

Sécurité de View

VMware Horizon 6
Version 6.2

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

FR-001910-01

vmware[®]

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

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

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

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

docfeedback@vmware.com

Copyright © 2015 VMware, Inc. Tous droits réservés. [Copyright et informations sur les marques.](#)

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

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

Table des matières

Sécurité de View	5
1 Référence sur la sécurité de View	7
Comptes View	7
Paramètres de sécurité de View	8
Ressources de View	18
Fichiers journaux de View	19
Ports TCP et UDP de View	20
Services sur un hôte du Serveur de connexion View	24
Services sur un serveur de sécurité	25
Configuration des protocoles de sécurité et des suites de chiffrement sur une instance de Serveur de connexion View ou sur un serveur de sécurité	26
Déploiement de périphériques USB dans un environnement View sécurisé	32
Index	35

Sécurité de View

Sécurité de View fournit une référence succincte sur les fonctionnalités de sécurité de VMware Horizon 6™.

- 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 View.

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 View.

Référence sur la sécurité de View

Lorsque vous configurez un environnement View sécurisé, vous pouvez modifier les paramètres et procéder à des réglages dans plusieurs zones afin de protéger vos systèmes.

Ce chapitre aborde les rubriques suivantes :

- [« Comptes View », page 7](#)
- [« Paramètres de sécurité de View », page 8](#)
- [« Ressources de View », page 18](#)
- [« Fichiers journaux de View », page 19](#)
- [« Ports TCP et UDP de View », page 20](#)
- [« Services sur un hôte du Serveur de connexion View », page 24](#)
- [« Services sur un serveur de sécurité », page 25](#)
- [« Configuration des protocoles de sécurité et des suites de chiffrement sur une instance de Serveur de connexion View ou sur un serveur de sécurité », page 26](#)
- [« Déploiement de périphériques USB dans un environnement View sécurisé », page 32](#)

Comptes View

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

Tableau 1-1. Comptes système View

Composant de View	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 View.
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 View. Pour plus d'informations sur les privilèges requis, reportez-vous au document <i>Installation de View</i> .

Tableau 1-1. Comptes système View (suite)

Composant de View	Comptes requis
View Composer	<p>Créez un compte d'utilisateur dans Active Directory à utiliser avec View Composer. View Composer a besoin de ce compte pour associer des postes de travail de clone lié à votre domaine Active Directory.</p> <p>Le compte d'utilisateur ne doit pas être un compte d'administration View. Donnez au compte les privilèges minimum qu'il requiert pour créer et supprimer des objets ordinateur dans un conteneur Active Directory spécifié. Par exemple, le compte ne requiert pas de privilèges d'administrateur de domaine.</p> <p>Pour plus d'informations sur les privilèges requis, reportez-vous au document <i>Installation de View</i>.</p>
Serveur de connexion View	<p>Lorsque vous installez View, 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 View. Nous vous recommandons de créer un groupe d'utilisateurs de domaine dédié d'administrateurs View. L'utilisateur par défaut est l'utilisateur de domaine actuellement connecté.</p> <p>Dans View Administrator, vous pouvez utiliser Configuration de View > Administrateurs pour modifier la liste des administrateurs View.</p> <p>Pour plus d'informations sur les privilèges requis, reportez-vous au document <i>Administration de View</i>.</p>

Tableau 1-2. Comptes de base de données View

Composant de View	Comptes requis
base de données View Composer	<p>Une base de données SQL Server ou Oracle stocke des données View Composer. Vous créez un compte d'administration pour la base de données que vous pouvez associer au compte d'utilisateur View Composer.</p> <p>Pour plus d'informations sur la configuration d'une base de données View Composer, reportez-vous au document <i>Installation de View</i>.</p>
Base de données des événements utilisée par le Serveur de connexion View	<p>Une base de données SQL Server ou Oracle stocke des données d'événements View. Vous créez un compte d'administration pour la base de données que View Administrator peut utiliser afin d'accéder aux données d'événements.</p> <p>Pour plus d'informations sur la configuration d'une base de données View Composer, reportez-vous au document <i>Installation de View</i>.</p>

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

- Configurez les bases de données View 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 des comptes séparés pour accéder aux bases de données View Composer et des événements.

Paramètres de sécurité de View

View inclut plusieurs paramètres que vous pouvez utiliser pour régler la sécurité de la configuration. Vous pouvez accéder aux paramètres en utilisant View Administrator, en modifiant des profils de groupe ou en utilisant l'utilitaire Éditeur ADSI, si nécessaire.

Paramètres généraux liés à la sécurité dans View Administrator

Les paramètres généraux relatifs à la sécurité des sessions et des connexions au client sont accessibles sous **Configuration de View > Paramètres généraux** dans View Administrator.

Tableau 1-3. Paramètres généraux liés à la sécurité

Paramètre	Description
Modifier le mot de passe de récupération de données	<p>Le mot de passe est requis lorsque vous restaurez la configuration View LDAP à partir d'une sauvegarde cryptée.</p> <p>Lorsque vous installez Serveur de connexion View version 5.1 ou supérieure, vous fournissez un mot de passe de récupération de données. Après l'installation, vous pouvez modifier ce mot de passe dans View Administrator.</p> <p>Lorsque vous sauvegardez Serveur de connexion View, la configuration de View LDAP est exportée sous forme de données LDIF cryptées. Pour restaurer la sauvegarde cryptée avec l'utilitaire <code>vdmimport</code>, 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.</p>
Mode de sécurité des messages	<p>Détermine le mécanisme de sécurité utilisé lorsque des messages JMS sont transmis entre composants View.</p> <ul style="list-style-type: none"> ■ 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 View rejettent les messages non signés. Ce mode prend en charge une combinaison de connexions SSL et JMS en texte brut. ■ S'il est défini sur Amélioré, SSL 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 View peuvent échanger des messages. ■ Si le paramètre est réglé sur Mélangé, le mode de sécurité des messages est activé, mais pas appliqué pour les composants View qui précèdent View Manager 3.0. <p>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.</p> <p>IMPORTANT VMware recommande vivement de régler le mode de sécurité des messages sur Amélioré après la mise à niveau de toutes les instances du Serveur de connexion View, des serveurs de sécurité et des postes de travail View 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).</p>
État de sécurité amélioré (lecture seule)	<p>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 :</p> <ul style="list-style-type: none"> ■ 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 View de l'espace ou le service Composant du bus de message VMware Horizon View sur tous les hôtes de Serveur de connexion View de l'espace. ■ Amélioré en attente est l'état suivant. Dès que tous les services Composant du bus de messages View ont été redémarrés, le système commence à modifier le mode de sécurité des messages sur Amélioré pour tous les postes de travail et serveurs de sécurité. ■ Amélioré est l'état final, indiquant que tous les composants utilisent maintenant le mode de sécurité des messages Amélioré.
Authentifier à nouveau les connexions par tunnel sécurisé après une interruption de réseau	<p>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 View à l'aide d'un tunnel sécurisé.</p> <p>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 View, car la connexion réseau a été temporairement interrompue.</p> <p>Ce paramètre est désactivé par défaut.</p>
Forcer la déconnexion des utilisateurs	<p>Déconnecte tous les postes de travail et toutes les applications une fois le nombre de minutes spécifié écoulé depuis l'ouverture de la session utilisateur sur View. 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.</p> <p>La valeur par défaut est de 600 minutes.</p>

Tableau 1-3. Paramètres généraux liés à la sécurité (suite)

Paramètre	Description
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	<p>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, View, 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.</p> <p>Si ce paramètre est défini sur Jamais, View ne déconnecte jamais les applications et n'ignore jamais les informations d'identification SSO suite à l'inactivité de l'utilisateur.</p> <p>La valeur par défaut est Jamais.</p>
Autres clients. Supprimer les informations d'identification SSO	<p>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 View, quelle que soit son activité sur le périphérique client.</p> <p>La valeur par défaut est Après 15 minutes.</p>
Activer IPSec pour le couplage du serveur de sécurité	<p>Détermine s'il est nécessaire d'utiliser IPSec (Internet Protocol Security) pour les connexions entre des serveurs de sécurité et des instances de Serveur de connexion View. Ce paramètre doit être désactivé avant d'installer un serveur de sécurité en mode FIPS ; sinon le couplage échoue.</p> <p>Par défaut, IPSec pour les connexions du serveur de sécurité est activé.</p>
Délai d'expiration de la session de View Administrator	<p>Détermine la durée pendant laquelle une session View Administrator inactive continue avant d'expirer.</p> <p>IMPORTANT Définir le délai d'expiration de la session View Administrator sur un nombre de minutes élevé augmente le risque d'utilisation non autorisée de View Administrator. Soyez prudent lorsque vous autorisez une session inactive à durer longtemps.</p> <p>Par défaut, le délai d'expiration de la session View Administrator est de 30 minutes. Vous pouvez définir un délai d'expiration de session compris entre 1 et 4 320 minutes.</p>

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

REMARQUE SSL est requis pour toutes les connexions d'Horizon Client et de View Administrator à View. Si votre déploiement de View utilise des équilibrateurs de charge ou d'autres serveurs intermédiaires client, vous pouvez télécharger SSL sur eux et configurer des connexions non-SSL sur des instances de Serveur de connexion View et des serveurs de sécurité individuels. Voir « Télécharger des connexions SSL sur des serveurs intermédiaires » dans le document *Administration de View*.

Paramètres de serveur liés à la sécurité dans View Administrator

Les paramètres de serveur relatifs à la sécurité sont accessibles sous **Configuration de View > Serveurs** dans View Administrator.

Tableau 1-4. 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 autre connexion sécurisée au Serveur de connexion View ou à l'hôte du serveur de sécurité lorsque les utilisateurs se connectent à des postes de travail et des applications View 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 View ou l'hôte des services Bureau à distance (Remote Desktop Services, RDS), contournant ainsi le Serveur de connexion View ou l'hôte du serveur de sécurité. Ce paramètre est désactivé par défaut.
Utiliser une connexion par tunnel sécurisé à la machine	Détermine si Horizon Client établit une autre connexion HTTPS au Serveur de connexion View ou à l'hôte du serveur de sécurité lorsque l'utilisateur se connecte à un poste de travail ou à une application de View. 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 View ou l'hôte des services Bureau à distance (Remote Desktop Services, RDS), contournant ainsi le Serveur de connexion View ou l'hôte du serveur de sécurité. Ce paramètre est activé par défaut.
Utiliser Blast Secure Gateway pour un HTML Access à la machine	Détermine si les clients qui accèdent à des postes de travail à l'aide d'un navigateur Web utilisent Blast Secure Gateway pour établir un tunnel sécurisé avec le Serveur de connexion View. S'il est désactivé, les navigateurs Web établissent des connexions directes aux postes de travail View, en contournant le Serveur de connexion View. 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 de View*.

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

Les paramètres liés à la sécurité sont fournis dans le fichier de modèle d'administration pour View Agent (`vdm_agent.adm`). Sauf indication contraire, les paramètres comprennent uniquement un paramètre Configuration ordinateur.

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

Tableau 1-5. Paramètres liés à la sécurité dans le modèle pour la configuration de View Agent

Paramètre	Description
AllowDirectRDP	<p>Détermine si des clients non-Horizon Client peuvent se connecter directement aux postes de travail View via RDP. Lorsque ce paramètre est désactivé, View Agent autorise uniquement les connexions gérées par View via Horizon Client. Par défaut, lorsqu'un utilisateur a ouvert une session de poste de travail View, vous pouvez utiliser RDP pour vous connecter à la machine virtuelle à l'extérieur de View. La connexion RDP met fin à la session du poste de travail View et les données et paramètres non enregistrés de l'utilisateur View risquent d'être perdus. L'utilisateur View ne peut pas se connecter au poste de travail tant que la connexion RDP externe est fermée. Pour éviter cette situation, désactivez le paramètre AllowDirectRDP.</p> <p>IMPORTANT Pour que View fonctionne correctement, les services Bureau à distance doivent s'exécuter sur le système d'exploitation invité de chaque poste de travail. Vous pouvez utiliser ce paramètre pour empêcher les utilisateurs de faire des connexions RDP directes sur leurs postes de travail.</p> <p>Ce paramètre est activé par défaut.</p> <p>La valeur de Registre Windows équivalente est AllowDirectRDP.</p>
AllowSingleSignon	<p>Détermine si l'authentification unique (Single Sign-On, SSO) est utilisée pour connecter les utilisateurs aux postes de travail et aux applications. Lorsque ce paramètre est activé, l'utilisateur doit entrer uniquement ses informations d'identification lorsqu'il se connecte à Horizon Client. Lorsqu'il est désactivé, les utilisateurs doivent s'authentifier de nouveau lorsque la connexion à distance est effectuée.</p> <p>Ce paramètre est activé par défaut.</p> <p>La valeur de Registre Windows équivalente est AllowSingleSignon.</p>
CommandsToRunOnConnect	<p>Spécifie une liste de commandes ou de scripts de commande à exécuter lorsqu'une session est connectée pour la première fois.</p> <p>Aucune liste n'est spécifiée par défaut.</p> <p>La valeur de Registre Windows équivalente est CommandsToRunOnConnect.</p>
CommandsToRunOnReconnect	<p>Spécifie une liste de commandes ou de scripts de commande à exécuter lorsqu'une session est reconnectée après une déconnexion.</p> <p>Aucune liste n'est spécifiée par défaut.</p> <p>La valeur de Registre Windows équivalente est CommandsToRunOnReconnect.</p>
CommandsToRunOnDisconnect	<p>Spécifie la liste des commandes ou des scripts de commande à exécuter lorsqu'une session est déconnectée.</p> <p>Aucune liste n'est spécifiée par défaut.</p> <p>La valeur de Registre Windows équivalente est CommandsToRunOnDisconnect.</p>
ConnectionTicketTimeout	<p>Spécifie la durée en secondes pendant laquelle le ticket de connexion View est valide.</p> <p>Si ce paramètre n'est pas configuré, le délai d'expiration par défaut est de 120 secondes.</p> <p>La valeur de Registre Windows équivalente est VdmConnectionTicketTimeout.</p>
CredentialFilterExceptions	<p>Spécifie les fichiers exécutables qui ne sont pas autorisés à charger l'agent CredentialFilter. Les noms de fichier ne doivent pas contenir de chemin d'accès ou de suffixe. Utilisez un point-virgule pour séparer plusieurs noms de fichier.</p> <p>Aucune liste n'est spécifiée par défaut.</p> <p>La valeur de Registre Windows équivalente est CredentialFilterExceptions.</p>

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

Paramètres de sécurité du modèle de configuration d' Horizon Client

Les paramètres liés à la sécurité sont fournis dans le fichier de modèle d'administration d'Horizon Client (`vdm_client.adm`). Sauf indication contraire, les paramètres comprennent uniquement un paramètre Configuration ordinateur. Si un paramètre Configuration utilisateur est disponible et si vous lui définissez une valeur, il remplace le paramètre Configuration ordinateur équivalent.

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

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

Tableau 1-6. Modèle de configuration d' Horizon Client : paramètres de sécurité

Paramètre	Description
Allow command line credentials (Paramètre de Configuration d'ordinateur)	<p>Détermine si les informations d'identification d'utilisateur peuvent être fournies avec des options de ligne de commande d'Horizon Client. Si ce paramètre est désactivé, les options <code>smartCardPIN</code> et <code>password</code> ne sont pas disponibles lorsque les utilisateurs exécutent Horizon Client à partir de la ligne de commande.</p> <p>Ce paramètre est activé par défaut.</p> <p>La valeur de Registre Windows équivalente est <code>AllowCmdLineCredentials</code>.</p>
Servers Trusted For Delegation (Paramètre de Configuration d'ordinateur)	<p>Spécifie les instances de Serveur de connexion View qui acceptent l'identité et les informations d'identification d'utilisateur qui sont transmises quand un utilisateur coche la case Log in as current user (Se connecter en tant qu'utilisateur actuel). Si vous ne spécifiez aucune instance de Serveur de connexion View, toutes les instances de Serveur de connexion View acceptent ces informations.</p> <p>Pour ajouter une instance de Serveur de connexion View, utilisez l'un des formats suivants :</p> <ul style="list-style-type: none"> ■ <code>domain\system\$</code> ■ <code>system\$@domain.com</code> ■ Nom principal de service (SPN) du service Serveur de connexion View. <p>La valeur de Registre Windows équivalente est <code>BrokersTrustedForDelegation</code>.</p>

Tableau 1-6. Modèle de configuration d' Horizon Client : paramètres de sécurité (suite)

Paramètre	Description
Certificate verification mode (Paramètre de Configuration d'ordinateur)	<p>Configure le niveau de la vérification de certificat exécutée par Horizon Client. Vous pouvez sélectionner l'un de ces modes :</p> <ul style="list-style-type: none"> ■ No Security. View n'effectue pas la vérification de certificat. ■ Warn But Allow. Lorsque les problèmes de certificat de serveur suivants se produisent, un avertissement s'affiche, mais l'utilisateur peut continuer à se connecter au Serveur de connexion View : <ul style="list-style-type: none"> ■ Un certificat auto-signé est fourni par View. Dans ce cas, cela est acceptable si le nom de certificat ne correspond pas au nom du Serveur de connexion View fourni par l'utilisateur dans Horizon Client. ■ Un certificat vérifiable qui a été configuré dans votre déploiement a expiré ou n'est pas encore valide. <p>Si une autre erreur de certificat se produit, View affiche une boîte de dialogue d'erreur et empêche l'utilisateur de se connecter au Serveur de connexion View.</p> <p>Warn But Allow est la valeur par défaut.</p> <ul style="list-style-type: none"> ■ Full Security. Si une erreur de type de certificat se produit, l'utilisateur ne peut pas se connecter au Serveur de connexion View. View affiche les erreurs de certificat à l'utilisateur. <p>Lorsque ce paramètre de stratégie de groupe est configuré, les utilisateurs peuvent voir le mode de vérification de certificat sélectionné dans Horizon Client, mais ils ne peuvent pas configurer le paramètre. La boîte de dialogue de configuration SSL informe les utilisateurs que l'administrateur a verrouillé le paramètre.</p> <p>Lorsque ce paramètre n'est pas configuré ou est désactivé, les utilisateurs d'Horizon Client peuvent sélectionner un mode de vérification de certificat.</p> <p>Pour autoriser un serveur View à vérifier les certificats fournis par Horizon Client, le client doit établir des connexions HTTPS avec l'hôte du Serveur de connexion View ou du serveur de sécurité. La vérification des certificats n'est pas prise en charge si vous déchargez SSL vers un serveur intermédiaire qui établit des connexions HTTP avec l'hôte de Serveur de connexion View ou du serveur de sécurité.</p> <p>Pour les clients Windows, si vous ne voulez pas configurer ce paramètre en tant que stratégie de groupe, vous pouvez également activer la vérification de certificat en ajoutant le nom de valeur CertCheckMode à l'une des clés de Registre suivantes sur l'ordinateur client :</p> <ul style="list-style-type: none"> ■ Pour Windows 32 bits : HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security ■ Pour Windows 64 bits : HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security <p>Utilisez les valeurs suivantes dans la clé de registre :</p> <ul style="list-style-type: none"> ■ 0 implémente No Security. ■ 1 implémente Warn But Allow. ■ 2 implémente Full Security. <p>Si vous configurez le paramètre de stratégie de groupe et le paramètre CertCheckMode dans la clé de Registre Windows, le paramètre de stratégie de groupe est prioritaire sur la valeur de la clé de registre.</p>

Tableau 1-6. Modèle de configuration d' Horizon Client : paramètres de sécurité (suite)

Paramètre	Description
Default value of the 'Log in as current user' checkbox (Paramètre de Configuration d'utilisateur et d'ordinateur)	<p>Spécifie la valeur par défaut de la case à cocher Se connecter en tant qu'utilisateur actuel dans la boîte de dialogue de connexion d'Horizon Client.</p> <p>Ce paramètre remplace la valeur par défaut spécifiée au cours de l'installation d'Horizon Client.</p> <p>Si un utilisateur exécute Horizon Client à partir de la ligne de commande et spécifie l'option <code>logInAsCurrentUser</code>, cette valeur remplace ce paramètre.</p> <p>Lorsque la case Se connecter en tant qu'utilisateur actuel est cochée, l'identité et les informations d'identification que l'utilisateur a fournies lors de la connexion au système client sont transmises à l'instance du Serveur de connexion View, puis au poste de travail distant. Lorsque la case n'est pas cochée, les utilisateurs doivent fournir leur identité et leurs informations d'identification plusieurs fois avant de pouvoir accéder à un poste de travail distant.</p> <p>Ce paramètre est désactivé par défaut.</p> <p>La valeur de Registre Windows équivalente est <code>LogInAsCurrentUser</code>.</p>
Display option to Log in as current user (Paramètre de Configuration d'utilisateur et d'ordinateur)	<p>Détermine si la case à cocher Se connecter en tant qu'utilisateur actuel doit être visible dans la boîte de dialogue de connexion d'Horizon Client.</p> <p>Lorsque la case est visible, les utilisateurs peuvent la cocher ou la décocher et remplacer sa valeur par défaut. Lorsque la case est masquée, les utilisateurs ne peuvent pas remplacer sa valeur par défaut dans la boîte de dialogue de connexion d'Horizon Client.</p> <p>Vous pouvez spécifier la valeur par défaut de la case Log in as current user (Se connecter en tant qu'utilisateur actuel) en utilisant le paramètre de règle <code>Default value of the 'Log in as current user' checkbox</code>.</p> <p>Ce paramètre est activé par défaut.</p> <p>La valeur de Registre Windows équivalente est <code>LogInAsCurrentUser_Display</code>.</p>
Enable jump list integration (Paramètre de Configuration d'ordinateur)	<p>Détermine si une liste de raccourcis doit s'afficher dans l'icône Horizon Client sur la barre des tâches des systèmes Windows 7 ou versions ultérieures. La liste des raccourcis permet aux utilisateurs de se connecter à des instances récentes du Serveur de connexion View et à des postes de travail récemment utilisés.</p> <p>Si Horizon Client est partagé, vous pouvez ne pas souhaiter que les utilisateurs voient les noms des postes de travail récemment utilisés. Vous pouvez désactiver la liste de raccourcis en désactivant ce paramètre.</p> <p>Ce paramètre est activé par défaut.</p> <p>La valeur de Registre Windows équivalente est <code>EnableJumpList</code>.</p>
Enable SSL encrypted framework channel (Paramètre de Configuration d'utilisateur et d'ordinateur)	<p>Détermine si SSL doit être activé pour les postes de travail View 5.0 et versions antérieures. Avant View 5.0, les données envoyées au poste de travail via le port TCP 32111 n'étaient pas chiffrées.</p> <ul style="list-style-type: none"> ■ Activer : active SSL, mais autorise le retour à la connexion non chiffrée précédente si le poste de travail distant ne prend pas en charge SSL. Par exemple, les postes de travail View 5.0 et versions antérieures ne prennent pas en charge SSL. Activer est le paramètre par défaut. ■ Désactiver : désactive SSL. Ce paramètre n'est pas recommandé, mais peut toutefois être utile pour le débogage ou si le canal n'est pas configuré en tunnel et peut par la suite faire l'objet d'une optimisation par un produit accélérateur WAN. ■ Appliquer : active SSL et refuse les connexions aux postes de travail qui ne prennent pas en charge SSL. <p>La valeur de Registre Windows équivalente est <code>EnableTicketSSLAuth</code>.</p>

Tableau 1-6. Modèle de configuration d' Horizon Client : paramètres de sécurité (suite)

Paramètre	Description
Configures SSL protocols and cryptographic algorithms (Paramètre de Configuration d'utilisateur et d'ordinateur)	<p>Configure la liste de chiffrements afin de limiter l'utilisation de certains protocoles et algorithmes de chiffrement avant l'établissement d'une connexion SSL chiffrée. La liste de chiffrements est composée d'une ou de plusieurs chaînes de chiffrement séparées par deux points.</p> <p>REMARQUE Toutes les chaînes de chiffrement sont sensibles à la casse.</p> <ul style="list-style-type: none"> ■ Si cette fonction est activée, la valeur par défaut d'Horizon Client 3.5 et versions ultérieures est TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:EC DH+AES:RSA+AES:@STRENGTH. ■ La valeur par défaut d'Horizon Client 3.3 et 3.4 est TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH. ■ La valeur dans Horizon Client 3.2 et versions antérieures est SSLv3:TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH. <p>Cela signifie que dans Horizon Client 3.5 et versions ultérieures, TLS v1.0, TLS v1.1 et TLS v1.2 sont activés. (SSL v2.0 et v3.0 sont désactivés.) Dans Horizon Client 3.3 et 3.4, TLS v1.0 et TLS v1.1 sont activés. (SSL v2.0, SSL v3.0 et TLS v1.2 sont désactivés.) Dans Horizon Client 3.2 et versions antérieures, SSL v3.0 est également activé. (SSL v2.0 et TLS v1.2 sont désactivés.)</p> <p>Les suites de chiffrement utilisent la spécification AES 128 ou 256 bits, suppriment les algorithmes DH anonymes, puis trient la liste de chiffrements actuels par longueur de clé de chiffrement.</p> <p>Lien de référence pour la configuration : http://www.openssl.org/docs/apps/ciphers.html.</p> <p>La valeur de Registre Windows équivalente est <code>SSLCipherList</code>.</p>
Enable Single Sign-On for smart card authentication (Paramètre de Configuration d'ordinateur)	<p>Détermine si l'authentification unique est activée pour l'authentification par carte à puce. Lorsque l'authentification unique est activée, Horizon Client stocke le code PIN de carte à puce chiffré dans la mémoire temporaire avant de l'envoyer au Serveur de connexion View. Lorsque l'authentification unique est désactivée, Horizon Client n'affiche pas de boîte de dialogue de code PIN personnalisé.</p> <p>La valeur de Registre Windows équivalente est <code>EnableSmartCardSSO</code>.</p>
Ignore bad SSL certificate date received from the server (Paramètre de Configuration d'ordinateur)	<p>(View 4.6 et versions antérieures uniquement) Détermine si les erreurs associées aux dates des certificats de serveur non valides doivent être ignorées. Ces erreurs se produisent quand un serveur envoie un certificat avec une date passée.</p> <p>La valeur de Registre Windows équivalente est <code>IgnoreCertDateInvalid</code>.</p>
Ignore certificate revocation problems (Paramètre de Configuration d'ordinateur)	<p>(View 4.6 et versions antérieures uniquement) Détermine si les erreurs associées à un certificat de serveur révoqué doivent être ignorées. Ces erreurs se produisent lorsque le serveur envoie un certificat qui a été révoqué et lorsque le client ne peut pas vérifier l'état de révocation d'un certificat.</p> <p>Ce paramètre est désactivé par défaut.</p> <p>La valeur de Registre Windows équivalente est <code>IgnoreRevocation</code>.</p>
Ignore incorrect SSL certificate common name (host name field) (Paramètre de Configuration d'ordinateur)	<p>(View 4.6 et versions antérieures uniquement) Détermine si les erreurs associées aux noms communs de certificats de serveur incorrects doivent être ignorées. Ces erreurs se produisent quand le nom commun sur le certificat ne correspond pas au nom d'hôte du serveur qui l'envoie.</p> <p>La valeur de Registre Windows équivalente est <code>IgnoreCertCnInvalid</code>.</p>

Tableau 1-6. Modèle de configuration d' Horizon Client : paramètres de sécurité (suite)

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

Pour plus d'informations sur ces paramètres et leurs implications en matière de sécurité, consultez le document *Utilisation de VMware Horizon Client pour Windows*.

Paramètres liés à la sécurité dans la section Définitions de script du modèle de configuration d' Horizon Client

Les paramètres liés à la sécurité sont fournis dans la section Définitions de script du fichier de modèle d'administration d'Horizon Client (`vdm_client.adm`). Sauf indication contraire, les paramètres incluent un paramètre Configuration ordinateur et un paramètre Configuration utilisateur. Si vous définissez un paramètre Configuration utilisateur, il remplace le paramètre Configuration ordinateur équivalent.

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

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

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

Tableau 1-7. Paramètres liés à la sécurité dans la section Définitions de script

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

Pour plus d'informations sur ces paramètres et leurs implications en matière de sécurité, consultez le document *Utilisation de VMware Horizon Client pour Windows*.

Paramètres liés à la sécurité dans View LDAP

Les paramètres liés à la sécurité sont fournis dans View 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 View. La modification se propage automatiquement à toutes les autres instances du Serveur de connexion View dans un groupe.

Tableau 1-8. Paramètres liés à la sécurité dans View LDAP

Paire nom/valeur	Description
<code>cs-allowunencryptedstartsession</code>	<p>L'attribut est <code>paé-NameValuePair</code>.</p> <p>Cet attribut contrôle si un canal sécurisé est requis entre une instance de Serveur de connexion View et un poste de travail lorsqu'une session d'utilisateur distante est démarrée.</p> <p>Lorsque View Agent 5.1 ou supérieur est installé sur un ordinateur de poste de travail, cet attribut n'a aucun effet et un canal sécurisé est toujours requis.</p> <p>Lorsque View Agent antérieur à View 5.1 est installé, un canal sécurisé ne peut pas être établi si l'ordinateur de poste de travail n'est pas membre d'un domaine avec une approbation bidirectionnelle vers le domaine de l'instance de Serveur de connexion View. Dans ce cas, l'attribut est important pour déterminer si une session d'utilisateur distante peut être démarrée sans canal sécurisé.</p> <p>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.</p> <p>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 View Agent 5.1 ou supérieur est installé sur tous les postes de travail.</p> <p>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 certains postes de travail ont des View Agents anciens et s'ils se ne trouvent pas dans des domaines approuvés.</p> <p>Le paramètre par défaut est</p> <p>1.</p>

Ressources de View

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

Tableau 1-9. Ressources du Serveur de connexion View et de serveur de sécurité

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	<Lettre de lecteur>:\Programdata\VMWare\VDM\backups (Windows Server 2008)	Protégé par un contrôle d'accès.
locked.properties (Fichier de propriétés de certificat)	install_directory\VMware\VMware View\Server\sslgateway\conf	Peut être protégé par un contrôle d'accès. Assurez-vous que ce fichier est sécurisé contre l'accès par des utilisateurs qui ne sont pas des administrateurs View.

Tableau 1-9. Ressources du Serveur de connexion View et de serveur de sécurité (suite)

Resource (Ressource)	Emplacement	Protection
Fichiers journaux	Reportez-vous à la section « Fichiers journaux de View », page 19	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 de View

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

REMARQUE Les fichiers journaux de View sont conçus pour être utilisés par le support VMware. VMware vous recommande de configurer et d'utiliser la base de données des événements pour contrôler View. Pour plus d'informations, reportez-vous aux documents *Installation de View* et *Intégration de View*.

Tableau 1-10. Fichiers journaux de View

Composant View	Chemin d'accès au fichier et autres informations
Tous les composants (journaux d'installation)	%TEMP%\vminst.log_date_timestamp %TEMP%\vmmsi.log_date_timestamp
View Agent	<Drive Letter>:\ProgramData\VMware\VDM\logs Pour accéder aux fichiers journaux de View stockés dans <Drive Letter>:\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 de PCoIP portent les noms pcoip_agent*.log et pcoip_server*.log.
Applications View	Base de données des événements View configurée sur un serveur de base de données SQL Server ou Oracle. Journaux d'événements d'application Windows. Désactivé par défaut.
View Composer	%system_drive%\Windows\Temp\vmware-viewcomposer-ga-new.log sur le poste de travail de clone lié. Le journal de View Composer contient des informations sur l'exécution des scripts QuickPrep et Sysprep. Le journal enregistre l'heure de début et l'heure de fin de l'exécution du script, ainsi que tous les messages de sortie ou d'erreur.
Serveur de connexion View ou serveur de sécurité	<Drive Letter>:\ProgramData\VMware\VDM\logs. Le répertoire des journaux est configurable dans les paramètres de configuration de journal du fichier de modèle d'administration pour la configuration commune de View (vdm_common.adm). Les journaux de PCoIP Secure Gateway sont écrits dans des fichiers avec le nom SecurityGateway_*.log dans le sous-répertoire PCoIP Secure Gateway du répertoire des journaux sur un serveur de sécurité.
Services View	Base de données des événements View configurée sur un serveur de base de données SQL Server ou Oracle. Journaux d'événements de système Windows.

Ports TCP et UDP de View

View utilise des ports TCP et UDP pour l'accès au réseau entre ses composants.

Lors de l'installation, View 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 View » dans le document *Installation de View*.

Tableau 1-11. Ports TCP et UDP utilisés par View

Source	Port	Cible	Port	Protocole	Description
Serveur de sécurité	55000	View Agent	4172	UDP	PCoIP (pas SALSA20) si PCoIP Secure Gateway est utilisé.
Serveur de sécurité	4172	Horizon Client	Varie	UDP	PCoIP (pas SALSA20) si PCoIP Secure Gateway est utilisé. REMARQUE Comme le port cible varie, voir « Notes et mises en garde pour les ports TCP et UDP utilisés par View », page 24.
Serveur de sécurité	500	Serveur de connexion View	500	UDP	Trafic de négociation IPsec.
Serveur de sécurité	*	Serveur de connexion View	4001	TCP	Trafic JMS.
Serveur de sécurité	*	Serveur de connexion View	4002	TCP	Trafic JMS SSL.
Serveur de sécurité	*	Serveur de connexion View	8009	TCP	Trafic Web AJP13, si IPsec n'est pas utilisé.
Serveur de sécurité	*	Serveur de connexion View	*	ESP	Trafic Web AJP13, quand IPsec est utilisé sans NAT.
Serveur de sécurité	4500	Serveur de connexion View	4500	UDP	Trafic Web AJP13, quand IPsec est utilisé via un périphérique NAT.
Serveur de sécurité	*	Machine virtuelle	3389	TCP	Trafic Microsoft RDP vers des postes de travail View.
Serveur de sécurité	*	Machine virtuelle	9427	TCP	Redirection multimédia (MMR) Windows Media et redirection de lecteur client.
Serveur de sécurité	*	Machine virtuelle	32111	TCP	Redirection USB.
Serveur de sécurité	*	Machine virtuelle	4172	TCP	PCoIP, si PCoIP Secure Gateway est utilisé.
Serveur de sécurité	*	Machine virtuelle	22443	TCP	HTML Access.
View Agent	4172	Horizon Client	Varie	UDP	PCoIP, si PCoIP Secure Gateway n'est pas utilisé. REMARQUE Comme le port cible varie, voir « Notes et mises en garde pour les ports TCP et UDP utilisés par View », page 24.

Tableau 1-11. Ports TCP et UDP utilisés par View (suite)

Source	Port	Cible	Port	Protocole	Description
View Agent	4172	Serveur de connexion View ou serveur de sécurité	55000	UDP	PCoIP (pas SALSA20) si PCoIP Secure Gateway est utilisé.
View Agent	4172	Dispositif Access Point	*	UDP	PCoIP. Des applications et des postes de travail View renvoient des données PCoIP à un dispositif Access Point 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.
Horizon Client	*	Serveur de connexion View ou serveur de sécurité ou dispositif Access Point	80	TCP	SSL (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 « Notes et mises en garde pour les ports TCP et UDP utilisés par View », page 24.
Horizon Client	*	Serveur de sécurité View ou dispositif Access Point	443	TCP	Accès HTTPS. Le port 443 est activé par défaut pour les connexions client. Le port 443 peut être modifié sur les serveurs de sécurité. Les tentatives de connexion via HTTP au port 80 sont redirigées vers le port 443 par défaut, mais le port 80 peut fournir les connexions client si SSL est déchargé sur un périphérique intermédiaire. Vous pouvez reconfigurer la règle de redirection si le port HTTPS a été modifié. Reportez-vous à la section « Notes et mises en garde pour les ports TCP et UDP utilisés par View », page 24.
Horizon Client	*	Serveur de connexion View	443	TCP	Accès HTTPS. Le port 443 est activé par défaut pour les connexions client. Le port 443 peut être modifié. Les tentatives de connexion client au port 80 sont redirigées vers le port 443 par défaut, mais le port 80 peut fournir les connexions client si SSL est déchargé sur un périphérique intermédiaire. Les tentatives de connexion au port 80 pour atteindre View Administrator ne sont pas redirigées. Vous pouvez vous connecter via HTTPS pour atteindre View Administrator. Vous pouvez empêcher la redirection HTTP et forcer les clients à utiliser HTTPS. Reportez-vous à la section « Notes et mises en garde pour les ports TCP et UDP utilisés par View », page 24.
Horizon Client	*	Serveur de connexion View ou serveur de sécurité ou dispositif Access Point	4172	TCP et UDP	PCoIP, si PCoIP Secure Gateway est utilisé.
Horizon Client	*	Machine virtuelle	3389	TCP	Trafic Microsoft RDP vers des postes de travail View si des connexions directes sont utilisées à la place de connexions par tunnel.

Tableau 1-11. Ports TCP et UDP utilisés par View (suite)

Source	Port	Cible	Port	Protocole	Description
Horizon Client	*	Machine virtuelle	9427	TCP	Redirection multimédia (MMR) Windows Media et redirection de lecteur client, si des connexions directes sont utilisées à la place de connexions par tunnel.
Horizon Client	*	Machine virtuelle	32111	TCP	Redirection USB si des connexions directes sont utilisées à la place de connexions par tunnel.
Horizon Client	*	View Agent	4172	TCP et UDP	PCoIP si PCoIP Secure Gateway n'est pas utilisé.
Horizon Client	Varie	View Agent	4172	UDP	PCoIP si PCoIP Secure Gateway n'est pas utilisé. REMARQUE Comme le port source varie, voir « Notes et mises en garde pour les ports TCP et UDP utilisés par View », page 24.
Horizon Client	Varie	Serveur de connexion View ou serveur de sécurité	4172	UDP	PCoIP (pas SALSA20) si PCoIP Secure Gateway est utilisé. REMARQUE Comme le port source varie, voir « Notes et mises en garde pour les ports TCP et UDP utilisés par View », page 24.
Navigateur Web	*	Serveur de sécurité ou dispositif Access Point	8443	TCP	HTML Access.
Serveur de connexion View	*	Serveur de connexion View	48080	TCP	Pour la communication interne entre les composants du Serveur de connexion View.
Serveur de connexion View	*	vCenter Server ou View Composer	80	TCP	Messages SOAP si SSL est désactivé pour l'accès à vCenter Server ou View Composer.
Serveur de connexion View	*	vCenter Server	443	TCP	Messages SOAP si SSL est activé pour l'accès à vCenter Server.
Serveur de connexion View	*	View Composer	18443	TCP	Messages SOAP si SSL est activé pour l'accès à View Composer.
Serveur de connexion View	55000	View Agent	4172	UDP	PCoIP (pas SALSA20) si PCoIP Secure Gateway via Serveur de connexion View est utilisé.
Serveur de connexion View	4172	Horizon Client	Varie	UDP	PCoIP (pas SALSA20) si PCoIP Secure Gateway via Serveur de connexion View est utilisé. REMARQUE Comme le port cible varie, voir « Notes et mises en garde pour les ports TCP et UDP utilisés par View », page 24.
Serveur de connexion View	*	Serveur de connexion View	4100	TCP	Trafic interroutage JMS.
Serveur de connexion View	*	Serveur de connexion View	4101	TCP	Trafic interroutage JMS SSL.
Serveur de connexion View	*	Machine virtuelle	3389	TCP	Trafic Microsoft RDP vers des postes de travail View si des connexions par tunnel via le Serveur de connexion View sont utilisées.
Serveur de connexion View	*	Machine virtuelle	4172	TCP	PCoIP si PCoIP Secure Gateway via le Serveur de connexion View est utilisé.

Tableau 1-11. Ports TCP et UDP utilisés par View (suite)

Source	Port	Cible	Port	Protocole	Description
Serveur de connexion View	*	Machine virtuelle	9427	TCP	Redirection Windows Media (MMR) et redirection de lecteur client, si des connexions par tunnel via le Serveur de connexion View sont utilisées.
Serveur de connexion View	*	Machine virtuelle	32111	TCP	Redirection USB si des connexions par tunnel via le Serveur de connexion View sont utilisées.
Serveur de connexion View	*	Serveur de connexion View	8472	TCP	Pour la communication entre espaces dans Architecture Cloud Pod.
Serveur de connexion View	*	Serveur de connexion View	22389	TCP	Pour la réplication LDAP globale dans Architecture Cloud Pod.
Serveur de connexion View	*	Serveur de connexion View	22636	TCP	Pour la réplication LDAP globale sécurisée dans Architecture Cloud Pod.
Dispositif Access Point	*	Serveur de connexion View ou équilibrage de charge	443	TCP	Accès HTTPS. Des dispositifs Access Point se connectent sur le port TCP 443 pour communiquer avec une instance du Serveur de connexion View ou un équilibrage de charge devant plusieurs instances du Serveur de connexion View.
Dispositif Access Point	*	Machine virtuelle	3389	TCP	Trafic Microsoft RDP vers des postes de travail View.
Dispositif Access Point	*	Machine virtuelle	9427	TCP	Redirection multimédia (MMR) Windows Media et redirection de lecteur client.
Dispositif Access Point	*	Application ou poste de travail View	4172	TCP et UDP	Des dispositifs Access Point se connectent aux applications et postes de travail View sur le port TCP 4172 et le port UDP 4172 pour échanger du trafic PCoIP.
Dispositif Access Point	*	Machine virtuelle	32111	TCP	Redirection USB si des connexions directes sont utilisées à la place de connexions par tunnel.
Dispositif Access Point	*	Machine virtuelle	22443	TCP	HTML Access.
Machine virtuelle	*	Instances de Serveur de connexion View	4002	TCP	Trafic JMS SSL.
service View Composer	*	Hôte ESXi	902	TCP	Utilisé lorsque View Composer personnalise des disques de clone lié, y compris des disques internes de View Composer et, s'ils sont spécifiés, des disques persistants et des disques supprimables par le système.

Notes et mises en garde pour les ports TCP et UDP utilisés par View

Les tentatives de connexion via HTTP sont redirigées en silence vers HTTPS, à l'exception des tentatives de connexion à View Administrator. La redirection HTTP n'est pas nécessaire pour les clients View plus récents car ils sont dirigés par défaut vers HTTPS. Mais elle est utile lorsque les utilisateurs se connectent avec un navigateur Web, par exemple pour télécharger View 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.

REMARQUE 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 via HTTP à View Administrator 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, consultez « Empêcher la redirection HTTP des connexions des clients vers le serveur de connexion » dans le document *Installation de View*.

Les connexions au port 80 d'une instance de Serveur de connexion View ou d'un serveur de sécurité peuvent également avoir lieu si vous déchargez les connexions client SSL sur un périphérique intermédiaire. Voir « Décharger des connexions SSL sur des serveurs intermédiaires » dans le document *Administration de View*.

Pour autoriser la redirection HTTP lorsque le numéro de port SSL a été modifié, consultez « Modifier le numéro de port de la redirection HTTP vers le serveur de connexion » dans le document *Installation de View*.

REMARQUE Le numéro de port UDP que les clients utilisent pour le protocole PCoIP est susceptible de changer. Si le port 50002 est utilisé, le client choisira 50003. Si le port 50003 est utilisé, le client choisira le port 50004, etc. Vous devez configurer le pare-feu avec TOUS où « Varie » est répertorié dans le tableau.

Services sur un hôte du Serveur de connexion View

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

Tableau 1-12. Services d'un hôte du Serveur de connexion View

Nom du service	Type de démarrage	Description
VMware Horizon 6 Blast Secure Gateway	Automatique	Fournit des services HTML Access sécurisés. Ce service doit être en cours d'exécution si des clients se connectent au Serveur de connexion View via HTML Access Secure Gateway.
Serveur de connexion VMware Horizon 6	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 View Script Host.
Composant de VMware Horizon 6 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 du bus de messages VMware Horizon 6	Manuel	Fournit des services de messagerie entre les composants View. Ce service doit toujours être en cours d'exécution.

Tableau 1-12. Services d'un hôte du Serveur de connexion View (suite)

Nom du service	Type de démarrage	Description
VMware Horizon 6 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 View via PCoIP Secure Gateway.
Hôte de script VMware Horizon 6	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 6 Security Gateway	Manuel	Fournit des services de passerelle communs. Ce service doit toujours être en cours d'exécution.
Composant Web VMware Horizon 6	Manuel	Fournit des services Web. Ce service doit toujours être en cours d'exécution.
VMwareVDMDS	Automatique	Fournit des services d'annuaire LDAP. Ce service doit toujours être en cours d'exécution. Pendant les mises à niveau de View, ce service garantit la migration correcte des données existantes.

Services sur un serveur de sécurité

Le fonctionnement de View dépend de plusieurs services s'exécutant sur un serveur de sécurité.

Tableau 1-13. Services de serveur de sécurité

Nom du service	Type de démarrage	Description
VMware Horizon 6 Blast Secure Gateway	Automatique	Fournit des services HTML Access sécurisés. Ce service doit être en cours d'exécution si des clients se connectent à ce serveur de sécurité via HTML Access Secure Gateway.
Serveur de sécurité VMware Horizon 6	Automatique	Fournit des services de serveur de sécurité. Ce service doit toujours être en cours d'exécution. Si vous démarrez ou arrêtez ce service, il démarre ou arrête également les services Framework et Security Gateway.
Composant de VMware Horizon 6 Framework	Manuel	Fournit des services de journalisation des événements, de sécurité et d'infrastructure COM+. Ce service doit toujours être en cours d'exécution.
VMware Horizon 6 PCoIP Secure Gateway	Manuel	Fournit des services PCoIP Secure Gateway. Ce service doit être en cours d'exécution si des clients se connectent à ce serveur de sécurité via PCoIP Secure Gateway.
Composant VMware Horizon 6 Security Gateway	Manuel	Fournit des services de passerelle communs. Ce service doit toujours être en cours d'exécution.

Configuration des protocoles de sécurité et des suites de chiffrement sur une instance de Serveur de connexion View ou sur un serveur de sécurité

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

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

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

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 1-14. Stratégies générales par défaut

Protocoles de sécurité par défaut	Suites de chiffrement par défaut
<ul style="list-style-type: none"> ■ TLS 1.2 ■ TLS 1.1 ■ TLS 1.0 	<ul style="list-style-type: none"> ■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ■ TLS_RSA_WITH_AES_128_CBC_SHA ■ TLS_RSA_WITH_AES_256_CBC_SHA

Si tous les clients se connectant prennent en charge TLS 1.1 et/ou TLS 1.2, vous pouvez retirer TLS 1.0 de la stratégie d'acceptation.

Configuration des stratégies d'acceptation et de proposition générales

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

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

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

Vous pouvez modifier les attributs View 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 :

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

L'attribut suivant répertorie les suites de chiffrement. L'ordre des suites de chiffrement n'est pas important. Cet exemple montre une liste abrégée :

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

Stratégies de proposition générales

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

```
paë-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 :

```
paë-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, vous utilisez l'utilitaire ADSI Edit (Éditeur ADSI) pour modifier les attributs View LDAP.

Prérequis

- Familiarisez-vous avec les attributs View LDAP qui définissent les stratégies d'acceptation et de proposition. Reportez-vous à la section « [Stratégies d'acceptation et de proposition générales définies dans View LDAP](#) », page 27.
- 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 View.
- 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 View 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 **OU=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 service Serveur de connexion VMware Horizon View.

Configurer des stratégies d'acceptation sur des View Server individuels

Pour spécifier une stratégie d'acceptation locale sur une instance de Serveur de connexion View ou un serveur de sécurité individuel, vous devez ajouter des propriétés au fichier `locked.properties`. Si le fichier `locked.properties` n'existe pas encore sur View Server, 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.

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 SSL sur l'ordinateur Serveur de connexion View ou du serveur de sécurité.
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 Serveur de connexion VMware Horizon View ou le service serveur de sécurité VMware Horizon View 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
secureProtocols.2=TLSv1.1
secureProtocols.3=TLSv1
```

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

```
preferredSecureProtocol=TLSv1.2
```

The order of the following list is unimportant:

```
enabledCipherSuite.1=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
enabledCipherSuite.2=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
enabledCipherSuite.3=TLS_RSA_WITH_AES_128_CBC_SHA256
enabledCipherSuite.4=TLS_RSA_WITH_AES_128_CBC_SHA
```

Configurer des stratégies de proposition sur des postes de travail View

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

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

Procédure

- 1 Lancez l'éditeur du Registre Windows sur le poste de travail View.
- 2 Accédez à la clé de registre HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration.
- 3 Ajoutez une nouvelle valeur de chaîne (REG_SZ), ClientSSLSecureProtocols.
- 4 Définissez la valeur sur une liste de suites de chiffrement au format `\LIST:protocol_1,protocol_2,...`
Répertoriez les protocoles avec le dernier protocole en premier. Par exemple :
`\LIST:TLSv1.2,TLSv1.1,TLSv1`
- 5 Ajoutez une nouvelle valeur de chaîne (REG_SZ), ClientSSLCipherSuites.
- 6 Définissez la valeur sur une liste de suites de chiffrement au format `\LIST:cipher_suite_1,cipher_suite_2,...`
La liste doit être dans l'ordre de préférence, avec la suite de chiffrement préférée en premier. Par exemple :
`\LIST:TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA`

Normes EITF (Internet Engineering Task Force)

Le Serveur de connexion View et le serveur de sécurité sont conformes à certaines normes IEFT (Internet Engineering Task Force).

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

REMARQUE La renégociation initiée par le client est désactivée par défaut sur les Serveurs de connexion et les serveurs de sécurité. 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.
- 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 stratégies d'acceptation sur des View Server individuels](#) », page 28.

Protocoles et chiffrements anciens désactivés dans View

Certains anciens protocoles et chiffrements qui ne sont plus considérés comme étant sécurisés sont désactivés par défaut dans View. 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, les serveurs de sécurité et les postes de travail View, vous pouvez activer ces suites de chiffrement en modifiant la base de données View LDAP, le fichier `locked.properties` ou le registre, comme décrit dans ce guide. Voir « [Modifier les stratégies d'acceptation et de proposition générales](#) », page 27, « [Configurer des stratégies d'acceptation sur des View Server individuels](#) », page 28 et « [Configurer des stratégies de proposition sur des postes de travail View](#) », page 29. 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 Composer et 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 View Composer et View Agent](#) » dans le document *Installation de View*.

```
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
```

REMARQUE 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

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

Pour les instances du Serveur de connexion, les serveurs de sécurité et les postes de travail View, vous pouvez activer SSLv3 en supprimant SSLv3 de la propriété `jdk.tls.disabledAlgorithms` dans le fichier `C:\Program Files\VMware\VMware View\Server\jre\lib\security\java.security` sur chaque instance du Serveur de connexion View et sur chaque serveur de sécurité.

Pour les machines View Composer et View Agent Direct-Connection (VADC), vous pouvez activer SSLv3 en ajoutant les valeurs suivantes (REG_DWORD) à la clé de registre `HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server :`

```
DisabledByDefault=0
Enabled=1
```

RC4

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

Pour les instances du Serveur de connexion, les serveurs de sécurité et les postes de travail View, vous pouvez activer RC4 sur un Serveur de connexion, un serveur de sécurité ou une machine View 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, le serveur de sécurité ou la machine View Agent, selon le cas.

Pour les machines View Composer et 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 View Composer et View Agent » dans le document *Installation de View*.

```
TLS_RSA_WITH_RC4_128_SHA
```

Réduction des risques de sécurité de type MIME

Par défaut, View 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, View 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, View accepte les demandes avec tout type de contenu déclaré, à l'exception des connexions à View Administrator.

Pour limiter les types de contenu acceptés par View, 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.

Vérification de l'origine

Par défaut, la protection contre la falsification de demande entre sites est désactivée.

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

```
checkOrigin=true
```

Si plusieurs Serveurs de connexion ou serveurs de sécurité sont à équilibrage de charge, vous devez spécifier l'adresse de l'équilibrage de charge en ajoutant l'entrée suivante au fichier `locked.properties`. Le port 443 est utilisé pour cette adresse.

```
balancedHost=load-balancer-name
```

Lorsque cette option est activée, des connexions à View peuvent être établies uniquement à l'adresse donnée dans l'URL externe, à l'adresse `balancedHost` ou à `localhost`.

Déploiement de périphériques USB dans un environnement View sécurisé

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 View contre cette vulnérabilité de sécurité.

En désactivant la redirection USB, vous pouvez empêcher toute redirection de périphérique USB vers les postes de travail et les applications View 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 postes de travail et leurs applications.

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 View. Au minimum, analysez sérieusement à quel degré votre organisation doit tenter de limiter son exposition à cette vulnérabilité de sécurité.

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 View 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 View Administrator, 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 RDS. Vous ne pouvez pas définir cette stratégie pour des pools d'applications ou de postes de travail RDS individuels.

- Dans View Administrator, dès que vous avez défini la stratégie au niveau du pool de postes de travail ou d'applications, vous pouvez remplacer la stratégie d'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 View Agent ou du côté client, selon le cas.

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 View Agent et Horizon Client. Le tableau suivant décrit comment la stratégie **Exclude All Devices** que vous pouvez définir pour View 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 1-15. Effet de la combinaison de règles Exclure tous les périphériques

Règle Exclure tous les périphériques sur View 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 d'`Exclude All Devices` dans View Agent n'est pas transmise à Horizon Client, mais View Agent et Horizon Client appliquent la valeur locale d'`Exclude All Devices`.

Ces stratégies sont incluses dans le fichier de modèle d'administration de configuration de View Agent (`vdm_agent.adm`). Pour obtenir plus d'informations, reportez-vous à « Paramètres USB du modèle d'administration de configuration de View Agent » du document *Configuration de pools de postes de travail et d'applications dans View*.

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 de View 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
```

REMARQUE 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, View 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 View provenant de l'extérieur du pare-feu de l'entreprise. Le périphérique USB peut être utilisé en interne, mais pas en externe.

Pour désactiver l'accès externe aux périphériques USB, vous pouvez bloquer le port TCP 32111 aux applications et postes de travail distants à partir du serveur de sécurité. 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 de configuration de View Agent (`vdm_agent.adm`). Pour obtenir plus d'informations, reportez-vous à « Paramètres USB du modèle d'administration de configuration de View Agent » du document *Configuration de pools de postes de travail et d'applications dans View*.

Index

A

attaques de script entre sites **31**

C

comptes **7**

F

Fichiers de modèle d'administration (ADM),
paramètres liés à la sécurité **8**

fichiers journaux **19**

H

HTTP, redirection **24**

L

locked.properties, configuration de stratégies
d'acceptation **28**

N

normes IEFT (Internet Engineering Task
Force) **29**

P

paramètres de pare-feu **20**

paramètres de sécurité, générale **8**

paramètres du serveur. liés à la sécurité **8**

ports TCP, 80 et 443 **24**

ports UDP **20**

postes de travail, configuration de stratégies de
proposition **29**

présentation de sécurité **5**

protocoles de sécurité
configuration pour le Serveur de connexion
View **26**

modification dans View LDAP **27**

stratégies par défaut **26**

R

RC4, désactivé dans View **30**

redirection USB

déploiement sécurisé les périphériques **32**

désactivation de périphériques spécifiques **33**

désactivation de tous les périphériques **32**

ressources **18**

risques de sécurité de type MIME **31**

S

sécurité de View **7**

Serveur de connexion View, services **24**

serveurs de sécurité, services **25**

service Blast Secure Gateway **24, 25**

service de serveur de sécurité **25**

service du serveur de connexion **24**

service Framework Component **24, 25**

service Message Bus Component **24**

service Script Host **24**

service Security Gateway Component **24, 25**

service VMwareVDMDS **24**

service Web Component **24**

services

hôtes de serveur de sécurité **25**

hôtes du Serveur de connexion View **24**

SSLv3, désactivé dans View **30**

stratégies d'acceptation, configuration
générale **26**

stratégies de proposition, configuration
générale **26**

suites de chiffrement

configuration pour le Serveur de connexion
View **26**

modification dans View LDAP **27**

stratégies générales par défaut **26**

V

vérification de l'origine **31**

vérification du type de contenu **31**

View LDAP, stratégies d'acceptation et de
proposition générales **27**

