par tunnel sont utilisées.)
Horizon Client	*	Serveur de connexion ou dispositif Unified Access Gateway	4172	TCP et UDP	PCoIP, si PCoIP Secure Gateway est utilisé.
Horizon Client	*	Horizon Agent	3389	TCP	Trafic Microsoft RDP vers des postes de travail VMware Horizon si des connexions directes sont utilisées à la place de connexions par tunnel.
Horizon Client	*	Horizon Agent	9427	TCP	Redirection multimédia Windows, redirection du lecteur client, optimisation de Microsoft Teams, redirection multimédia HTML5, redirection de l'imprimante VMware et redirection USB lors de l'utilisation de connexions directes plutôt que des connexions par tunnel.
Horizon Client	*	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	*	Horizon Agent	4172	TCP et UDP	PCoIP, si PCoIP Secure Gateway n'est pas utilisé. **Note** Comme le port source varie, voir la note sous ce tableau.
Horizon Client	*	Horizon Agent	22443	TCP et UDP	VMware Blast
Horizon Client	*	Serveur de connexion ou dispositif Unified Access Gateway	4172	TCP et UDP	PCoIP (pas SALSA20) si PCoIP Secure Gateway est utilisé. **Note** Comme le port source varie, voir la note sous ce tableau.
Navigateur Web	*	Dispositif Unified Access Gateway	8443	TCP	HTML Access.
Serveur de connexion	*	Serveur de connexion	48080	TCP	Pour la communication interne entre les composants du Serveur de connexion.

Tableau 3-1. Ports TCP et UDP utilisés par VMware Horizon (suite)

Source	Port	Cible	Port	Protocole	Description
Serveur de connexion	*	vCenter Server	80	TCP	Messages SOAP si TLS est désactivé pour l'accès à des serveurs vCenter Server.
Serveur de connexion	*	vCenter Server	443	TCP	Messages SOAP si TLS est activé pour l'accès à des serveurs vCenter Server.
Serveur de connexion	*	Serveur de connexion	4100	TCP	Trafic interroutage JMS.
Serveur de connexion	*	Serveur de connexion	4101	TCP	Trafic interroutage JMS TLS.
Serveur de connexion	*	Serveur de connexion	8472	TCP	Pour la communication entre espaces dans Architecture Cloud Pod.
Serveur de connexion	*	Serveur de connexion	22389	TCP	Pour la réplication LDAP globale dans Architecture Cloud Pod.
Serveur de connexion	*	Serveur de connexion	22636	TCP	Pour la réplication LDAP globale sécurisée dans Architecture Cloud Pod.
Serveur de connexion	*	Serveur de connexion	32111	TCP	Trafic de partage de clé.
Serveur de connexion	*	Autorité de certification	*	HTTP, HTTPS	Requêtes CRL ou OCSP
Dispositif Unified Access Gateway	*	Serveur de connexion ou équilibrage de charge	443	TCP	Accès HTTPS. Des dispositifs Unified Access Gateway se connectent sur le port TCP 443 pour communiquer avec une instance du Serveur de connexion ou un équilibrage de charge devant plusieurs instances du Serveur de connexion.
Horizon Help Desk Tool	*	Horizon Agent	3389	TCP	Trafic RDP Microsoft vers des postes de travail Horizon pour l'assistance à distance.

Note 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.

Note Microsoft Windows Server requiert qu'une plage de ports dynamique soit ouverte entre tous les Serveurs de connexion dans l'environnement VMware Horizon. Ces ports sont requis par Microsoft Windows pour le fonctionnement normal de l'appel de procédure distante (RPC) et la réplication Active Directory. Pour plus d'informations sur la plage de ports dynamique, consultez la documentation de Microsoft Windows Server.

Note Sur une instance du Serveur de connexion, le port 389 est accessible pour des connexions ad hoc peu fréquentes. Il est accessible lors de l'installation d'un agent non géré, comme indiqué dans le tableau, et également lors de l'utilisation d'un éditeur LDAP pour modifier directement la base de données, ainsi que lors de l'émission de commandes à l'aide d'un outil tel que repadmin. Une règle de pare-feu est créée à cet effet lors de l'installation d'AD LDS, mais elle peut être désactivée si l'accès au port n'est pas requis.

Note VMware Blast Extreme Adaptive Transport réserve des ports à partir de la plage de ports éphémères 49152-65535, par défaut. Consultez l'article 52558 de la base de connaissances.

Redirection HTTP dans VMware Horizon

Les tentatives de connexion sur HTTP sont redirigées en mode silencieux vers HTTPS, à l'exception des tentatives de connexion à Horizon Console. La redirection HTTP n'est pas nécessaire pour les clients Horizon plus récents, car ils sont dirigés par défaut vers HTTPS. Elle est cependant utile lorsque les utilisateurs se connectent avec un navigateur Web, par exemple pour télécharger Horizon Client.

Le problème de la redirection HTTP est qu'il s'agit d'un protocole non sécurisé. Si un utilisateur ne prend pas l'habitude d'entrer **`https://`** dans la barre d'adresse, une personne malveillante peut compromettre le navigateur Web, installer un programme malveillant ou voler des informations d'identification, même lorsque la page attendue est affichée correctement.

Note La redirection HTTP pour les connexions externes peut avoir lieu uniquement si vous configurez votre pare-feu externe pour qu'il autorise le trafic entrant sur le port TCP 80.

Les tentatives de connexion sur HTTP à Horizon Console ne sont pas redirigées. Au lieu de cela, un message d'erreur indiquant que vous devez utiliser HTTPS est renvoyé.

Pour empêcher la redirection de toutes les tentatives de connexion HTTP, reportez-vous à la section « Empêcher la redirection HTTP des connexions des clients vers le Serveur de connexion » dans le document *Installation d'Horizon*.

Les connexions au port 80 d'une instance du Serveur de connexion peuvent également avoir lieu si vous déchargez les connexions du client TLS sur un périphérique intermédiaire. Reportez-vous à la section « Décharger des connexions TLS sur des serveurs intermédiaires » dans le document *Administration d'Horizon*.

Pour autoriser la redirection HTTP lorsque le numéro de port TLS a été modifié, reportez-vous à la section « Modifier le numéro de port de la redirection HTTP vers le serveur de connexion » dans le document *Installation d'Horizon*.

Ports TrueSSO d'VMware Horizon

VMware Horizon utilise des ports TrueSSO pour la voie de communication (port et protocole) et des contrôles de sécurité utilisés pour que le certificat puisse passer entre Horizon Connection

Server et le poste de travail virtuel ou l'application publiée pour une connexion de certificat associée à la solution TrueSSO.

Tableau 3-2. Ports TrueSSO utilisés par VMware Horizon

Source	Cible	Port	Protocole	Description
Horizon Client	Dispositif VMware Identity Manager	TCP 443	HTTPS	Démarrez VMware Horizon depuis le dispositif VMware Identity Manager qui génère l'assertion SAML et l'artefact.
Horizon Client	Horizon Connection Server	TCP 443	HTTPS	Lancer Horizon Client.
Horizon Connection Server	Dispositif VMware Identity Manager	TCP 443	HTTPS	Le Serveur de connexion effectue une résolution SAML sur VMware Identity Manager. VMware Identity Manager valide l'artefact et renvoie l'assertion.
Horizon Connection Server	Serveur d'inscription d'Horizon	TCP 32111		Utilisez le serveur d'inscription.
Serveur d'inscription	ADCS			Le serveur d'inscription demande un certificat auprès de l'autorité de certification Microsoft pour générer un certificat temporaire de courte durée. Le service d'inscription utilise l'appel de procédure distante TCP 135 pour la communication initiale avec l'autorité de certification, puis un port aléatoire compris entre 1024 et 5000 et entre 49152 et 65535. Reportez-vous à la section Services de certificats dans https://support.microsoft.com/en-us/help/832017#method4. Le serveur d'inscription communique également avec des contrôleurs de domaine, à l'aide de tous les ports appropriés afin de découvrir un contrôleur de domaine, de se lier à Active Directory et de l'interroger. Reportez-vous aux sections https://support.microsoft.com/en-us/help/832017#method1 et https://support.microsoft.com/en-us/help/832017#method12.
Horizon Agent	Horizon Connection Server	TCP 4002	JMS sur TLS	Horizon Agent demande et reçoit un certificat pour la connexion.
Poste de travail virtuel ou application publiée	AD DC			Windows vérifie l'authenticité du certificat avec Active Directory. Consultez la documentation de Microsoft pour obtenir une liste des ports et des protocoles, car de nombreux ports peuvent être nécessaires.
Horizon Client	Horizon Agent (session de protocole)	TCP/UDP 22 443	Blast	Ouvrez une session sur le poste de travail ou l'application Windows et une session distante est lancée sur Horizon Client.
Horizon Client	Horizon Agent (session de protocole)	UDP 4172	PCoIP	Ouvrez une session sur le poste de travail ou l'application Windows et une session distante est lancée sur Horizon Client.

Services sur un hôte du Serveur de connexion

Le fonctionnement d'VMware Horizon dépend de plusieurs services s'exécutant sur un hôte du Serveur de connexion.

Tableau 3-3. Services d'un hôte du Serveur de connexion Horizon

Nom du service	Type de démarrage	Description
VMware Horizon Blast Secure Gateway	Automatique	Fournit des services HTML Access et Blast Extreme sécurisés. Ce service doit être en cours d'exécution si des clients se connectent au Serveur de connexion via Blast Secure Gateway.
Serveur de connexion VMware Horizon	Automatique	Fournit des services de Broker pour les connexions. Ce service doit toujours être en cours d'exécution. Si vous démarrez ou arrêtez ce service, il démarre ou arrête également les services Framework, Message Bus, Security Gateway et Web. Ce service ne démarre ni n'arrête le service VMwareVDMDS ou VMware Horizon Script Host.
Composant VMware Horizon Framework	Manuel	Fournit des services de journalisation des événements, de sécurité et d'infrastructure COM+. Ce service doit toujours être en cours d'exécution.
Composant VMware Horizon Message Bus	Manuel	Fournit des services de messagerie entre les composants VMware Horizon. Ce service doit toujours être en cours d'exécution.
VMware Horizon PCoIP Secure Gateway	Manuel	Fournit des services PCoIP Secure Gateway. Ce service doit être en cours d'exécution si des clients se connectent au Serveur de connexion via PCoIP Secure Gateway.
VMware Horizon Script Host	Désactivé	Fournit la prise en charge de scripts tiers s'exécutant lorsque vous supprimez des machines virtuelles. Par défaut, ce service est désactivé. Vous devez activer ce service si vous voulez exécuter des scripts.
Composant VMware Horizon Security Gateway	Manuel	Fournit des services de passerelle communs. Ce service doit toujours être en cours d'exécution.
Composant Web VMware Horizon	Manuel	Fournit des services Web. Ce service doit toujours être en cours d'exécution.
VMwareVDMDS	Automatique	Fournit des services Horizon LDAP. Ce service doit toujours être en cours d'exécution. Pendant les mises à niveau d'VMware Horizon, ce service garantit la migration correcte des données existantes.

Vérification de l'empreinte numérique de certificat et génération automatique des certificats

4

VMware Horizon utilise un grand nombre de certificats de clé publique. Certains de ces certificats sont vérifiés à l'aide de mécanismes impliquant un tiers de confiance, mais ces mécanismes ne fournissent pas toujours la précision, la vitesse et la flexibilité nécessaires. VMware Horizon utilise un autre mécanisme appelé vérification de l'empreinte numérique dans plusieurs situations.

Au lieu de valider des champs individuels de certificat ou de créer une chaîne de confiance, la vérification des empreintes numériques traite le certificat comme un jeton, en faisant correspondre la séquence d'octets complète (ou un hachage cryptographique de celle-ci) à une séquence ou un hachage d'octets pré-partagé. En général, cela est partagé juste-à-temps sur un canal de confiance séparé et signifie que le certificat présenté par un service peut être vérifié pour être le certificat exact qui était attendu.

Le bus de messages Horizon communique entre des Serveurs de connexion, ainsi qu'entre des instances d'Horizon Agent et du Serveur de connexion. Les canaux de configuration utilisent des signatures par message et le chiffrement de charge utile, alors que les canaux principaux sont protégés à l'aide de TLS avec l'authentification mutuelle. Lors de l'utilisation de TLS pour protéger un canal, l'authentification du client et du serveur implique des certificats TLS et une validation des empreintes numériques. Pour les canaux du bus de messages Horizon, le serveur est toujours un routeur de message. Le client peut également être un routeur de message, car c'est ainsi que les routeurs de message partagent des messages. Toutefois, les clients sont des instances du Serveur de connexion ou des agents Horizon Agent.

Les empreintes numériques de certificat et les clés de signature de message de configuration initiales sont fournies de différentes manières. Sur les Serveurs de connexion, les empreintes numériques de certificat sont stockées dans LDAP, afin que les agents Horizon Agent puissent communiquer avec n'importe quel Serveur de connexion, et tous les Serveurs de connexion peuvent communiquer entre eux. Les certificats de serveur et de client du bus de message Horizon sont générés automatiquement et échangés régulièrement, et les certificats périmés sont automatiquement supprimés, donc aucune intervention manuelle n'est nécessaire, ou possible. Les certificats à chaque extrémité des canaux principaux sont générés automatiquement et régulièrement et échangés sur les canaux de configuration. Vous ne pouvez pas remplacer ces certificats vous-même. Les certificats expirés sont supprimés automatiquement.

Un mécanisme similaire s'applique à la communication inter-espace.

D'autres canaux de communication peuvent utiliser des certificats fournis par le client, mais la valeur par défaut consiste à générer automatiquement les certificats. Ces canaux incluent les connexions du tunnel sécurisé, du serveur d'inscription et de vCenter, le protocole d'affichage et des canaux auxiliaires. Pour plus d'informations sur la façon de remplacer ces certificats, consultez le document *Administration d'Horizon*. Les certificats par défaut sont générés lors de l'installation et ne sont pas automatiquement renouvelés, à l'exception de PCoIP. Si un certificat généré par l'infrastructure à clé publique n'est pas disponible pour une utilisation par le protocole PCoIP, il génère automatiquement un nouveau certificat à chaque démarrage. La vérification de l'empreinte numérique est utilisée pour la plupart de ces canaux, même si un certificat généré par l'infrastructure à clé publique est utilisé.

La vérification des certificats vCenter utilise une combinaison de techniques. Les instances du Serveur de connexion tentent toujours de valider le certificat reçu à l'aide de l'infrastructure à clé publique. Si cette validation échoue, après avoir examiné le certificat, l'administrateur VMware Horizon peut autoriser la poursuite de la connexion, et le Serveur de connexion mémorise le hachage cryptographique du certificat pour les prochaines acceptations sans surveillance à l'aide de la vérification de l'empreinte numérique.

Configuration des protocoles de sécurité et des suites de chiffrement sur une instance du Serveur de connexion

5

Vous pouvez configurer les protocoles de sécurité et les suites de chiffrement qui sont acceptés par le Serveur de connexion. Vous pouvez définir une stratégie d'acceptation générale qui s'applique à toutes les instances du Serveur de connexion dans un groupe répliqué ou définir une stratégie d'acceptation pour des instances du Serveur de connexion.

Vous pouvez également configurer les protocoles de sécurité et les suites de chiffrement que les instances du Serveur de connexion proposent lors de la connexion à vCenter Server. Vous pouvez définir une stratégie de proposition générale qui s'applique à toutes les instances du Serveur de connexion dans un groupe répliqué. Vous ne pouvez pas définir des instances individuelles à exclure d'une stratégie de proposition générale.

Note Les paramètres de sécurité du Serveur de connexion ne s'appliquent pas à Blast Secure Gateway (BSG). Vous devez configurer la sécurité pour BSG séparément. Reportez-vous à la section Chapitre 6 Configuration des protocoles de sécurité et des suites de chiffrement pour Blast Secure Gateway.

Les fichiers Unlimited Strength Jurisdiction Policy d'Oracle sont inclus en standard, ce qui autorise les clés 256 bits par défaut.

Ce chapitre contient les rubriques suivantes :

Stratégies générales 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.

Tableau 5-1. Stratégie d'acceptation globale par défaut

Protocoles de sécurité par défaut	Suites de chiffrement par défaut
■ TLS 1.2	■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Tableau 5-2. Stratégie de proposition globale par défaut

Protocoles de sécurité par défaut	Suites de chiffrement par défaut
■ TLS 1.2	■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

En mode FIPS, seules les suites de chiffrement GCM sont activées.

Configuration des stratégies d'acceptation et de proposition générales

Les stratégies d'acceptation et de proposition générales sont définies dans les attributs Horizon LDAP. Ces stratégies s'appliquent à toutes les instances du Serveur de connexion. Pour modifier une stratégie générale, vous pouvez modifier Horizon LDAP sur n'importe quelle instance du Serveur de connexion.

Chaque stratégie est un attribut à une seule valeur dans l'emplacement Horizon LDAP suivant : `cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int`

Stratégies d'acceptation et de proposition générales définies dans Horizon LDAP

Vous pouvez modifier les attributs Horizon LDAP qui définissent les stratégies d'acceptation et de proposition générales.

Stratégies d'acceptation générales

L'attribut suivant répertorie les protocoles de sécurité. Vous devez classer la liste en plaçant le dernier protocole en premier :

```
pae-ServerSSLSecureProtocols = \LIST:TLSv1.2,TLSv1.1,TLSv1
```

L'attribut suivant répertorie les suites de chiffrement. Cet exemple montre une liste abrégée :

```
pae-ServerSSLCipherSuites =
\LIST:TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

L'attribut suivant contrôle la priorité des suites de chiffrement. En temps normal, le classement des suites de chiffrement du serveur n'est pas important et le classement du client est utilisé. Pour utiliser plutôt le classement des suites de chiffrement du serveur, définissez l'attribut suivant :

```
pae-ServerSSLHonorClientOrder = 0
```

Stratégies de proposition générales

L'attribut suivant répertorie les protocoles de sécurité. Vous devez classer la liste en plaçant le dernier protocole en premier :

```
pae-ClientSSLSecureProtocols = \LIST:TLSv1.2,TLSv1.1,TLSv1
```

L'attribut suivant répertorie les suites de chiffrement. Cette liste doit être dans l'ordre de préférence. Placez la suite de chiffrement préférée en premier, puis la deuxième suite préférée, etc. Cet exemple montre une liste abrégée :

```
pae-ClientSSLCipherSuites =
\LIST:TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

Modifier les stratégies d'acceptation et de proposition générales

Pour modifier les stratégies d'acceptation et de proposition générales pour des protocoles de sécurité et des suites de chiffrement, utilisez l'utilitaire ADSI Edit pour modifier les attributs Horizon LDAP.

Conditions préalables

- Familiarisez-vous avec les attributs Horizon LDAP qui définissent les stratégies d'acceptation et de proposition. Reportez-vous à la section Stratégies d'acceptation et de proposition générales définies dans Horizon LDAP.
- Pour plus d'informations sur l'utilisation de l'utilitaire ADSI Edit sur votre version du système d'exploitation Windows Server, consultez le site Web Microsoft TechNet.

Procédure

1. Démarrez l'utilitaire ADSI Edit sur votre ordinateur Serveur de connexion.
2. Dans l'arborescence de la console, sélectionnez **Se connecter à**.
3. Dans la zone de texte **Sélectionnez ou entrez un nom unique ou un contexte d'attribution de noms**, tapez le nom unique **`DC=vdi, DC=vmware, DC=int`**.
4. Dans la zone de texte **Sélectionnez ou entrez un domaine ou un serveur**, sélectionnez ou tapez **`localhost:389`** ou le nom de domaine complet de l'ordinateur Serveur de connexion suivi du port 389.

   Par exemple : **`localhost:389`** ou **`mycomputer.mydomain.com:389`**

5 Développez l'arborescence d'ADSI Edit, développez **OU=Properties**, sélectionnez **OU=Global** et sélectionnez **CN=Common** dans le volet de droite.

6 Sur l'objet **CN=Common, OU=Global, OU=Properties**, sélectionnez chaque attribut que vous voulez modifier et tapez la nouvelle liste de protocoles de sécurité ou de suites de chiffrement.

7 Redémarrez le composant de la passerelle de sécurité de VMware Horizon du service Windows sur chaque instance du Serveur de connexion si vous avez modifié `pae-ServerSSLSecureProtocols`.

   Vous n'avez pas besoin de redémarrer les services après avoir modifié `pae-ClientSSLSecureProtocols`.

Configurer des stratégies d'acceptation sur des serveurs individuels

Pour spécifier une stratégie d'acceptation locale sur une instance individuelle du Serveur de connexion, vous devez ajouter des propriétés au fichier `locked.properties`. Si le fichier `locked.properties` n'existe pas encore sur le serveur, vous devez le créer.

Vous ajoutez une entrée `secureProtocols.`*`n`* pour chaque protocole de sécurité que vous voulez configurer. Utilisez la syntaxe suivante : `secureProtocols.`*`n=protocole de sécurité`*.

Vous ajoutez une entrée `enabledCipherSuite.`*`n`* pour chaque suite de chiffrement que vous voulez configurer. Utilisez la syntaxe suivante : `enabledCipherSuite.`*`n=suite de chiffrement`*.

La variable *`n`* est un entier que vous ajoutez dans l'ordre (1, 2, 3) pour chaque type d'entrée.

Vous ajoutez une entrée `honorClientOrder` pour contrôler la priorité des suites de chiffrement. En temps normal, le classement des suites de chiffrement du serveur n'est pas important et le classement du client est utilisé. Pour utiliser plutôt le classement des suites de chiffrement du serveur, utilisez la syntaxe suivante :

```
honorClientOrder=false
```

Vérifiez que les entrées dans le fichier `locked.properties` respectent la syntaxe et que les noms des suites de chiffrement et des protocoles de sécurité sont bien orthographiés. Toute erreur dans le fichier peut entraîner l'échec de la négociation entre le client et le serveur.

Procédure

1 Créez ou modifiez le fichier `locked.properties` dans le dossier de configuration de la passerelle TLS/SSL sur l'ordinateur exécutant le Serveur de connexion.

   Par exemple : *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\`

2 Ajoutez les entrées `secureProtocols.`*`n`* et `enabledCipherSuite.`*`n`*, y compris les protocoles de sécurité et les suites de chiffrement associés.

3 Enregistrez le fichier `locked.properties`.

4 Redémarrez le service VMware Horizon Connection Server pour que vos modifications prennent effet.

Exemple : Stratégies d'acceptation par défaut sur un serveur individuel

L'exemple suivant montre les entrées dans le fichier `locked.properties` qui sont nécessaires pour spécifier les stratégies par défaut :

```
# The following list should be ordered with the latest protocol first:

secureProtocols.1=TLSv1.2

# This setting must be the latest protocol given in the list above:

preferredSecureProtocol=TLSv1.2

# The order of the following list is unimportant unless honorClientOrder is false:

enabledCipherSuite.1=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
enabledCipherSuite.2=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
enabledCipherSuite.3=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
enabledCipherSuite.4=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

# Use the client's ordering of cipher suites (ignores the ordering given above):

honorClientOrder=true
```

Note En mode FIPS, seules les suites de chiffrement GCM sont activées.

Configurer des stratégies de proposition sur des postes de travail distants

Pour contrôler la sécurité des connexions du bus de messages au Serveur de connexion, vous pouvez configurer les stratégies de proposition sur des postes de travail distants qui exécutent Windows.

Conditions préalables

Pour éviter un échec de la connexion, configurez le Serveur de connexion afin qu'il accepte les mêmes stratégies.

Procédure

1 Sur le poste de travail distant, démarrez l'éditeur du Registre Windows.

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
   ```

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
   ```

Protocoles et chiffrements anciens désactivés dans VMware Horizon

Certains anciens protocoles et chiffrements qui ne sont plus considérés comme étant sécurisés sont désactivés par défaut dans VMware Horizon. Si nécessaire, vous pouvez les activer manuellement.

Suites de chiffrement DHE

Pour plus d'informations, consultez http://kb.vmware.com/kb/2121183. Les suites de chiffrement qui sont compatibles avec les certificats DSA utilisent des clés Diffie-Hellman éphémères, et ces suites ne sont plus activées par défaut, à compter d'Horizon 6 version 6.2.

Pour les instances du Serveur de connexion et les postes de travail VMware Horizon, vous pouvez activer ces suites de chiffrement en modifiant la base de données Horizon LDAP, le fichier `locked.properties` ou le registre, comme décrit dans ce guide. Voir Modifier les stratégies d'acceptation et de proposition générales, Configurer des stratégies d'acceptation sur des serveurs individuels et Configurer des stratégies de proposition sur des postes de travail distants. Vous pouvez définir une liste de suites de chiffrement qui inclut une ou plusieurs des suites suivantes, dans cet ordre :

- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (TLS 1.2 uniquement, pas FIPS)
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (TLS 1.2 uniquement, pas FIPS)
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (TLS 1.2 uniquement)
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (TLS 1.2 uniquement)
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA

Pour les machines View Agent Direct-Connection (VADC), vous pouvez activer des suites de chiffrement DHE en ajoutant ce qui suit à la liste de chiffrements lorsque vous suivez la procédure « Désactiver les chiffrements faibles dans les protocoles SSL/TLS pour les machines Horizon Agent » dans le document *Installation d'Horizon*.

```
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
```

Note Il n'est pas possible d'activer la prise en charge pour les certificats ECDSA. Ces certificats n'ont jamais été pris en charge.

SSLv3

Dans VMware Horizon, SSL version 3.0 a été supprimé.

Pour plus d'informations, reportez-vous à la section http://tools.ietf.org/html/rfc7568.

RC4

Pour plus d'informations, reportez-vous à la section http://tools.ietf.org/html/rfc7465.

Pour les instances du Serveur de connexion et les postes de travail VMware Horizon, vous pouvez activer RC4 sur un Serveur de connexion ou une machine Horizon Agent en modifiant le fichier de configuration `C:\Program Files\VMware\VMware View\Server\jre\lib\security\java.security`. À la fin du fichier se trouve une entrée multiligne appelée `jdk.tls.legacyAlgorithms`. Supprimez `RC4_128` et la virgule qui suit de cette entrée et redémarrez le Serveur de connexion ou la machine Horizon Agent, selon le cas.

Pour les machines View Agent Direct-Connection (VADC), vous pouvez activer RC4 en ajoutant ce qui suit à la liste de chiffrements lorsque vous suivez la procédure « Désactiver les chiffrements faibles dans les protocoles SSL/TLS pour les machines Horizon Agent » dans le document *Installation d'Horizon*.

```
TLS_RSA_WITH_RC4_128_SHA
```

TLS 1.0

Dans VMware Horizon, TLS 1.0 est désactivé par défaut.

Pour plus d'informations, consultez https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf et http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf. Pour obtenir des instructions sur l'activation de TLS 1.0, reportez-vous à la section « Activer TLSv1 sur des connexions vCenter depuis le Serveur de connexion » et le document *Mises à niveau d'Horizon*.

Configuration des protocoles de sécurité et des suites de chiffrement pour Blast Secure Gateway

6

Les paramètres de sécurité du Serveur de connexion ne s'appliquent pas à Blast Secure Gateway (BSG). Vous devez configurer la sécurité pour BSG séparément.

Ce chapitre contient les rubriques suivantes :

Configurer des protocoles de sécurité et des suites de chiffrement pour Blast Secure Gateway (BSG)

Vous pouvez configurer les protocoles de sécurité et les suites de chiffrement que l'écouteur côté client de BSG accepte en modifiant le fichier `absg.properties`.

Les protocoles autorisés sont, du plus faible au plus élevé, tls1.0, tls1.1 et tls1.2. Les protocoles plus anciens, tels que SSLv3 et version antérieure, ne sont jamais autorisés. Deux propriétés, `localHttpsProtocolLow` et `localHttpsProtocolHigh`, déterminent la plage de protocoles que l'écouteur BSG acceptera. Par exemple, si vous définissez `localHttpsProtocolLow=tls1.0` et `localHttpsProtocolHigh=tls1.2`, l'écouteur accepte TLS 1.0, TLS 1.1 et TLS 1.2. Les paramètres par défaut sont `localHttpsProtocolLow=tls1.2` et `localHttpsProtocolHigh=tls1.2`, ce qui signifie que seul TLS 1.2 est autorisé par défaut. Vous pouvez examiner le fichier `absg.log` de BSG pour voir les valeurs qui sont appliquées pour une instance de BSG spécifique.

Vous devez spécifier la liste de chiffrements en utilisant le format défini dans OpenSSL. Vous pouvez rechercher `openssl cipher string` dans un navigateur Web et déterminer le format de la liste de chiffrement. La liste de chiffrements suivante est celle par défaut :

```
ECDHE+AESGCM
```

Note En mode FIPS, seules les suites de chiffrement GCM sont activées (`ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256`).

Procédure

1. Sur l'instance du Serveur de connexion, modifiez le fichier *install_directory*\VMware\VMware View\Server\appblastgateway\absg.properties.

   Par défaut, le répertoire d'installation est *%ProgramFiles%*.

2. Modifiez les propriétés `localHttpsProtocolLow` et `localHttpsProtocolHigh` pour spécifier une plage de protocoles.

   Par exemple,

   ```
   localHttpsProtocolLow=tls1.0
   localHttpsProtocolHigh=tls1.2
   ```

   Pour activer un seul protocole, spécifiez le même protocole pour `localHttpsProtocolLow` et `localHttpsProtocolHigh`.

3. Modifiez la propriété `localHttpsCipherSpec` pour spécifier une liste de suites de chiffrement.

   Par exemple,

   ```
   localHttpsCipherSpec=!aNULL:kECDH+AESGCM:ECDH+AESGCM:kECDH+AES:ECDH+AES
   ```

4. Redémarrez VMware Horizon Blast Secure Gateway du service Windows.

Configuration des protocoles de sécurité et des suites de chiffrement pour PCoIP Secure Gateway

7

Les paramètres de sécurité du Serveur de connexion ne s'appliquent pas à PCoIP Secure Gateway (PSG). Vous devez configurer la sécurité pour PSG séparément.

Ce chapitre contient les rubriques suivantes :

Configurer des protocoles de sécurité et des suites de chiffrement pour PCoIP Secure Gateway (PSG)

Vous pouvez configurer les protocoles de sécurité et les suites de chiffrement que l'écouteur côté client de PSG accepte en modifiant le registre. Si nécessaire, cette tâche peut également être exécutée sur un hôte RDS.

Les protocoles autorisés sont, du plus faible au plus élevé, tls1.0, tls1.1 et tls1.2. Les protocoles plus anciens, tels que SSLv3 et version antérieure, ne sont jamais autorisés. Le paramètre par défaut est `tls1.2:tls1.1`.

Note En mode FIPS, seul TLS 1.2 est activé (TLS 1.2).

La liste de chiffrements suivante est celle par défaut :

```
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:@STRENGTH"
```

Note En mode FIPS, seules les suites de chiffrement GCM sont activées (`ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256`).

Procédure

1 Sur l'instance du Serveur de connexion ou sur l'hôte RDS, ouvrez un éditeur de Registre et accédez à `HKLM\Software\Teradici\SecurityGateway`.

2 Ajoutez ou modifiez la valeur du registre REG_SZ `SSLProtocol` pour spécifier une liste de protocoles.

   Par exemple,

   ```
   tls1.2:tls1.1
   ```

3 Ajoutez ou modifiez la valeur du registre REG_SZ `SSLCipherList` pour spécifier une liste de suites de chiffrement.

   Par exemple,

   ```
   ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256
   ```

4 Ajoutez ou modifiez la valeur de Registre REG_SZ `SSLDisableAES128` pour filtrer les suites de chiffrement qui négocient une clé de chiffrement AES 128 bits. Si elle n'est pas définie, la valeur par défaut est de **0**. De cette façon, le filtre n'est pas appliqué. Pour exclure ces suites de chiffrement, activez le filtre en définissant la valeur de Registre sur **1**.

5 Ajoutez ou modifiez la valeur de Registre REG_SZ `SSLDisableRSACipher` pour filtrer les suites de chiffrement qui utilisent RSA pour l'échange de clés. Si elle n'est pas définie, la valeur par défaut est de **1**. De cette façon, ces suites de chiffrement sont filtrées de la liste. S'il est nécessaire de les inclure, désactivez le filtre en définissant la valeur de Registre sur **0**.

Déploiement de périphériques USB dans un environnement VMware Horizon sécurisé

8

Les périphériques USB peuvent être vulnérables à une menace de sécurité nommée BadUSB, dans laquelle le microprogramme de certains périphériques USB peut être piraté et remplacé par un logiciel malveillant. Par exemple, un périphérique peut ainsi être amené à rediriger le trafic réseau, ou à émuler un clavier et capturer la frappe effectuée. Vous pouvez configurer la fonctionnalité de redirection USB de manière à protéger votre déploiement VMware Horizon contre cette vulnérabilité de sécurité.

En désactivant la redirection USB, vous pouvez empêcher toute redirection de périphérique USB vers les applications et les postes de travail distants de vos utilisateurs. Vous pouvez également désactiver la redirection de périphériques USB spécifiques, pour permettre aux utilisateurs d'avoir uniquement accès à des périphériques spécifiques sur leurs applications et leurs postes de travail distants.

Le choix de prendre ou non ces mesures dépend des exigences de sécurité de votre organisation. Ces étapes ne sont pas obligatoires. Vous pouvez installer la redirection USB et laisser la fonctionnalité activée pour tous les périphériques USB de votre déploiement VMware Horizon. Au minimum, analysez sérieusement à quel degré votre organisation doit tenter de limiter son exposition à cette vulnérabilité de sécurité.

Ce chapitre contient les rubriques suivantes :

Désactivation de la redirection USB pour tous les types de périphériques

Certains environnements hautement sécurisés nécessitent que vous empêchiez tous les périphériques USB que les utilisateurs peuvent avoir connectés à leurs périphériques clients d'être redirigés vers leurs applications et postes de travail distants. Vous pouvez désactiver la redirection USB pour tous les pools de postes de travail, des pools de postes de travail spécifiques ou des utilisateurs spécifiques dans un pool de postes de travail.

Utilisez l'une des stratégies suivantes, selon votre situation :

- Lorsque vous installez Horizon Agent sur une image de poste de travail ou un hôte RDS, désactivez l'option de configuration **Redirection USB**. (L'option est décochée par défaut.) Cette approche empêche d'accéder à des périphériques USB sur l'ensemble des applications et des postes de travail distants qui sont déployés à partir de l'image du poste de travail ou de l'hôte RDS.
- Dans Horizon Console, modifiez la stratégie **Accès USB** pour autoriser ou refuser l'accès sur un pool spécifique. Avec cette approche, vous n'avez pas besoin de modifier l'image du poste de travail et pouvez accéder aux périphériques USB de pools d'applications et de postes de travail spécifiques.

  Seule la stratégie globale **Accès USB** est disponible pour les pools d'applications et de postes de travail publiés. Vous ne pouvez pas définir cette stratégie pour des pools d'applications ou de postes de travail publiés individuels.
- Dans Horizon Console, après avoir défini la stratégie au niveau du pool de postes de travail ou d'applications, vous pouvez remplacer la stratégie pour un utilisateur spécifique du pool en sélectionnant le paramètre **Remplacements d'utilisateur** et en sélectionnant un utilisateur.
- Définissez la stratégie `Exclude All Devices` sur **`true`**, du côté Horizon Agent ou du côté client, selon le cas.
- Utilisez Stratégies de carte à puce pour créer une stratégie qui désactive le paramètre de stratégie Horizon **Redirection USB**. Avec cette approche, vous pouvez désactiver la redirection USB sur un poste de travail distant spécifique si certaines conditions sont respectées. Par exemple, vous pouvez configurer une stratégie qui désactive la redirection USB lorsque des utilisateurs se connectent à un poste de travail distant depuis l'extérieur du réseau d'entreprise.

Si vous définissez la stratégie `Exclude All Devices` sur **`true`**, Horizon Client empêche la redirection de tous les périphériques USB. Vous pouvez utiliser d'autres paramètres de règle pour autoriser la redirection de périphériques spécifiques ou de familles de périphériques. Si vous définissez la stratégie sur **`false`**, Horizon Client autorise la redirection de tous les périphériques USB sauf ceux qui sont bloqués par d'autres paramètres de stratégie. Vous pouvez définir la stratégie dans Horizon Agent et Horizon Client. Le tableau suivant décrit comment la stratégie `Exclude All Devices` que vous pouvez définir pour Horizon Agent et Horizon Client se combinent pour produire une stratégie efficace pour l'ordinateur client. Par défaut, tous les périphériques USB sont autorisés à être redirigés, sauf blocage contraire.

Tableau 8-1. Effet de la combinaison de règles Exclure tous les périphériques

Stratégie Exclure tous les périphériques sur Horizon Agent	Stratégie Exclure tous les périphériques dans Horizon Client	Règle Exclure tous les périphériques effective combinée
false ou non défini (inclure tous les périphériques USB)	**false** ou non défini (inclure tous les périphériques USB)	Inclure tous les périphériques USB
false (inclure tous les périphériques USB)	**true** (exclure tous les périphériques USB)	Exclure tous les périphériques USB
true (exclure tous les périphériques USB)	Aucun ou non défini	Exclure tous les périphériques USB

Si vous avez défini la stratégie `Disable Remote Configuration Download` sur **true**, la valeur `Exclude All Devices` dans Horizon Agent n'est pas transmise à Horizon Client, mais Horizon Agent et Horizon Client appliquent la valeur locale `Exclude All Devices`.

Ces stratégies sont incluses dans le fichier de modèle d'administration ADMX pour la configuration d'Horizon Agent (`vdm_agent.admx`). Pour plus d'informations, reportez-vous à la section « Paramètres USB dans le modèle d'administration ADMX pour la configuration d'Horizon Agent » dans *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Désactivation de la redirection USB pour des périphériques spécifiques

Certains utilisateurs peuvent devoir rediriger des périphériques USB localement connectés afin de pouvoir effectuer des tâches sur leurs applications ou postes de travail distants. Par exemple, un médecin peut devoir utiliser un périphérique dictaphone USB pour enregistrer des informations médicales dans le dossier d'un patient. Dans ce cas, vous ne pouvez pas désactiver l'accès à tous les périphériques USB. Vous pouvez utiliser les paramètres de stratégie de groupe pour activer ou désactiver une redirection USB pour des périphériques spécifiques.

Avant d'activer la redirection USB pour des périphériques spécifiques, assurez-vous que vous approuvez les périphériques physiques connectés à des machines clientes dans votre entreprise. Assurez-vous de pouvoir approuver votre chaîne d'approvisionnement. Si possible, assurez le suivi d'une chaîne de sécurité pour les périphériques USB.

En outre, formez vos employés pour vous assurer qu'ils ne connectent pas des périphériques provenant de sources inconnues. Si possible, restreignez les périphériques de votre environnement à ceux qui acceptent uniquement des mises à jour de microprogramme signées, bénéficient d'une certification FIPS 140-2 Niveau 3 et ne prennent pas en charge tout type de microprogramme autorisant la mise à jour sur site. Ces types de périphériques USB peuvent poser des problèmes d'approvisionnement et, selon la configuration requise de vos périphériques, peuvent s'avérer impossibles à trouver. Ces choix peuvent être difficiles à mettre en œuvre dans la pratique, mais ils méritent d'être envisagés.

Chaque périphérique USB a son propre fournisseur et ID de produit qui l'identifie sur l'ordinateur. En configurant les paramètres de la stratégie de groupe Configuration d'Horizon Agent, vous pouvez définir une stratégie d'inclusion de ces types de périphériques connus. Avec cette approche, vous éliminez le risque d'autoriser l'insertion de périphériques inconnus dans votre environnement.

Par exemple, vous pouvez empêcher tous les périphériques, à l'exception de ceux associés à un fournisseur de périphériques et à un ID de produit connus, `vid/pid=0123/abcd`, d'être redirigés vers l'application ou le poste de travail distant :

```
ExcludeAllDevices   Enabled

IncludeVidPid       o:vid-0123_pid-abcd
```

Note Cet exemple de configuration fournit une protection, mais comme un périphérique compromis peut communiquer n'importe quel vid/pid, une attaque peut toujours éventuellement se produire.

Par défaut, Horizon interdit la redirection de certaines familles de périphériques vers l'application ou le poste de travail distant. Par exemple, les périphériques d'interface utilisateur et les claviers sont interdits d'affichage dans l'invité. Certains codes BadUSB récemment publiés ciblent les claviers USB.

Vous pouvez interdire la redirection de familles spécifiques de périphériques vers l'application ou le poste de travail distant. Par exemple, vous pouvez bloquer tous les périphériques vidéo, audio et de stockage de masse :

```
ExcludeDeviceFamily   o:video;audio;storage
```

À l'inverse, vous pouvez créer une liste blanche interdisant la redirection de tous les périphériques mais autorisant l'utilisation d'une famille spécifique de périphériques. Par exemple, vous pouvez bloquer tous les périphériques à l'exception des périphériques de stockage :

```
ExcludeAllDevices     Enabled

IncludeDeviceFamily   o:storage
```

Un autre risque peut survenir lorsqu'un utilisateur distant se connecte à un poste de travail ou à une application et l'infecte. Vous pouvez empêcher l'accès USB à toute connexion Horizon provenant de l'extérieur du pare-feu de l'entreprise. Le périphérique USB peut être utilisé en interne, mais pas en externe.

Sachez que si vous bloquez le port TCP 32111 pour désactiver l'accès externe aux périphériques USB, la synchronisation de fuseau horaire ne fonctionnera pas, car le port 32111 est également utilisé pour la synchronisation de fuseau horaire. Pour les clients zéro, le trafic USB est intégré dans un canal virtuel sur le port UDP 4172. Comme le port 4172 est utilisé pour

le protocole d'affichage ainsi que pour la redirection USB, vous ne pouvez pas bloquer le port 4172. Si nécessaire, vous pouvez désactiver la redirection USB sur les clients zéro. Pour plus d'informations, reportez-vous à la documentation du produit client zéro et contactez son fournisseur.

La définition de stratégies pour bloquer certaines familles de périphériques ou des périphériques spécifiques peut contribuer à réduire les risques d'infection avec le logiciel malveillant BadUSB. Ces stratégies ne réduisent pas tous les risques, mais peuvent s'inscrire dans une stratégie de sécurité globale.

Ces stratégies sont incluses dans le fichier de modèle d'administration ADMX pour la configuration d'Horizon Agent (`vdm_agent.admx`). Pour plus d'informations, reportez-vous à la section *Configuration des fonctionnalités de poste de travail distant dans Horizon*.

Mesures de protection HTTP sur les Serveurs de connexion 9

emploie certaines mesures pour protéger la communication qui utilise le protocole HTTP.

Ce chapitre contient les rubriques suivantes :

- Normes IETF (Internet Engineering Task Force)
- Normes World Wide Web Consortium
- Autres mesures de protection
- Configurer des mesures de protection HTTP

Normes IETF (Internet Engineering Task Force)

Le Serveur de connexion est conforme à certaines normes IETF (Internet Engineering Task Force).

- La norme RFC 5746 Transport Layer Security (TLS) – Renegotiation Indication Extension, également appelée renégociation sécurisée, est activée par défaut.

  Note La renégociation initiée par le client est désactivée par défaut sur les Serveurs de connexion. Pour l'activer, modifiez la valeur de registre `[HKLM\SOFTWARE\VMware, Inc.\VMware VDM\plugins\wsnm\TunnelService\Params]JvmOptions` et supprimez **`-Djdk.tls.rejectClientInitiatedRenegotiation=true`** de la chaîne.

- La norme RFC 6797 HTTP Strict Transport Security (HSTS), également appelée sécurité du transport, est activée par défaut. Ce paramètre ne peut pas être désactivé.
- La norme RFC 7034 HTTP Header Field X-Frame-Options, également appelée contournement du détournement de clic, est activée par défaut. Vous pouvez la désactiver en ajoutant l'entrée `x-frame-options=OFF` au fichier `locked.properties`. Pour plus d'informations sur l'ajout de propriétés au fichier `locked.properties`, reportez-vous à Configurer des mesures de protection HTTP.

  Note Dans les versions antérieures à la version 7.2, la modification de cette option n'affectait pas les connexions à HTML Access.

- La vérification de l'origine RFC 6454, qui protège contre la falsification de requête intersites, est activée par défaut. Vous pouvez la désactiver en ajoutant l'entrée `checkOrigin=false` à `locked.properties`. Pour plus d'informations, reportez-vous à la section Partage des ressources cross-origin.

  Note Dans les versions antérieures, cette protection était désactivée par défaut.

HTTP Strict Transport Security

La fonctionnalité HTTP Strict Transport Security (HSTS) est un mécanisme de stratégie de sécurité qui permet de se protéger contre les attaques d'intercepteur en indiquant aux navigateurs Web qu'ils doivent utiliser uniquement le protocole HTTPS pour se connecter.

L'en-tête est ajouté à toutes les réponses HTTP sur le port 443, spécifiant une durée de vie d'un an. Des propriétés facultatives peuvent être définies en ajoutant des hstsFlags de propriété à valeurs multiples au fichier locked.properties. Les valeurs suivantes peuvent être définies.

Propriété	Valeur
includeSubDomains	S'applique à tous les sous-domaines de ce site.
preload	Indication pour inclure ce site dans les listes de préchargement HSTS.

Note Ces propriétés ne sont pas définies par défaut, car elles peuvent également affecter les URL non-Horizon. Ne les définissez pas si vous n'en comprenez pas les implications.

Normes World Wide Web Consortium

Le Serveur de connexion est conforme à certaines normes World Wide Web Consortium (W3).

- Le partage des ressources cross-origin (CORS) contraint les demandes cross-origin côté client. Vous pouvez l'activer en ajoutant l'entrée `enableCORS=true` ou le désactiver en ajoutant l'entrée `enableCORS=false` à `locked.properties`.
- La stratégie de sécurité de contenu (CSP), qui corrige de nombreuses vulnérabilités d'injection de contenu, est activée par défaut. Vous pouvez la désactiver en ajoutant l'entrée `enableCSP=false` à `locked.properties`.

Partage des ressources cross-origin

La fonctionnalité de partage des ressources cross-origin (CORS) régule les demandes cross-origin côté client en fournissant des déclarations de stratégie au client à la demande et en vérifiant les demandes pour assurer la conformité avec la stratégie. Cette fonctionnalité peut être configurée et activée si nécessaire.

Les stratégies incluent l'ensemble des méthodes HTTP à l'origine des demandes qui peuvent être acceptées, ainsi que les types de contenu valides. Ces stratégies varient en fonction de l'URL de demande et peuvent être reconfigurées selon vos besoins en ajoutant des entrées au fichier `locked.properties`.

Les points de suspension après un nom de propriété indiquent que la propriété peut accepter une liste.

Tableau 9-1. Propriétés de CORS

Propriété	Type de valeur	Valeur maître par défaut	Autres valeurs par défaut
`enableCORS`	`true` `false`	`true`	`n/a`
`acceptContentType ...`	`http-content-type`	`application/x-www-form-urlencoded,application/xml,text/xml`	`admin`=application/json,application/text,application/x-www-form-urlencoded `portal`=application/json `rest`=application/json `sse`=application/json `view-vlsi-rest`=application/json

Tableau 9-1. Propriétés de CORS (suite)

Propriété	Type de valeur	Valeur maître par défaut	Autres valeurs par défaut
acceptHeader...	http-header-name	*	admin=Accept,Accept-Encoding,Accept-Charset,Accept-Language,Authorization,Cache-Control,Connection,Content-Language,Content-Length,Content-Type,Cookie,csrftoken,DNT,Host,Origin,Referer,User-Agent broker=Accept,Accept-Encoding,Accept-Charset,Accept-Language,Authorization,Connection,Content-Language,Content-Length,Content-Type,Cookie,Gateway-Location,Gateway-Name,Gateway-Type,Host,Origin,Referer,User-Agent,X-CSRF-Token,X-EUC-Gateway,X-EUC-Health,X-Forwarded-For,X-Forwarded-Host,X-Forwarded-Proto portal=Accept,Accept-Encoding,Accept-Charset,Accept-Language,Authorization,Connection,Content-Language,Content-Length,Content-Type,Cookie,Host,Origin,Referer,User-Agent,X-CSRF-Token rest=Accept,Accept-Encoding,Accept-Charset,Accept-Language,Authorization,Connection,Content-Language,Content-Length,Content-Type,Cookie,csrfToken,Host,Origin,Referer,User-Agent,X-Require-Cloud-Admin-Privilege view-vlsi=Accept,Accept-Encoding,Accept-Charset,Accept-Language,Authorization,Connection,Content-Language,Content-Length,Content-Type,Cookie,csrfToken,Host,Origin,Referer,User-Agent,X-Require-Cloud-Admin-Privilege view-vlsi-rest=Accept,Accept-Encoding,Accept-Charset,Accept-Language,Authorization,Connection,Content-Language,Content-Length,Content-Type,Cookie,csrfToken,Host,Origin,Referer,User-Agent,X-Require-Cloud-Admin-Privilege

Tableau 9-1. Propriétés de CORS (suite)

Propriété	Type de valeur	Valeur maître par défaut	Autres valeurs par défaut
exposeHeader...	http-header-name	*	n/a
filterHeaders	true false	true	n/a
checkOrigin	true false	true	n/a
checkReferer	true false	false	n/a
allowCredentials	true false	false	admin =true broker=true health=true misc =true portal=true rest=true saml=true sse=true tunnel=true view-vlsi=true view-vlsi-rest=true
allowMethod...	http-method-name	GET,HEAD,POST	health =GET,HEAD misc =GET,HEAD rest=GET,POST,PUT, PATCH,DELETE saml =GET,HEAD sse=GET,POST tunnel=GET,POST
allowPreflight	true false	true	n/a
maxAge	cache-time	0	n/a
balancedHost	load-balancer-name	OFF	n/a
portalHost...	gateway-name	OFF	n/a
chromeExtension...	chrome-extension-hash	ppkfnjlimknmjoaemnpidmdlfchhehel **Note** Cette valeur est l'ID d'extension de Chrome pour Horizon Client pour Chrome.	n/a

Voici des exemples de propriétés CORS dans le fichier `locked.properties`.

```
enableCORS = true
allowPreflight = true
```

```
checkOrigin = true
checkOrigin-misc = false
allowMethod.1 = GET
allowMethod.2 = HEAD
allowMethod.3 = POST
allowMethod-saml.1 = GET
allowMethod-saml.2 = HEAD
acceptContentType.1 = application/x-www-form-urlencoded
acceptContentType.2 = application/xml
acceptContentType.3 = text/xml
```

Vérification de l'origine

La vérification de l'origine est activée par défaut. Lorsqu'elle est activée, une demande est acceptée uniquement sans origine, ou avec une origine égale à l'adresse spécifiée par l'URL externe, à l'adresse `balancedHost`, à n'importe quelle adresse `portalHost`, à n'importe quel hachage `chromeExtension`, à `null` ou à `localhost`. Si l'origine ne correspond à aucune de ces valeurs, l'erreur « Origine inattendue » est journalisée et l'état 404 est renvoyé.

Note Certains navigateurs ne fournissent pas un en-tête Origine ou n'en fournissent pas toujours un. Éventuellement, l'en-tête Référent dans une demande peut être vérifié en l'absence d'en-tête Origine. L'en-tête Référent comporte un « r » dans le nom d'en-tête. Pour vérifier l'en-tête Référent, ajoutez la propriété suivante au fichier `locked.properties` :

```
checkReferer=true
```

Si plusieurs hôtes du Serveur de connexion sont à équilibrage de charge, vous devez spécifier l'adresse de l'équilibrage de charge en ajoutant une entrée `balancedHost` au fichier `locked.properties`. Le port 443 est utilisé pour cette adresse.

Si les clients se connectent via un dispositif Unified Access Gateway ou une autre passerelle, vous devez spécifier toutes les adresses de passerelle en ajoutant des entrées `portalHost` au fichier `locked.properties`. Le port 443 est utilisé pour ces adresses. Vous devez également spécifier des entrées `portalHost` pour fournir l'accès à un hôte du Serveur de connexion par le biais d'un nom différent de celui spécifié par l'URL externe.

Les clients d'extension Chrome définissent leur origine initiale sur leur propre identité. Pour que les connexions aboutissent, enregistrez l'extension en ajoutant une entrée `chromeExtension` au fichier `locked.properties`. Par exemple :

```
chromeExtension.1=bpifadopbphhpkkcfohecfadckmpjmjd
```

Stratégie de sécurité de contenu

La fonctionnalité de stratégie de sécurité de contenu (CSP) corrige de nombreuses vulnérabilités d'injection de contenu, par exemple le script de site à site (XSS), en fournissant des directives de stratégie aux navigateurs compatibles. Cette fonctionnalité est activée par défaut. Vous pouvez reconfigurer les directives de stratégie en ajoutant des entrées à `locked.properties`.

Tableau 9-2. Propriétés de CSP

Propriété	Type de valeur	Valeur maître par défaut	Autres valeurs par défaut
enableCSP	true false	true	n/a
content-security-policy	directives-list	default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe-eval' data:;style-src 'self' 'unsafe-inline';font-src 'self' data: ;frame-ancestors 'none'	admin=default-src 'self' https://feedback.esp.vmware.com; script-src https://feedback.esp.vmware.com https://lumos.vmware.com 'unsafe-inline' 'unsafe-eval';style-src 'self' 'unsafe-inline';font-src 'self' data:;img-src 'self' data:;connect-src 'self' https:;frame-ancestors 'none' portal=default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe-eval' data:;style-src 'self' 'unsafe-inline';font-src 'self' data:;img-src 'self' data: blob:;media-src 'self' blob:;connect-src 'self' wss:;frame-src 'self' blob:;child-src 'self' blob:;object-src 'self' blob:;frame-ancestors 'self' rest = default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe-eval' data:;style-src 'self' 'unsafe-inline';font-src 'self' data:;img-src 'self' data:;connect-src 'self' https:;frame-ancestors 'none'
x-content-type-options	OFF specification	nosniff	n/a
x-frame-options	OFF specification	deny	portal = sameorigin
x-xss-protection	OFF specification	1; mode=block	n/a

Vous pouvez ajouter des propriétés de CSP au fichier `locked.properties`. Exemples de propriétés de CSP :

```
enableCSP = true
content-security-policy = default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe-eval'
data:;style-src 'self'
 'unsafe-inline';font-src 'self' data:
content-security-policy-newadmin = default-src 'self';script-src 'self' 'unsafe-inline'
'unsafe-eval' data:;style-src 'self'
 'unsafe-inline';font-src 'self' data:;img-src 'self' data:;connect-src 'self' https:
content-security-policy-portal = default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe-
eval' data:;style-src 'self'
'unsafe-inline';font-src 'self' data:;img-src 'self' data: blob:;media-src 'self'
blob:;connect-src 'self' wss:;frame-src
'self' blob:;child-src 'self' blob:;object-src 'self' blob:
x-content-type-options = nosniff
x-frame-options = deny
x-frame-options-portal = sameorigin
x-xss-protection = 1; mode=block
```

Autres mesures de protection

Outre les normes IETF (Internet Engineering Task Force) et W3, VMware Horizon emploie d'autres mesures pour protéger les communications utilisant le protocole HTTP.

Réduction des risques de sécurité de type MIME

Par défaut, VMware Horizon envoie l'en-tête `x-content-type-options: nosniff` dans ses réponses HTTP pour permettre d'éviter les attaques basées sur une confusion de type MIME.

Vous pouvez désactiver cette fonction en ajoutant l'entrée suivante au fichier `locked.properties` :

```
x-content-type-options=OFF
```

Réduction des attaques de script entre sites

Par défaut, VMware Horizon utilise la fonction de filtre XSS (script entre sites) pour réduire les attaques de script entre sites en envoyant l'en-tête `x-xss-protection=1; mode=block` dans ses réponses HTTP.

Vous pouvez désactiver cette fonction en ajoutant l'entrée suivante au fichier `locked.properties` :

```
x-xss-protection=OFF
```

Vérification du type de contenu

Par défaut, VMware Horizon accepte les demandes avec les types de contenu déclaré suivants uniquement :

- application/x-www-form-urlencoded
- application/xml
- text/xml

Note Dans les versions antérieures, cette protection était désactivée par défaut.

Pour limiter les types de contenu acceptés par VMware Horizon, ajoutez l'entrée suivante au fichier `locked.properties` :

```
acceptContentType.1=content-type
```

Par exemple :

```
acceptContentType.1=x-www-form-urlencoded
```

Pour accepter un autre type de contenu, ajoutez l'entrée `acceptContentType.2=content-type`, etc.

Pour accepter les demandes avec n'importe quel type de contenu déclaré, spécifiez `acceptContentType=*`.

Surveillance de comportement du client

Les Serveurs de connexion disposent de ressources limitées pour traiter les demandes des clients, et les clients avec un mauvais comportement peuvent accaparer ces ressources, empêchant ainsi les autres d'y accéder. La surveillance du comportement du client est une classe de détections et d'atténuations qui protègent contre un mauvais comportement.

Surveillance des négociations

Les négociations TLS sur le port 443 doivent se terminer dans une période configurable, sinon elles seront terminées de force. Par défaut, cette période est de 10 secondes. Si l'authentification par carte à puce est activée, les négociations TLS sur le port 443 peuvent s'exécuter en 100 secondes.

Si nécessaire, vous pouvez régler l'heure des négociations TLS sur le port 443 en ajoutant la propriété suivante au fichier `locked.properties` :

```
handshakeLifetime = lifetime_in_seconds
```

Par exemple :

```
handshakeLifetime = 20
```

Éventuellement, le client responsable d'une négociation TLS qui dépasse la durée peut être automatiquement ajouté à une liste noire. Pour plus d'informations, reportez-vous à la section Mise sur liste noire du client.

Surveillance de la réception des demandes

Les demandes HTTP doivent être entièrement reçues dans les 30 secondes. Sinon, la connexion sera arrêtée de force.

Éventuellement, un client qui dépasse le délai d'envoi d'une demande peut être automatiquement ajouté à une liste noire. Pour plus d'informations, reportez-vous à la section Mise sur liste noire du client.

Comptage des demandes

Un client unique n'est pas censé envoyer plus de 100 demandes HTTP par minute, bien que par défaut aucune action ne soit effectuée si ce seuil est dépassé.

Éventuellement, un client qui dépasse ce seuil peut être automatiquement ajouté à une liste noire. Pour plus d'informations, reportez-vous à la section Mise sur liste noire du client.

Si la mise sur liste noire du client a été activée, vous devrez peut-être configurer les seuils de comptage des demandes.

Vous pouvez ajuster le nombre maximal de demandes HTTP traitées par client en ajoutant la propriété suivante au fichier `locked.properties` :

```
requestTallyThreshold = max_served_requests_in_30_seconds
```

Exemple :

```
requestTallyThreshold = 100
```

Vous pouvez ajuster le nombre maximal de demandes HTTP ayant échoué par client en ajoutant la propriété suivante au fichier `locked.properties` :

```
 tarPitGraceThreshold = max_failed_requests_in_30_seconds
```

Exemple :

```
 tarPitGraceThreshold = 5
```

Mise sur liste noire du client

Ce type de protection est désactivé par défaut, car cela peut réduire les performances et gêner les utilisateurs s'il n'est pas correctement configuré. N'activez pas la mise sur liste noire du client si vous utilisez une passerelle, telle qu'un dispositif Unified Access Gateway, qui présente toutes les connexions clientes en tant que même adresse IP.

Si cette option est activée, les connexions des clients sur la liste noire sont retardées pendant une période configurable avant le traitement. Si plusieurs connexions du même client sont retardées simultanément, d'autres connexions de ce client sont refusées, plutôt que retardées. Ce seuil est configurable.

Vous pouvez activer cette fonctionnalité en ajoutant la propriété suivante au fichier `locked.properties` :

```
secureHandshakeDelay = delay_in_milliseconds
```

Par exemple :

```
secureHandshakeDelay = 2000
```

Pour désactiver la mise sur liste noire des connexions HTTPS, supprimez l'entrée `secureHandshakeDelay` ou définissez-la sur 0.

Lorsqu'une négociation TLS dépasse la durée, l'adresse IP du client est ajoutée à la liste noire pendant une période minimale égale à la somme de `handshakeLifetime` et de `secureHandshakeDelay`.

En utilisant les valeurs des exemples ci-dessus, l'adresse IP d'un client avec un mauvais comportement est mise sur liste noire pendant 22 secondes.

```
(20 * 1000) + 2000 = 22 seconds
```

La période minimale est étendue chaque fois qu'une connexion à partir de la même adresse IP a un mauvais comportement. Une fois que la période minimale a expiré et que la dernière connexion retardée à partir de cette adresse IP est traitée, l'adresse IP est supprimée de la liste noire.

Une négociation TLS qui dépasse la durée n'est pas la seule raison pour mettre un client sur liste noire. Les autres raisons incluent une série de connexions abandonnées ou une série de demandes se terminant par erreur, telles que plusieurs tentatives pour accéder à des URL inexistantes. Ces déclencheurs ont des périodes de mise sur liste noire minimales différentes. Pour étendre la surveillance de ces déclencheurs supplémentaires au port 80, ajoutez l'entrée suivante au fichier `locked.properties` :

```
insecureHandshakeDelay = delay_in_milliseconds
```

Par exemple :

```
insecureHandshakeDelay = 1000
```

Pour désactiver la mise sur liste noire des connexions HTTP, supprimez l'entrée `insecureHandshakeDelay` ou définissez-la sur 0.

Propriétés de la surveillance de comportement

Utilisez ces propriétés pour surveiller le comportement du client. Elles incluent des propriétés pour les détections et les atténuations qui protègent contre un mauvais comportement.

Tableau 9-3. Propriétés de la surveillance de comportement

Propriété	Description	Valeur par défaut	Dynamique
`handshakeLifetime`	Délai maximal pour la négociation TLS, en secondes.	10 ou 100 (reportez-vous à la section Surveillance des négociations.)	Non
`secureHandshakeDelay`	Délai avant la négociation TLS lors de la mise sur liste noire, en millisecondes.	0 (mise sur liste noire désactivée)	Non
`insecureHandshakeDelay`	Délai avant la négociation non-TLS lors de la mise sur liste noire, en millisecondes.	0 (mise sur liste noire désactivée)	Non
`requestTallyThreshold`	Demandes HTTP traitées par période de 30 secondes pour la mise sur liste noire du client.	50	Non
`tarPitGraceThreshold`	Demandes HTTP non traitées par période de 30 secondes pour la mise sur liste noire du client.	3	Non
`secureBlacklist...`	Liste d'adresses IP sur le port 443 à rejeter immédiatement lors de la mise sur liste noire.	s/o	Oui
`insecureBlacklist...`	Liste d'adresses IP sur le port 80 à rejeter immédiatement lors de la mise sur liste noire.	s/o	Oui
`secureWhitelist...`	Liste d'adresses IP sur le port 443 à exclure de la mise sur liste noire.	s/o	Oui
`insecureWhitelist...`	Liste d'adresses IP sur le port 80 à exclure de la mise sur liste noire.	s/o	Oui

Les modifications apportées aux entrées dynamiques s'appliqueront immédiatement, sans un redémarrage du service.

Mise en liste blanche d'agents d'utilisateur

Définissez une liste blanche pour restreindre les agents d'utilisateur pouvant interagir avec VMware Horizon. Par défaut, tous les agents d'utilisateur sont acceptés.

Note Il ne s'agit pas à proprement parler d'une fonctionnalité de sécurité. La détection d'agent d'utilisateur repose sur l'en-tête de demande d'agent utilisateur fourni par le client ou le navigateur se connectant, qui peut être usurpé. Certains navigateurs autorisent les utilisateurs à modifier l'en-tête de demande.

Un agent d'utilisateur est spécifié par son nom et une version minimale. Par exemple :

```
clientWhitelist-portal.1 = Chrome-14
clientWhitelist-portal.2 = Safari-5.1
```

Cela signifie que seuls Google Chrome 14 et versions ultérieures et Safari 5.1 et versions ultérieures sont autorisés à se connecter à l'aide de HTML Access. Tous les navigateurs peuvent se connecter à d'autres services.

Vous pouvez entrer les noms d'agent d'utilisateur reconnus suivants :

- Android
- Chrome
- Edge
- IE
- Firefox
- Opera
- Safari

Note Ces agents d'utilisateur ne sont pas tous pris en charge par VMware Horizon. Voici des exemples.

Configurer des mesures de protection HTTP

Pour configurer des mesures de protection HTTP, vous devez créer ou modifier le fichier `locked.properties` dans le dossier de configuration de la passerelle sur l'instance du Serveur de connexion.

Par exemple : *`install_directory`*`\VMware\VMware View\Server\sslgateway\conf\locked.properties`

- Utilisez la syntaxe suivante pour configurer une propriété dans `locked.properties` :

  ```
  myProperty = newValue
  ```

- Le nom de propriété est toujours sensible à la casse et la valeur peut l'être. Un espace blanc autour du signe = est facultatif.
- Pour les propriétés de CORS et de CSP, il est possible de définir des valeurs spécifiques au service ainsi qu'une valeur maître. Par exemple, le service d'administration est chargé de la gestion des demandes d'Horizon Console. Vous pouvez alors définir une propriété pour ce service sans affecter les autres services en ajoutant `-admin` après le nom de propriété.

  ```
  myProperty-admin = newValueForAdmin
  ```

- Si une valeur maître et une valeur spécifique au service sont spécifiées, la valeur spécifique au service s'applique au service nommé, et la valeur maître s'applique à tous les autres services. La seule exception est la valeur spéciale OFF. Si la valeur maître d'une propriété est définie sur OFF, toutes les valeurs spécifiques au service pour cette propriété sont ignorées.

  Par exemple :

  ```
  myProperty = OFF
  myProperty-admin = newValueForAdmin    ; ignored
  ```

- Certaines propriétés peuvent accepter une liste de valeurs.

  Pour définir une valeur unique, entrez la propriété suivante :

  ```
  myProperty = newValue
  myProperty-admin = newValueForAdmin
  ```

  Pour définir plusieurs valeurs pour une propriété qui accepte des valeurs de liste, vous pouvez spécifier chaque valeur sur une ligne distincte :

  ```
  myProperty.1 = newValue1
  myProperty.2 = newValue2
  myProperty-admin.1 = newValueForAdmin1
  myProperty-admin.2 = newValueForAdmin2
  ```

- Pour déterminer le nom de service correct à utiliser lors d'une configuration spécifique au service, recherchez dans les journaux de débogage les lignes contenant la séquence suivante :

  ```
  (ajp:admin:Request21) Request from abc.def.com/10.20.30.40: GET /admin/
  ```

  Dans cet exemple, le nom du service est `admin`. Vous pouvez utiliser les noms de service par défaut suivants :

  - `newadmin` pour Horizon Console
  - `broker` pour le Serveur de connexion
  - `docroot` pour le service de fichier local
  - `portal` pour HTML Access

- `saml` pour la communication SAML (vIDM)
- `tunnel` pour le tunnel sécurisé
- `view-vlsi` pour View API
- `misc` pour d'autres
- `rest` pour l'API REST