Sécurité de View

VMware Horizon 6.0

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-001486-00

vmware®

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

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

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

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

docfeedback@vmware.com

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

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

Table des matières

Sécurité de View

Sécurité de View fournit une référence succincte sur les fonctionnalités de sécurité de VMware Horizon (avec View)™.

- 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 1

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.

- Comptes View page 8

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

- Paramètres de sécurité de View page 9

  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.

- Ressources de View page 18

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

- Fichiers journaux de View page 18

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

- Ports TCP et UDP de View page 19

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

- Services sur un hôte du Serveur de connexion View page 22

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

- Services sur un serveur de sécurité page 23

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

- 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 24

  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.

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 *Installation de View*.
View Composer	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. 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. Pour plus d'informations sur les privilèges requis, reportez-vous au document *Installation de View*.
Serveur de connexion View ou serveur de sécurité	Lorsque vous installez View, vous pouvez choisir les membres du groupe d'administrateurs local (`BUILTIN\Administrators`) qui sont autorisés à se connecter à View Administrator. Dans View Administrator, utilisez **Configuration de View > Administrateurs** pour modifier la liste des administrateurs View. Pour plus d'informations sur les privilèges requis, reportez-vous au document *Administration de View*.

Tableau 1-2. Comptes de base de données View

Composant de View	Comptes requis
base de données View Composer	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. Pour plus d'informations sur la configuration d'une base de données View Composer, reportez-vous au document *Installation de View*.
Base de données des événements utilisée par le Serveur de connexion View	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. Pour plus d'informations sur la configuration d'une base de données View Composer, reportez-vous au document *Installation de View*.

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	Le mot de passe est requis lorsque vous restaurez la configuration View LDAP à partir d'une sauvegarde cryptée. 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. Lorsque vous sauvegardez Serveur de connexion View, la configuration View LDAP est exportée sous forme de données LDIF cryptées. 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.
Message security mode (Mode de sécurité des messages)	Détermine si la signature et la vérification des messages JMS transmis entre les composants de View a lieu. Si le paramètre est réglé sur **Désactivé**, le mode de sécurité des messages est désactivé. Si le paramètre est réglé sur **Activé**, les composants View rejettent les messages non signés. 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. Le paramètre par défaut est **Activé** pour les nouvelles installations.
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 View 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 View, car la connexion réseau a été temporairement interrompue. Ce paramètre est activé par défaut.
Forcer la déconnexion des utilisateurs	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. 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**, 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**, View 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**.

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

Paramètre	Description
Autres clients. **Supprimer les informations d'identification SSO**	Ignore les informations d'identification SSO au bout d'un certain temps. Ce paramètres 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. La valeur par défaut est **Après 15 minutes**.
Activer IPSec pour le couplage du serveur de sécurité	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. Par défaut, IPSec pour les connexions du serveur de sécurité est activé.
Délai d'expiration de la session de View Administrator	Détermine la durée pendant laquelle une session View Administrator inactive continue avant d'expirer. 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. 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.

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 équilibreurs de charge ou d'autres serveurs intermédiaires client, vous pouvez décharger SSL sur eux et configurer des connexions non-SSL sur des instances de Serveur de connexion View et des serveurs de sécurité individuels. Voir « Décharger 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 cliente sous `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Agent\Configuration`.

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

Paramètre	Nom de la valeur de registre	Description
AllowDirectRDP	AllowDirectRDP	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. IMPORTANT Pour que View fonctionne correctement, les services Bureau à distance doivent s'exécuter sur le système d'exploitation invité de chaque poste de travail. Vous pouvez utiliser ce paramètre pour empêcher les utilisateurs de faire des connexions RDP directes sur leurs postes de travail. Ce paramètre est activé par défaut.
AllowSingleSignon	AllowSingleSignon	Détermine si l'authentification unique (Single Sign-On, SSO) est utilisée pour connecter les utilisateurs aux postes de travail et aux applications. Lorsque ce paramètre est activé, 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. Ce paramètre est activé par défaut.
CommandsToRunOnConnect	CommandsToRunOnConnect	Spécifie une liste de commandes ou de scripts de commande à exécuter lorsqu'une session est connectée pour la première fois. Aucune liste n'est spécifiée par défaut.
CommandsToRunOnReconnect	CommandsToRunOnReconnect	Spécifie une liste de commandes ou de scripts de commande à exécuter lorsqu'une session est reconnectée après une déconnexion. Aucune liste n'est spécifiée par défaut.
CommandsToRunOnDisconnect	CommandsToRunOnDisconnect	Spécifie la liste des commandes ou des scripts de commande à exécuter lorsqu'une session est déconnectée. Aucune liste n'est spécifiée par défaut.
ConnectionTicketTimeout	VdmConnectionTicketTimeout	Spécifie la durée en secondes pendant laquelle le ticket de connexion View est valide. Si ce paramètre n'est pas configuré, le délai d'expiration par défaut est de 120 secondes.
CredentialFilterExceptions	CredentialFilterExceptions	Spécifie les fichiers exécutables qui ne sont pas autorisés à charger l'agent CredentialFilter. Les noms de fichier ne doivent pas contenir de chemin d'accès ou de suffixe. Utilisez un point-virgule pour séparer plusieurs noms de fichier. Aucune liste n'est spécifiée par défaut.

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 `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\Security`.

Tableau 1-6. Paramètres de sécurité du modèle de configuration d' Horizon Client

Paramètre	Nom de la valeur de registre	Description
`Allow command line credentials`	`AllowCmdLineCredentials`	Détermine si les informations d'identification de l'utilisateur peuvent être fournies avec les options de ligne de commande d'Horizon Client. Si ce paramètre est désactivé, les options `smartCardPIN` et `password` ne sont pas disponibles lorsque l'utilisateur exécute Horizon Client à partir de la ligne de commande. Ce paramètre est activé par défaut.
`Brokers Trusted For Delegation`	`BrokersTrustedForDelegation`	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 **Se connecter en tant qu'utilisateur actuel**. Si vous ne spécifiez aucune instance de Serveur de connexion View, toutes les instances de Serveur de connexion View acceptent ces informations. Pour ajouter une instance de Serveur de connexion View, utilisez l'un des formats suivants : ■ **`domain\system$`** ■ **`system$@domain.com`** ■ Nom principal de service (SPN) du service Serveur de connexion View.

Tableau 1-6. Paramètres de sécurité du modèle de configuration d' Horizon Client (suite)

Paramètre	Nom de la valeur de registre	Description

`Certificate verification mode`	`CertCheckMode`	Configure le niveau de vérification du certificat effectué par Horizon Client. Vous pouvez sélectionner l'un de ces modes :
		■ `No Security`. View n'effectue pas la vérification de certificat.
		■ `Warn But Allow`. Lorsque les problèmes de certificat de serveur suivants se produisent, un avertissement s'affiche, mais l'utilisateur peut continuer à se connecter au Serveur de connexion View :
		  ■ Un certificat auto-signé est fourni par View. Dans ce cas, il est acceptable si son nom ne correspond pas à celui du Serveur de connexion View fourni par l'utilisateur dans Horizon Client.
		  ■ Sur un client ultra léger, la vérification du certificat n'est pas possible, car le magasin d'approbations est vide.
		  Si une autre condition d'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.
		■ `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 des erreurs de certificat à l'utilisateur.
		La valeur par défaut est `Avertir, mais autoriser`.
		IMPORTANT La valeur par défaut de `Avertir, mais autoriser` vise à simplifier le déploiement et les tests dans un environnement de pré-production. Seul le paramètre `Sécurité totale` est recommandé pour la production.
		Lorsque ce paramètre de stratégie de groupe est configuré, les utilisateurs peuvent afficher le mode de vérification de certificat sélectionné dans Horizon Client, mais ne peuvent pas configurer le paramètre. La boîte de dialogue de configuration SSL informe les utilisateurs que l'administrateur a verrouillé le paramètre.
		Lorsque ce paramètre n'est pas configuré ou est désactivé, les utilisateurs d'Horizon Client peuvent configurer SSL et sélectionner un mode de vérification de certificat.
		Pour les clients Windows, si vous ne voulez pas configurer ce paramètre en tant que stratégie de groupe, vous pouvez activer la vérification de certificat en ajoutant le nom de valeur `CertCheckMode` à la clé de registre suivante sur l'ordinateur client :
		`HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security`
		Utilisez les valeurs suivantes dans la clé de registre :
		■ **`0`** implémente `No Security`.
		■ **`1`** implémente `Warn But Allow`.
		■ **`2`** implémente `Full Security`.
		Si vous configurez le paramètre de stratégie de groupe et le paramètre `CertCheckMode` dans la clé de registre, le paramètre de stratégie de groupe est prioritaire sur la valeur de la clé de registre.

Tableau 1-6. Paramètres de sécurité du modèle de configuration d' Horizon Client (suite)

Paramètre	Nom de la valeur de registre	Description
Default value of the 'Log in as current user' checkbox	LogInAsCurrentUser	Spécifie la valeur par défaut de la case à cocher **Ouvrir une session en tant qu'utilisateur actuel** dans la boîte de dialogue de connexion d'Horizon Client. Ce paramètre remplace la valeur par défaut spécifiée pendant l'installation d'Horizon Client. Si un utilisateur exécute Horizon Client depuis la ligne de commande et spécifie l'option `logInAsCurrentUser`, cette valeur remplace ce paramètre. Lorsque la case **Ouvrir une session en tant qu'utilisateur actuel** est cochée, l'identité et les informations d'identification que l'utilisateur a fournies lors de l'ouverture de la session sur le système client sont transmises d'abord à l'instance du Serveur de connexion View, puis au poste de travail ou à l'application View. Lorsque la case est décochée, les utilisateurs doivent fournir leur identité et leurs informations d'identification à plusieurs reprises avant de pouvoir accéder au poste de travail ou à l'application View. Un paramètre Configuration utilisateur est disponible en plus du paramètre Configuration ordinateur. Ces paramètres sont désactivés par défaut.
Display option to Log in as current user	LogInAsCurrentUser_Display	Détermine si la case à cocher **Log in as current user** check box is visible on the Horizon Client connection dialog box. Lorsque la case est visible, les utilisateurs peuvent la cocher ou la décocher et remplacer sa valeur par défaut. Lorsque la case à cocher est masquée, les utilisateurs ne peuvent pas remplacer sa valeur par défaut dans la boîte de dialogue de connexion à Horizon Client. Vous pouvez spécifier la valeur par défaut de la case **Se connecter en tant qu'utilisateur actuel** en utilisant le paramètre de règle `Valeur par défaut de la case à cocher 'Se connecter en tant qu'utilisateur actuel'`. Un paramètre Configuration utilisateur est disponible en plus du paramètre Configuration ordinateur. Ces paramètres sont activés par défaut.
Enable jump list integration	EnableJumplist	Détermine si une liste de raccourcis doit s'afficher dans l'icône Horizon Client icon on the taskbar of Windows 7 and later systems. La liste des raccourcis permet aux utilisateurs de se connecter aux instances récentes du Serveur de connexion View et aux applications et postes de travail View récents. Si Horizon Client est partagé, vous pouvez souhaiter que les utilisateurs ne voient pas les noms des applications et postes de travail récents. Vous pouvez désactiver la liste de raccourcis en désactivant ce paramètre. Ce paramètre est activé par défaut.
Enable Single Sign-On for smart card authentication	EnableSmartCardSSO	Détermine si l'authentification unique est activée pour l'authentification par carte à puce. Lorsque l'authentification unique (Single Sign-On) est activée, Horizon Client stocke le code PIN de la carte à puce chiffrée dans sa mémoire temporaire avant de l'envoyer au Serveur de connexion View. Lorsque l'authentification unique (Single Sign-On) est désactivée, Horizon Client n'affiche pas de boîte de dialogue de code PIN personnalisée. Ce paramètre est désactivé par défaut.
Ignore bad SSL certificate date received from the server	IgnoreCertDateInvalid	Détermine si les erreurs associées aux dates des certificats de serveur non valides sont ignorées. Ces erreurs se produisent quand un serveur envoie un certificat avec une date passée. Ce paramètre est activé par défaut. Ce paramètre s'applique uniquement à View 4.6 et versions antérieures.

Tableau 1-6. Paramètres de sécurité du modèle de configuration d' Horizon Client (suite)

Paramètre	Nom de la valeur de registre	Description
`Ignore certificate revocation problems`	`IgnoreRevocation`	Détermine si les erreurs associées à un certificat de serveur révoqué sont ignorées. Ces erreurs se produisent lorsque le serveur envoie un certificat qui a été révoqué et lorsque le client ne peut pas vérifier l'état de révocation d'un certificat. Ce paramètre est désactivé par défaut. Ce paramètre s'applique uniquement à View 4.6 et versions antérieures.
`Ignore incorrect SSL certificate common name (host name field)`	`IgnoreCertCnInvalid`	Détermine si les erreurs associées à des noms communs de certificats de serveur incorrects sont ignorées. Ces erreurs se produisent quand le nom commun sur le certificat ne correspond pas au nom d'hôte du serveur qui l'envoie. Ce paramètre est désactivé par défaut. Ce paramètre s'applique uniquement à View 4.6 et versions antérieures.
`Ignore incorrect usage problems`	`IgnoreWrongUsage`	Détermine si les erreurs associées à une utilisation incorrecte d'un certificat de serveur sont 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. Ce paramètre est désactivé par défaut. Ce paramètre s'applique uniquement à View 4.6 et versions antérieures.
`Ignore unknown certificate authority problems`	`IgnoreUnknownCa`	Détermine si les erreurs associées à une autorité de certification inconnue sur le certificat du serveur sont ignorées. Ces erreurs se produisent lorsque le serveur envoie un certificat signé par une autorité tierce non approuvée. Ce paramètre est désactivé par défaut. Ce paramètre s'applique uniquement à View 4.6 et versions antérieures.
`EnableTicketSSLAuth`	`EnableTicketSSLAuth`	Active le canal d'infrastructure chiffré SSL. Ce paramètre peut avoir les valeurs suivantes : ■ **Activer** : activez SSL, autorisez le retour aux postes de travail sans prise en charge de SSL. ■ **Désactiver** : désactivez SSL. ■ **Appliquer** : activez SSL, refusez la connexion à des postes de travail sans prise en charge de SSL. La valeur par défaut est **Activer**.
`SSLCipherList`	`SSLCipherList`	Configure la liste de chiffrement pour limiter l'utilisation de certains algorithmes et protocoles cryptographiques avant d'établir une connexion SSL chiffrée. La valeur par défaut est 'SSLv3:TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH'. C'est-à-dire : SSL v3.0, TLS v1.0 et TLS v1.1 sont activés (SSL v2.0 et TLS v1.2 sont désactivés).

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 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 sont stockés dans le registre sur la machine hôte sous `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client`.

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

Paramètre	Nom de la valeur de registre	Description
`Connect all USB devices to the desktop on launch`	`connectUSBOnStartup`	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.
`Connect all USB devices to the desktop when they are plugged in`	`connectUSBOnInsert`	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.
`Logon Password`	`Password`	Spécifie le mot de passe qu'Horizon Client utilise lors de l'ouverture de session. Active Directory stocke ce mot de passe en texte brut. Ce paramètre n'est pas défini 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 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	Attribut	Description
cs-allowunencryptedstartsession	`pae-NameValuePair`	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. 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. 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. 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 View Agent 5.1 ou supérieur 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 certains postes de travail ont des View Agents anciens et s'ils se ne trouvent pas dans des domaines approuvés. Le paramètre par défaut est **1**.

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.
Fichiers journaux	Reportez-vous à la section « Fichiers journaux de View », page 18	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	Système d'exploitation client Windows XP : *<Drive Letter>*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs Système d'exploitation client Windows Vista, Windows 7 et Windows 8 : *<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 avec des 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.

Tableau 1-10. Fichiers journaux de View (suite)

Composant View	Chemin d'accès au fichier et autres informations
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	50001	UDP	PCoIP (pas SALSA20) si PCoIP Secure Gateway est utilisé.
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	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 de	3389	TCP	Trafic Microsoft RDP vers des postes de travail View.
Serveur de sécurité	*	machine virtuelle de	9427	TCP	Redirection Wyse MMR.
Serveur de sécurité	*	machine virtuelle de	32111	TCP	Redirection USB.
Serveur de sécurité	*	machine virtuelle de	4172	TCP	PCoIP (HTTPS) si PCoIP Secure Gateway est utilisé.

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

Source	Port	Cible	Port	Protocole	Description
Serveur de sécurité	*	machine virtuelle de	22443	TCP	HTML Access.
View Agent	4172	Horizon Client	50001	UDP	PCoIP, si PCoIP Secure Gateway n'est pas utilisé.
View Agent	4172	Serveur de connexion View ou serveur de sécurité	55000	UDP	PCoIP (pas SALSA20) si PCoIP Secure Gateway est utilisé.
Horizon Client	*	Serveur de connexion View ou serveur de sécurité	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 « Notes et mises en garde pour les ports TCP et UDP utilisés par View », page 22.
Horizon Client	*	Serveur de sécurité 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 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 22.
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 22.
Horizon Client	*	Serveur de connexion View ou serveur de sécurité	4172	TCP	PCoIP (HTTPS) si PCoIP Secure Gateway est utilisé.
Horizon Client	*	machine virtuelle de	3389	TCP	Trafic Microsoft RDP vers des postes de travail View si des connexions directes sont utilisées à la place de connexions par tunnel.
Horizon Client	*	machine virtuelle de	9427	TCP	Redirection Wyse MMR si des connexions directes sont utilisées à la place de connexions par tunnel.
Horizon Client	*	machine virtuelle de	32111	TCP	Redirection USB si des connexions directes sont utilisées à la place de connexions par tunnel.
Horizon Client	*	View Agent	4172	TCP	PCoIP (HTTPS) si PCoIP Secure Gateway n'est pas utilisé.
Horizon Client	50001	View Agent	4172	UDP	PCoIP, si PCoIP Secure Gateway n'est pas utilisé.

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

Source	Port	Cible	Port	Protocole	Description
Horizon Client	50001	Serveur de connexion View ou serveur de sécurité	4172	UDP	PCoIP (pas SALSA20) si PCoIP Secure Gateway est utilisé.
Navigateur Web	*	Serveur de sécurité	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 ou View Composer	443	TCP	Messages SOAP si SSL est activé pour l'accès à vCenter Server ou 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	50001	UDP	PCoIP (pas SALSA20) si PCoIP Secure Gateway via Serveur de connexion View est utilisé.
Serveur de connexion View	*	Serveur de connexion View	4100	TCP	Trafic interroutage JMS.
Serveur de connexion View	*	machine virtuelle de	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 de	4172	TCP	PCoIP (HTTPS) si PCoIP Secure Gateway via le Serveur de connexion View est utilisé.
Serveur de connexion View	*	machine virtuelle de	9427	TCP	Redirection Wyse MMR si des connexions par tunnel via le Serveur de connexion View sont utilisées.
Serveur de connexion View	*	machine virtuelle de	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 Cloud Pod Architecture.
Serveur de connexion View	*	Serveur de connexion View	22389	TCP	Pour la réplication LDAP globale dans Cloud Pod Architecture.
Serveur de connexion View	*	Serveur de connexion View	22636	TCP	Pour la réplication LDAP globale sécurisée dans Cloud Pod Architecture.
machine virtuelle de	*	Instances de Serveur de connexion View	4001	TCP	Trafic JMS.
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. Consultez la section « Décharger des connexions SSL sur des serveurs intermédiaires » dans le document *Administration de VMware Horizon 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 50001 est en cours d'utilisation, le client choisira le port 50002. Si ce dernier est en cours d'utilisation, le client choisira le port 50003, et ainsi de suite. Vous devez configurer le pare-feu avec la valeur ANY lorsque 50001 figure 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 View 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 View	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 View Framework	Manuel	Fournit des services de journalisation des événements, de sécurité et d'infrastructure COM+. 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
Composant du bus de message VMware Horizon View	Manuel	Fournit des services de messagerie entre les composants View. Ce service doit toujours être en cours d'exécution.
VMware Horizon View 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 View	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 View Security Gateway	Manuel	Fournit des services de passerelle communs. Ce service doit toujours être en cours d'exécution.
Composant Web VMware Horizon View	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 View 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 View	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 View 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 View 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 View 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 stratégies par défaut et les procédures pour configurer des stratégies ont été modifiées dans View 5.2. Pour plus d'informations sur les versions antérieures de View, consultez l'article 1021466 de la base de connaissances VMware à l'adresse http://kb.vmware.com/kb/1021466.

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

Certains protocoles de sécurité et suites de chiffrement sont fournis par défaut dans View 5.2 et versions supérieures. Par défaut, les stratégies d'acceptation et de proposition générales sont très similaires.

Tableau 1-14. Stratégies générales par défaut

Protocoles de sécurité par défaut	Suites de chiffrement par défaut
■ `TLS 1.1` ■ `TLS 1.0` ■ `SSLv2Hello` (stratégie d'acceptation uniquement)	■ `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA` ■ `TLS_DHE_DSS_WITH_AES_128_CBC_SHA` ■ `TLS_DHE_RSA_WITH_AES_128_CBC_SHA` ■ `TLS_RSA_WITH_AES_128_CBC_SHA` ■ `SSL_RSA_WITH_RC4_128_SHA`

Vous pouvez modifier les stratégies par défaut comme suit :

- Si tous les clients se connectant prennent en charge `TLS 1.1`, vous pouvez supprimer `TLS 1.0` et `SSLv2Hello` de la stratégie d'acceptation.
- Vous pouvez ajouter `TLS 1.2` aux stratégies d'acceptation et de proposition, qui sera ensuite sélectionné si l'autre extrémité de la connexion prend en charge `TLS 1.2`.
- Si tous les clients se connectant prennent en charge les suites de chiffrement `AES`, vous pouvez supprimer `SSL_RSA_WITH_RC4_128_SHA` de la stratégie d'acceptation.

Mise à jour des fichiers de stratégie JCE pour prendre en charge les suites de chiffrement à haute résistance

Vous pouvez ajouter des suites de chiffrement à haute résistance pour une meilleure assurance, mais vous devez d'abord mettre à jour les fichiers de stratégie `local_policy.jar` et `US_export_policy.jar` pour JRE 7 sur chaque instance de Serveur de connexion View et sur chaque serveur de sécurité. Vous mettez à jour ces fichiers de stratégie en téléchargeant Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 7 sur le site de téléchargement d'Oracle Java SE.

Si vous incluez des suites de chiffrement à haute résistance dans la liste et que vous ne remplacez pas les fichiers de stratégie, vous ne pouvez pas redémarrer le service Serveur de connexion VMware Horizon View.

Les fichiers de stratégie sont situés dans le répertoire `C:\Program Files\VMware\VMware View\Server\jre\lib\security`.

Pour plus d'informations sur le téléchargement de JCE Unlimited Strength Jurisdiction Policy Files 7, rendez-vous sur le site de téléchargement d'Oracle Java SE : http://www.oracle.com/technetwork/java/javase/downloads/index.html.

Après avoir mis à jour les fichiers de stratégie, vous devez créer des sauvegardes des fichiers. Si vous mettez à niveau l'instance de Serveur de connexion View ou le serveur de sécurité, toutes les modifications que vous apportez à ces fichiers pourront être écrasées et vous devrez peut-être restaurer les fichiers à partir de la sauvegarde.

Configuration des stratégies d'acceptation et de proposition générales

Les stratégies d'acceptation et de proposition générales par défaut sont définies dans les attributs View LDAP. Ces stratégies s'appliquent à toutes les instances de Serveur de connexion View 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 :

```
pae-ServerSSLSecureProtocols = "\LIST: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 :

```
pae-ServerSSLCipherSuites = "\LIST:TLS_DHE_RSA_WITH_AES_128_CBC_SHA,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 :

```
pae-ClientSSLSecureProtocols = "\LIST: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_DHE_RSA_WITH_AES_128_CBC_SHA,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 25.
- 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=security protocol`*.

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

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=TLSv1.1
secureProtocols.2=TLSv1
secureProtocols.3=SSLv2Hello

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

preferredSecureProtocol=TLSv1.1

# The order of the following list is unimportant:

enabledCipherSuite.1=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
enabledCipherSuite.2=TLS_DHE_DSS_WITH_AES_128_CBC_SHA
enabledCipherSuite.3=TLS_DHE_RSA_WITH_AES_128_CBC_SHA
enabledCipherSuite.4=TLS_RSA_WITH_AES_128_CBC_SHA
enabledCipherSuite.5=SSL_RSA_WITH_RC4_128_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.
- La norme RFC 6797 Strict Transport Security (HSTS), également appelée sécurité du transport, est activée par défaut.
- La norme RFC 7034 Header Field X-Frame-Options, également appelée contournement du clickjacking, est désactivée par défaut. Vous pouvez l'activer en ajoutant l'entrée `x-frame-options=<options>` 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 26. Le paramètre `<options>` peut avoir l'une des valeurs suivantes (sensibles à la casse) :
  - `OFF` - Désactiver le contournement du clickjacking (par défaut).
  - `DENY` - Ne pas utiliser les trames.
  - `SAMEORIGIN` - Ne pas utiliser de trames étrangères.

- `ALLOW-FROM <URL>` - Ne pas utiliser les trames étrangères, sauf <URL>, où <URL> spécifie une origine approuvée supplémentaire.

Pour plus informations sur la norme RFC 7034, reportez-vous à http://tools.ietf.org/html/rfc7034.

Remarque Le contournement du clickjacking empêche le bon fonctionnement de HTML Access lors de l'utilisation d'une Blast Secure Gateway (BSG), c'est pourquoi il est désactivé par défaut.

Perfect Forward Secrecy

PFS (Perfect Forward Secrecy) garantit que la remise en cause de la sécurité d'une session SSL n'affecte pas les autres sessions SSL qui utilisent le même certificat de serveur. Il s'agit d'une propriété des suites de chiffrement dont le nom inclut les lettres DHE. Parmi les cinq suites de chiffrement que nous activons par défaut, trois suites possèdent cette propriété. Comme PFS risque de réduire les performances, il convient de rechercher un équilibre.

View prend en charge les suites de chiffrement DHE-DSS, DHE-RSA et ECDHE-RSA. Les deux premières peuvent être activées avec des certificats DSS ou RSA standard. ECDHE-RSA offre de meilleures performances mais nécessite un certificat ECC signé avec une clé RSA. Ne demandez pas à une autorité de certification un certificat ECC signé avec une clé EC, car View ne peut pas l'utiliser.

Index