Sécurité de VMware View

View 5.0
View Manager 5.0
View Composer 2.7

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-000575-00

vmware®

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

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

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 VMware View 5

Référence sur la sécurité de VMware View 7
- Comptes VMware View 8
- Paramètres de sécurité de VMware View 9
- Ressources de VMware View 18
- Fichiers journaux de VMware View 19
- Ports TCP et UDP de VMware View 20
- Services sur un hôte de View Connection Server 25
- Services sur un serveur de sécurité 26
- Services sur un hôte de View Transfer Server 26

Index 29

Sécurité de VMware View

Sécurité de VMware View fournit une référence succincte sur les fonctions de sécurité de VMware 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 fonctionnement correct de VMware 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 VMware View. Ce guide de référence doit être utilisé avec le guide *VMware View Hardening Guide* et les autres documentations de VMware View.

Référence sur la sécurité de VMware 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.

- Comptes VMware View page 8

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

- Paramètres de sécurité de VMware View page 9

  VMware View comporte 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 VMware View page 18

  VMware View comporte plusieurs fichiers de configuration et ressources similaires qui doivent être protégés.

- Fichiers journaux de VMware View page 19

  Le logiciel VMware View crée des fichiers journaux enregistrant l'installation et le fonctionnement de ses composants.

- Ports TCP et UDP de VMware View page 20

  View utilise des ports TCP et UDP pour l'accès au réseau entre ses composants. Vous pouvez avoir à reconfigurer un pare-feu pour autoriser l'accès sur les ports appropriés.

- Services sur un hôte de View Connection Server page 25

  Le fonctionnement de View Manager dépend de plusieurs services s'exécutant sur un hôte de View Connection Server. Si vous voulez ajuster le fonctionnement de ces services, il est important que vous les connaissiez.

- Services sur un serveur de sécurité page 26

  Le fonctionnement de View Manager dépend de plusieurs services s'exécutant sur un serveur de sécurité. Si vous voulez ajuster le fonctionnement de ces services, il est important que vous les connaissiez.

- Services sur un hôte de View Transfer Server page 26

  Les opérations de transfert pour les postes de travail locaux dépendent des services qui s'exécutent sur un hôte de View Transfer Server. Si vous voulez ajuster le fonctionnement de ces services, il est important que vous les connaissiez.

Comptes VMware View

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

Tableau 1. Comptes de système VMware View

Composant VMware View	Comptes requis
View Client	Configurez des comptes d'utilisateur dans Active Directory pour les utilisateurs qui ont accès à des postes de travail View. 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.
View Client avec mode local	Configurez des comptes d'utilisateur dans Active Directory pour les utilisateurs qui ont accès à des postes de travail View en mode local. Les comptes d'utilisateur ne requièrent pas de privilèges d'administrateur View. En tant que meilleure pratique standard pour les postes de travail, assurez-vous qu'un mot de passe unique est créé pour le compte d'administrateur local sur chaque poste de travail View que vous prévoyez d'utiliser en mode local.
vCenter Server	Configurez un compte d'utilisateur dans Active Directory avec une autorisation d'effectuer les opérations dans vCenter Server qui sont nécessaires pour prendre en charge View Manager. Pour plus d'informations sur les privilèges requis, consultez le document *Installation de VMware 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, consultez le document *Installation de VMware View*.
View Connection Server, Security Server ou View Transfer Server	À l'origine, tous les utilisateurs qui sont membres du groupe d'administrateurs local (BUILTIN\Administrators) sur l'ordinateur View Connection Server sont autorisés à ouvrir une session sur View Administrator. Dans View Administrator, vous pouvez utiliser **[View Configuration (Configuration de View)] > [Administrators (Administrateurs)]** pour modifier la liste d'administrateurs de View. Pour plus d'informations sur les privilèges requis, consultez le document *Administration de VMware View*.

Tableau 2. Comptes de base de données VMware View

Composant VMware 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, consultez le document *Installation de VMware View*.
Base de données des événements utilisée par View Connection Server	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, consultez le document *Installation de VMware View*.

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

- Configurez des bases de données View sur des serveurs séparés d'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 VMware View

VMware View comporte 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 liés à la sécurité pour les sessions et les connexions client sont accessibles sous **[View Configuration (Configuration de View)] > [Global Settings (Paramètres généraux)]** dans View Administrator.

Tableau 3. Paramètres généraux liés à la sécurité

Paramètre	Description
[Disable Single Sign-on for Local Mode operations (Désactiver l'authentification unique pour les opérations en mode local)]	Détermine si l'authentification unique est activée lorsque des utilisateurs ouvrent une session sur leurs postes de travail locaux. Ce paramètre est désactivé par défaut.
[Enable automatic status updates (Activer les mises à jour d'état automatiques)]	Détermine si View Manager met régulièrement à jour le volet d'état général et le tableau de bord dans View Administrator. Si vous activez ce paramètre, les sessions inactives n'expirent pas pour les utilisateurs dont une session est ouverte sur View Administrator. Ce paramètre est désactivé par défaut.
[Message security mode (Mode de sécurité des messages)]	Détermine si la signature et la vérification des messages JMS transmis entre les composants View Manager ont lieu. Si le paramètre est réglé sur **[Disabled (Désactivé)]**, le mode de sécurité des messages est désactivé. Si le paramètre est réglé sur **[Enabled (Activé)]**, les composants View rejettent les messages non signés. Si le paramètre est réglé sur **[Mixed (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 **[Disabled (Désactivé)]**.
[Authentifier à nouveau les connexions par tunnel sécurisées après une interruption de réseau]	Détermine si les informations d'identification d'utilisateur doivent être réauthentifiées après une interruption de réseau lorsque des clients View utilisent des connexions par tunnel sécurisé vers des postes de travail View. Ce paramètre est activé par défaut.

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

Paramètre	Description
[Require SSL for client connections and View Administrator (SSL requis pour les connexions client et View Administrator)]	Détermine si un canal de communication sécurisé SSL est utilisé entre View Connection Server et des clients de poste de travail View, et entre View Connection Server et des clients qui accèdent à View Administrator. Ce paramètre est activé par défaut.
[Session timeout (Délai d'expiration de la session)]	Détermine la durée pendant laquelle un utilisateur peut garder une session ouverte après l'ouverture de session sur View Connection Server. La valeur par défaut est de 600 minutes.

Pour plus d'informations sur ces paramètres et leurs implications en matière de sécurité, consultez le document *Administration de VMware View*.

Paramètres de serveur liés à la sécurité dans View Administrator

Les paramètres de serveur liés à la sécurité sont accessibles sous **[View Configuration (Configuration de View)] > [Server]** dans View Administrator.

Tableau 4. Paramètres de serveur liés à la sécurité

Paramètre	Description
[Connect using SSL (Connexion avec SSL)]	Si ce paramètre est activé, View communique avec vCenter Server à l'aide du chiffrement SSL. Ce paramètre est activé par défaut.
[Use PCoIP Secure Gateway for PCoIP connections to desktop (Utiliser PCoIP Secure Gateway pour des connexions PCoIP vers le poste de travail)]	Si ce paramètre est activé, View Client effectue une autre connexion sécurisée avec l'hôte de View Connection Server ou du serveur de sécurité lorsque des utilisateurs se connectent à un poste de travail View avec le protocole d'affichage PCoIP. Si ce paramètre est désactivé, la session de postes de travail est établie directement entre le système client et la machine virtuelle de poste de travail View, en outrepassant l'hôte de View Connection Server ou du serveur de sécurité. Ce paramètre est désactivé par défaut.
[Use secure tunnel connection to desktop (Utiliser une connexion par tunnel vers le poste de travail)]	Si ce paramètre est activé, View Client effectue une autre connexion HTTPS avec l'hôte de View Connection Server ou du serveur de sécurité lorsque des utilisateurs se connectent à un poste de travail View. Si ce paramètre est désactivé, la session de postes de travail est établie directement entre le système client et la machine virtuelle de poste de travail View, en outrepassant l'hôte de View Connection Server ou du serveur de sécurité. Ce paramètre est activé par défaut.
[Use secure tunnel connection for Local Mode operations (Utiliser une connexion par tunnel sécurisée pour des opérations en mode local)]	Si ce paramètre est activé, les postes de travail locaux utilisent des communications par tunnel. Le trafic du réseau est routé via View Connection Server ou un serveur de sécurité, si un serveur de ce type est configuré. Si ce paramètre est désactivé, les transferts de données ont lieu directement entre des postes de travail locaux et les postes de travail distants correspondants dans le datacenter. Ce paramètre est désactivé par défaut.

Tableau 4. Paramètres de serveur liés à la sécurité (suite)

Paramètre	Description
[Use SSL for Local Mode operations (Utiliser SSL pour des opérations en mode local)]	Si ce paramètre est activé, les communications et les transferts de données entre des ordinateurs client et le datacenter utilisent le chiffrement SSL. Ces opérations comprennent la restitution et l'emprunt de postes de travail et la réplication de données depuis des ordinateurs client vers le datacenter, mais n'incluent pas les transferts d'images de base de View Composer. Ce paramètre est désactivé par défaut.
[Use SSL when provisioning desktops in Local Mode (Utiliser SSL lors de l'approvisionnement de postes de travail en mode local)]	Si ce paramètre est activé, les transferts de fichiers d'image de base View Composer depuis le référentiel de Transfer Server vers des ordinateurs client utilisent le chiffrement SSL. Ce paramètre est désactivé par défaut.

Pour plus d'informations sur ces paramètres et leurs implications en matière de sécurité, consultez le document *Administration de VMware 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 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 les clients non View peuvent se connecter directement à des postes de travail View avec RDP. Lorsque ce paramètre est désactivé, View Agent n'autorise que les connexions gérées par View via View Client. **Important** Pour que View fonctionne correctement, le service Windows Terminal Services doit être exécuté sur le système d'exploitation client 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 une authentification unique (SSO) est utilisée pour connecter des utilisateurs à des postes de travail View. Lorsque ce paramètre est activé, les utilisateurs doivent uniquement saisir leurs informations d'identification lors de la connexion à View 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.

Tableau 5. Paramètres liés à la sécurité dans le modèle pour la configuration de View Agent (suite)

Paramètre	Nom de la valeur de registre	Description
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.
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 matière de sécurité, consultez le document *Administration de VMware View*.

Paramètres de sécurité dans le modèle pour la configuration de View Client

Les paramètres liés à la sécurité sont fournis dans le fichier de modèle d'administration pour View 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 6. Paramètres de sécurité dans le modèle pour la configuration de View Client

Paramètre	Nom de la valeur de registre	Description
Allow command line credentials (Autoriser les informations d'identification de ligne de commande)	AllowCmdLineCredentials	Détermine si les informations d'identification d'utilisateur peuvent être fournies avec des options de ligne de commande View Client. Si ce paramètre est activé, les options `smartCardPIN` et `password` ne sont pas disponibles lorsque les utilisateurs exécutent View Client à partir de la ligne de commande. Ce paramètre est activé par défaut.
Brokers Trusted For Delegation (Brokers approuvés pour la délégation)	BrokersTrustedForDelegation	Spécifie les instances de View Connection Server 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 View Connection Server, toutes les instances de View Connection Server acceptent ces informations. Pour ajouter une instance de View Connection Server, utilisez l'un des formats suivants : ■ **`domain\system$`** ■ **`system$@domain.com`** ■ Nom principal de service (SPN) du service View Connection Server.

Tableau 6. Paramètres de sécurité dans le modèle pour la configuration de View Client (suite)

Paramètre	Nom de la valeur de registre	Description
`Certificate verification mode`	`CertCheckMode`	Configure le niveau de la vérification de certificat exécutée par View Client. Vous pouvez sélectionner l'un de ces modes : ■ `No Security` (Pas de sécurité). View n'effectue pas la vérification de certificat. ■ `Warn But Allow` (Avertir, mais autoriser). Lorsque les problèmes de certificat de serveur suivants se produisent, un avertissement s'affiche, mais l'utilisateur peut continuer à se connecter à View Connection Server : ■ Un certificat auto-signé est fourni par View. Dans ce cas, il est acceptable si le nom de certificat ne correspond pas au nom de View Connection Server fourni par l'utilisateur dans View Client. ■ Un certificat vérifiable qui a été configuré dans votre déploiement a expiré ou n'est pas encore valide.

Tableau 6. Paramètres de sécurité dans le modèle pour la configuration de View Client (suite)

Paramètre	Nom de la valeur de registre	Description
		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 à View Connection Server. `Warn But Allow` (Avertir, mais autoriser) est la valeur par défaut. ■ `Full Security`. Si une erreur de type de certificat se produit, l'utilisateur ne peut pas se connecter à View Connection Server. View affiche des erreurs de certificat à l'utilisateur. Pour permettre à View Client de réaliser des vérifications du type de certificat, vous devez sélectionner le paramètre général **[Require SSL for client connections and View Administrator (SSL requis pour les connexions client et View Administrator)]** dans View Administrator. Lorsque ce paramètre de stratégie de groupe est configuré, les utilisateurs peuvent voir le mode de vérification de certificat sélectionné dans View Client, mais ils ne peuvent pas configurer le paramètre. La boîte de dialogue de configuration SSL informe les utilisateurs que l'administrateur a verrouillé le paramètre. Lorsque ce paramètre n'est pas configuré ou est désactivé, les utilisateurs de View 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` (Pas de sécurité). ■ **`1`** implémente `Warn But Allow` (Avertir, mais autoriser). ■ **`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 6. Paramètres de sécurité dans le modèle pour la configuration de View Client (suite)

Paramètre	Nom de la valeur de registre	Description
Default value of the 'Log in as current user' checkbox (Valeur par défaut de la case à cocher 'Log in as current user (Se connecter en tant qu'utilisateur actuel))	LogInAsCurrentUse	Spécifie la valeur par défaut de la case **[Se connecter en tant qu'utilisateur actuel]** dans la boîte de dialogue de connexion de View Client. Ce paramètre remplace la valeur par défaut spécifiée lors de l'installation de View Client. Si un utilisateur exécute View Client à partir de la ligne de commande et qu'il spécifie l'option `logInAsCurrentUser`, cette valeur remplace ce paramètre. Lorsque la case **[Se connecter en tant qu'utilisateur actuel]** est cochée, l'identité et les informations d'identification que l'utilisateur a fournies lors de l'ouverture de session sur le système client sont transmises à l'instance de View Connection Server, puis au poste de travail View. Lorsque la case est décochée, les utilisateurs doivent fournir leur identité et leurs informations d'identification plusieurs fois avant de pouvoir accéder à un poste de travail 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 (Option d'affichage pour l'option Log in as current user (Se connecter en tant qu'utilisateur actuel))	LogInAsCurrentUser_Display	Détermine si la case **[Se connecter en tant qu'utilisateur actuel]** est visible dans la boîte de dialogue de connexion de View Client. Lorsque la case est visible, les utilisateurs peuvent la cocher ou la décocher et remplacer sa valeur par défaut. Lorsque la case est masquée, les utilisateurs ne peuvent pas remplacer sa valeur par défaut dans la boîte de dialogue de connexion de View Client. Vous pouvez spécifier la valeur par défaut de la case **[Se connecter en tant qu'utilisateur actuel]** en utilisant le paramètre de stratégie `Default value of the 'Log in as current user' checkbox (Valeur par défaut de la case 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 (Activer l'intégration des listes de raccourcis)	EnableJumplist	Détermine si une liste de raccourcis apparaît dans l'icône de View Client sur la barre des tâches de Windows 7 et des systèmes supérieurs. La liste de raccourcis permet aux utilisateurs de se connecter à des instances de View Connection Server et des postes de travail View récents. Si View Client est partagé, il se peut que vous ne vouliez pas que les utilisateurs voient les noms des 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 (Activer l'authentification unique pour l'authentification par carte à puce)	EnableSmartCardSSO	Détermine si l'authentification unique est activée pour l'authentification par carte à puce. Lorsque l'authentification unique est activée, View Client stocke le code PIN de carte à puce crypté dans la mémoire temporaire avant de le soumettre à View Connection Server. Lorsque l'authentification unique est désactivée, View Client n'affiche pas de boîte de dialogue de code PIN personnalisé. Ce paramètre est désactivé par défaut.

Tableau 6. Paramètres de sécurité dans le modèle pour la configuration de View Client (suite)

Paramètre	Nom de la valeur de registre	Description
Ignore bad SSL certificate date received from the server (Ignorer la date incorrecte de certificat SSL reçue depuis le serveur)	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.
Ignore certificate revocation problems (Ignorer les problèmes de révocation de certificat)	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) (Ignorer le nom commun de certificat SSL incorrect (champ de nom d'hôte))	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 (Ignorer les problèmes d'utilisation incorrecte)	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 (Ignorer les problèmes d'autorité de certification inconnue)	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.

Pour plus d'informations sur ces paramètres et leurs implications en matière de sécurité, consultez le document *Administration de VMware View*.

Paramètres liés à la sécurité dans la section Définitions de script du modèle pour la configuration de View Client

Les paramètres liés à la sécurité sont fournis dans la section Définitions de script du fichier de modèle d'administration pour View 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 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 (Connecter tous les périphériques USB au poste de travail au démarrage)	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 (Connecter tous les périphériques USB au poste de travail lors de leur branchement)	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 (Mot de passe d'ouverture de session)	Password	Spécifie le mot de passe que View 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 matière de sécurité, consultez le document *Administration de VMware 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 de View Connection Server. La modification se propage automatiquement à toutes les autres instances de View Connection Server dans un groupe.

Tableau 8. Paramètres liés à la sécurité dans View LDAP

Paire nom/valeur	Attribut	Description
[cs-allowunencryptedstartsession]	`pae-NameValuePair`	Permet d'utiliser la protection par clé statique pour l'authentification unique sur des postes de travail qui ne se trouvent pas dans un domaine approuvé sur lequel la négociation SSPI (Security Support Provider Interface) est prise en charge. La protection par clé statique est connue pour être un peu moins sûre que SSPI. Si le paramètre est réglé sur **[0]**, la protection par clé statique n'est pas autorisée. Ce paramètre est approprié si tous les postes de travail se trouvent dans des domaines approuvés. Si la négociation SSPI échoue, la session ne démarre pas. Si le paramètre est réglé sur **[1]**, la protection par clé statique peut être utilisée si la négociation SSPI échoue. Ce paramètre est approprié si certains postes de travail ne se trouvent pas dans des domaines approuvés. Le paramètre par défaut est **[1]**.
	`pae-OVDIKeyCipher`	Spécifie le cryptage de clé de chiffrement que View Connection Server utilise pour chiffrer le fichier de disque virtuel (`.vmdk`) lorsque des utilisateurs restituent et empruntent un poste de travail local. Vous pouvez définir la valeur du cryptage de clé de chiffrement sur **[AES-128]**, **[AES-192]** ou **[AES-256]**. La valeur par défaut est **[AES-128]**.
	`pae-SSOCredentialCacheTimeout`	Définit la limite d'expiration de l'authentification unique (SSO) en minutes après laquelle les informations d'identification SSO d'un utilisateur ne sont plus valides. La valeur par défaut est **[15]**. Une valeur de **[-1]** signifie qu'aucune limite du délai d'expiration SSO n'est définie. Une valeur de **[0]** désactive l'authentification unique.

Ressources de VMware View

VMware View comporte plusieurs fichiers de configuration et ressources similaires qui doivent être protégés.

Tableau 9. Ressources de View Connection Server et de serveur de sécurité

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	*<Drive Letter>*`:\Programdata\VMWare\VDM\backups` (Windows Server 2008) *<Drive Letter>*`:\Documents and Settings\All Users\Application Data\VMWare\VDM\backups` (Windows Server 2003)	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 9. Ressources de View Connection Server et de serveur de sécurité (suite)

Ressource	Emplacement	Protection
Fichiers journaux	*%ALLUSERSPROFILE%*\Application Data\VMware\VDM\logs *<Drive Letter>*:\Documents and Settings\All Users\Application Data\VMware\VDM\logs	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.

Tableau 10. Ressources de View Transfer Server

Ressource	Emplacement	Protection
httpd.conf (Fichier de configuration Apache)	*install_directory*\VMware\VMware View\Server\httpd\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	*<Drive Letter>*:\ProgramData\VMware\VDM\logs (Windows Server 2008 R2) *%ALLUSERSPROFILE%*\Application Data\VMware\VDM\logs (Windows Server 2003 et Windows Server 2003 R2) *<Drive Letter>*:\Program Files\Apache Group\Apache2\logs (serveur Apache)	Protégé par un contrôle d'accès.

Fichiers journaux de VMware View

Le logiciel VMware View crée des fichiers journaux enregistrant l'installation et le fonctionnement de ses composants.

Remarque Les fichiers journaux de VMware 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, consultez les documents *Installation de VMware View* et *Intégration de VMware View*.

Tableau 11. Fichiers journaux de VMware View

Composant VMware 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 et Windows 7 : *<Drive Letter>*:\ProgramData\VMware\VDM\logs Si un disque de données utilisateur (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 11. Fichiers journaux de VMware View (suite)

Composant VMware View	Chemin d'accès au fichier et autres informations

View Client with Local Mode	Système d'exploitation hôte Windows XP :
	`C:\Documents and Settings\%username%\Local Settings\Application Data\VMware\VDM\Logs\`
	Système d'exploitation hôte Windows Vista et Windows 7 :
	`C:\Users\%username%\AppData\VMware\VDM\Logs\`

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.
View Connection Server ou serveur de sécurité	*%ALLUSERSPROFILE%*`\Application Data\VMware\VDM\logs\*.txt` sur le serveur. *<Drive Letter>*`:\Documents and Settings\All Users\Application Data\VMware\VDM\logs\*.txt` sur le serveur. 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.
View Transfer Server	Windows Server 2008 R2 : *<Drive Letter>*`:\ProgramData\VMware\VDM\logs\*.txt` Windows Server 2003 et Windows Server 2003 R2 : *%ALLUSERSPROFILE%*`\Application Data\VMware\VDM\logs\*.txt` Serveur Apache : *<Drive Letter>*`:\Program Files\Apache Group\Apache2\logs\error.log`

Ports TCP et UDP de VMware View

View utilise des ports TCP et UDP pour l'accès au réseau entre ses composants. Vous pouvez avoir à reconfigurer un pare-feu pour autoriser l'accès sur les ports appropriés.

Tableau 12. Ports TCP et UDP utilisés par View, en excluant Local Mode

Source	Port	Cible	Port	Protocole	Description
Serveur de sécurité	4172	View Agent 4.5 ou antérieur	50002 (peut être modifié par stratégie de groupe)	UDP	PCoIP (AES-128-GCM uniquement) si PCoIP Secure Gateway est utilisé.
Serveur de sécurité	4172	View Agent 4.6 ou supérieur	4172	UDP	PCoIP (AES-128-GCM uniquement) si PCoIP Secure Gateway est utilisé.
Serveur de sécurité	4172	View Client 4.5 ou antérieur	50002 (ne peut pas être modifié)	UDP	PCoIP (AES-128-GCM uniquement) si PCoIP Secure Gateway est utilisé.

Tableau 12. Ports TCP et UDP utilisés par View, en excluant Local Mode (suite)

Source	Port	Cible	Port	Protocole	Description
Serveur de sécurité	4172	View Client 4.6 ou supérieur	4172	UDP	PCoIP (AES-128-GCM uniquement) si PCoIP Secure Gateway est utilisé.
Serveur de sécurité	*	View Connection Server	4001	TCP	Trafic JMS.
Serveur de sécurité	*	View Connection Server	8009	TCP	Trafic Web AJP13.
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	*	Poste de travail View 4.5 ou antérieur	50002 (peut être modifié par stratégie de groupe)	TCP	PCoIP (HTTPS) si PCoIP Secure Gateway est utilisé.
Serveur de sécurité	*	Poste de travail View 4.6 ou supérieur	4172	TCP	PCoIP (HTTPS) si PCoIP Secure Gateway est utilisé.
View Agent 4.5 ou antérieur	50002 (peut être modifié par stratégie de groupe)	View Client 4.5 ou antérieur	50002 (ne peut pas être modifié)	UDP	PCoIP (AES-128-GCM ou SALSA20) si PCoIP Secure Gateway n'est pas utilisé.
View Agent 4.5 ou antérieur	50002 (peut être modifié par stratégie de groupe)	View Client 4.6 ou supérieur	4172	UDP	PCoIP (AES-128-GCM ou SALSA20) si PCoIP Secure Gateway n'est pas utilisé.
View Agent 4.6 ou supérieur	4172	View Client 4.5 ou antérieur	50002 (ne peut pas être modifié)	UDP	PCoIP (AES-128-GCM ou SALSA20) si PCoIP Secure Gateway n'est pas utilisé.
View Agent 4.6 ou supérieur	4172	View Client 4.6 ou supérieur	4172	UDP	PCoIP (AES-128-GCM ou SALSA20) si PCoIP Secure Gateway n'est pas utilisé.
View Agent 4.5 ou antérieur	50002 (peut être modifié par stratégie de groupe)	View Connection Server ou serveur de sécurité	4172	UDP	PCoIP (AES-128-GCM uniquement) si PCoIP Secure Gateway est utilisé.
View Agent 4.6 ou supérieur	4172	View Connection Server ou serveur de sécurité	4172	UDP	PCoIP (AES-128-GCM uniquement) si PCoIP Secure Gateway est utilisé.
View Client	*	View Connection Server ou serveur de sécurité	80	TCP	Accès HTTP si SSL est désactivé pour les connexions client.
View Client	*	View Connection Server ou serveur de sécurité	443	TCP	Accès HTTPS si SSL est activé pour les connexions client.

Tableau 12. Ports TCP et UDP utilisés par View, en excluant Local Mode (suite)

Source	Port	Cible	Port	Protocole	Description
View Client	*	View Connection Server ou serveur de sécurité	4172	TCP	PCoIP (HTTPS) si PCoIP Secure Gateway est utilisé.
View 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.
View Client	*	machine virtuelle de	9427	TCP	Redirection Wyse MMR si des connexions directes sont utilisées à la place de connexions par tunnel.
View Client	*	machine virtuelle de	32111	TCP	Redirection USB si des connexions directes sont utilisées à la place de connexions par tunnel.
View Client 4.5 ou antérieur	*	View Agent 4.5 ou antérieur	50002 (peut être modifié par stratégie de groupe)	TCP	PCoIP (HTTPS) si PCoIP Secure Gateway n'est pas utilisé.
View Client 4.5 ou antérieur	50002 (ne peut pas être modifié)	View Agent 4.5 ou antérieur	50002 (peut être modifié par stratégie de groupe)	UDP	PCoIP (AES-28-GCM ou SALSA20) si PCoIP Secure Gateway n'est pas utilisé.
View Client 4.5 ou antérieur	*	View Agent 4.6 ou supérieur	4172	TCP	PCoIP (HTTPS) si PCoIP Secure Gateway n'est pas utilisé.
View Client 4.5 ou antérieur	50002 (ne peut pas être modifié)	View Agent 4.6 ou supérieur	4172	UDP	PCoIP (AES-28-GCM ou SALSA20) si PCoIP Secure Gateway n'est pas utilisé.
View Client 4.5 ou antérieur	50002 (ne peut pas être modifié)	View Connection Server ou serveur de sécurité	4172	UDP	PCoIP (AES-128-GCM uniquement) si PCoIP Secure Gateway est utilisé.
View Client 4.6 ou supérieur	*	View Agent 4.5 ou antérieur	50002 (peut être modifié par stratégie de groupe)	TCP	PCoIP (HTTPS) si PCoIP Secure Gateway n'est pas utilisé.
View Client 4.6 ou supérieur	4172	View Agent 4.5 ou antérieur	50002 (peut être modifié par stratégie de groupe)	UDP	PCoIP (AES-28-GCM ou SALSA20) si PCoIP Secure Gateway n'est pas utilisé.
View Client 4.6 ou supérieur	*	View Agent 4.6 ou supérieur	4172	TCP	PCoIP (HTTPS) si PCoIP Secure Gateway n'est pas utilisé.
View Client 4.6 ou supérieur	4172	View Agent 4.6 ou supérieur	4172	UDP	PCoIP (AES-28-GCM ou SALSA20) si PCoIP Secure Gateway n'est pas utilisé.

Tableau 12. Ports TCP et UDP utilisés par View, en excluant Local Mode (suite)

Source	Port	Cible	Port	Protocole	Description
View Client 4.6 ou supérieur	4172	View Connection Server ou serveur de sécurité	4172	UDP	PCoIP (AES-128-GCM uniquement) si PCoIP Secure Gateway est utilisé.
View Connection Server	*	vCenter Server ou View Composer	80	TCP	Messages SOAP si SSL est désactivé pour l'accès à vCenter Server ou View Composer.
View Connection Server	*	vCenter Server ou View Composer	443	TCP	Messages SOAP si SSL est activé pour l'accès à vCenter Server ou View Composer.
View Connection Server	4172	View Agent 4.5 ou antérieur	50002 (peut être modifié par stratégie de groupe)	UDP	PCoIP (AES-128-GCM uniquement) si PCoIP Secure Gateway via View Connection Server est utilisé.
View Connection Server	4172	View Agent 4.6 ou supérieur	4172	UDP	PCoIP (AES-128-GCM uniquement) si PCoIP Secure Gateway via View Connection Server est utilisé.
View Connection Server	4172	View Client 4.5 ou antérieur	50002 (ne peut pas être modifié)	UDP	PCoIP (AES-128-GCM uniquement) si PCoIP Secure Gateway via View Connection Server est utilisé.
View Connection Server	4172	View Client 4.6 ou supérieur	4172	UDP	PCoIP (AES-128-GCM uniquement) si PCoIP Secure Gateway via View Connection Server est utilisé.
View Connection Server	*	View Connection Server	4100	TCP	Trafic interroutage JMS.
View Connection Server	*	machine virtuelle de	3389	TCP	Trafic Microsoft RDP vers des postes de travail View si des connexions par tunnel via View Connection Server sont utilisées.
View Connection Server	*	machine virtuelle de	4172	TCP	PCoIP (HTTPS) si PCoIP Secure Gateway via View Connection Server est utilisé.
View Connection Server	*	machine virtuelle de	9427	TCP	Redirection Wyse MMR si des connexions par tunnel via View Connection Server sont utilisées.
View Connection Server	*	machine virtuelle de	32111	TCP	Redirection USB si des connexions par tunnel via View Connection Server sont utilisées.

Tableau 12. Ports TCP et UDP utilisés par View, en excluant Local Mode (suite)

Source	Port	Cible	Port	Protocole	Description
machine virtuelle de	*	Instances de View Connection Server	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.

Pour que la fonction Local Mode s'exécute correctement, vous devez ouvrir un nombre de ports supplémentaires.

Tableau 13. Ports TCP et UDP utilisés par Local Mode

Source	Port	Cible	Port	Protocole	Description
Serveur de sécurité	*	View Transfer Server	80	TCP	Téléchargement de postes de travail View et réplication de données si des connexions par tunnel sont utilisées et si SSL est désactivé pour les opérations en mode local.
Serveur de sécurité	*	View Transfer Server	443	TCP	Téléchargement de postes de travail View et réplication de données si des connexions par tunnel sont utilisées et si SSL est activé pour les opérations en mode local.
View Client with Local Mode	*	View Transfer Server	80	TCP	Téléchargement de postes de travail View et réplication de données si des connexions directes sont utilisées à la place de connexions par tunnel et si SSL est désactivé pour les opérations en mode local.
View Client with Local Mode	*	View Transfer Server	443	TCP	Téléchargement de postes de travail View et réplication de données si des connexions directes sont utilisées à la place de connexions par tunnel et si SSL est activé pour les opérations en mode local.

Tableau 13. Ports TCP et UDP utilisés par Local Mode (suite)

Source	Port	Cible	Port	Protocole	Description
View Connection Server	*	hôte ESX	902	TCP	Utilisé lors de l'emprunt de postes de travail locaux.
View Connection Server	*	View Transfer Server	80	TCP	Téléchargement de postes de travail View et réplication de données si des connexions par tunnel via View Connection Server sont utilisées et si SSL est désactivé pour les opérations en mode local.
View Connection Server	*	View Transfer Server	443	TCP	Téléchargement de postes de travail View et réplication de données si des connexions par tunnel via View Connection Server sont utilisées et si SSL est activé pour les opérations en mode local.
View Connection Server	*	View Transfer Server	4001	TCP	Trafic JMS pour prendre en charge le mode local.
View Transfer Server	*	hôte ESX	902	TCP	Publication de packages View Composer pour le mode local.

Services sur un hôte de View Connection Server

Le fonctionnement de View Manager dépend de plusieurs services s'exécutant sur un hôte de View Connection Server. Si vous voulez ajuster le fonctionnement de ces services, il est important que vous les connaissiez.

Tableau 14. Services d'un hôte de View Connection Server

Nom du service	Type de démarrage	Description
VMware View Connection Server	Automatique	Fournit des services de Broker pour les connexions. Ce service doit être exécuté pour le fonctionnement correct de View Manager. 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 ou n'arrête pas les services VMwareVDMDS ou VMware View Script Host.
VMware View Framework Component	Manuel	Fournit des services de journalisation des événements, de sécurité et d'infrastructure COM+ pour View Manager. Ce service doit être exécuté pour le fonctionnement correct de View Manager.
VMware View Message Bus Component	Manuel	Fournit des services de messagerie entre des composants View Manager. Ce service doit être exécuté pour le fonctionnement correct de View Manager.
VMware 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 View Connection Server via PCoIP Secure Gateway.

Tableau 14. Services d'un hôte de View Connection Server (suite)

Nom du service	Type de démarrage	Description
VMware View Script Host	Automatique (si activé)	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.
VMware View Security Gateway Component	Manuel	Fournit des services de tunnel sécurisés pour View Manager. Ce service doit être exécuté pour le fonctionnement correct de View Manager.
VMware View Web Component	Manuel	Fournit des services Web pour View Manager. Ce service doit être exécuté pour le fonctionnement correct de View Manager.
VMwareVDMDS	Automatique	Fournit des services de répertoire LDAP Web pour View Manager. Ce service doit être exécuté pour le fonctionnement correct de View Manager. Ce service doit être exécuté lors des mises à niveau de VMware View pour garantir que des données existantes sont migrées correctement.

Services sur un serveur de sécurité

Le fonctionnement de View Manager dépend de plusieurs services s'exécutant sur un serveur de sécurité. Si vous voulez ajuster le fonctionnement de ces services, il est important que vous les connaissiez.

Tableau 15. Services de serveur de sécurité

Nom du service	Type de démarrage	Description
VMware View Security Server	Automatique	Fournit des services de serveur de sécurité. Ce service doit être exécuté pour le fonctionnement correct d'un serveur de sécurité. Si vous démarrez ou arrêtez ce service, il démarre ou arrête également les services Framework et Security Gateway.
VMware View Framework Component	Manuel	Fournit des services de journalisation des événements, de sécurité et d'infrastructure COM+. Ce service doit être exécuté pour le fonctionnement correct d'un serveur de sécurité.
VMware 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 un serveur de sécurité via PCoIP Secure Gateway.
VMware View Security Gateway Component	Manuel	Fournit des services de tunnel sécurisés. Ce service doit être exécuté pour le fonctionnement correct d'un serveur de sécurité.

Services sur un hôte de View Transfer Server

Les opérations de transfert pour les postes de travail locaux dépendent des services qui s'exécutent sur un hôte de View Transfer Server. Si vous voulez ajuster le fonctionnement de ces services, il est important que vous les connaissiez.

Tous les services installés avec View Transfer Server doivent être en cours d'exécution pour le fonctionnement correct des postes de travail locaux dans View Manager.

Tableau 16. Services d'un hôte de View Transfer Server

Nom du service	Type de démarrage	Description
VMware View Transfer Server	Automatique	Fournit des services qui coordonnent les services liés à View Transfer Server. Si vous démarrez ou arrêtez ce service, il démarre ou arrête également les services View Transfer Server Control Service et Framework.
VMware View Transfer Server Control Service	Manuel	Fournit des capacités de gestion pour View Transfer Server et gère la communication avec View Connection Server.
VMware View Framework Component	Manuel	Fournit des services de journalisation des événements, de sécurité et d'infrastructure COM+ pour View Manager.
Service Apache2.2	Automatique	Fournit des capacités de transfert des données pour des ordinateurs client qui exécutent des postes de travail View en mode local. Le service Apache2.2 est démarré lorsque vous ajoutez View Transfer Server à View Manager.

Index

C

comptes **8**

F

fichiers de modèle d'administration, paramètres liés à la sécurité **9**

fichiers journaux **19**

G

gestion de View Transfer Server, services sur un hôte de View Transfer Server **26**

P

paramètres de pare-feu **20**

paramètres de sécurité, générale **9**

paramètres de serveur liés à la sécurité **9**

ports TCP **20**

ports UDP **20**

présentation de sécurité **5**

R

ressources **18**

S

sécurité de View **7**

serveurs de sécurité, services **26**

service Connection Server **25**

service de serveur de sécurité **26**

service Framework Component **25, 26**

service Message Bus Component **25**

service Script Host **25**

service Security Gateway Component **25, 26**

service Transfer Server **26**

service VMwareVDMDS **25**

service Web Component **25**

services

- hôtes de serveur de sécurité **26**
- hôtes de View Connection Server **25**
- hôtes de View Transfer Server **26**

T

Transfer Server Control Service **26**

V

View Connection Server, services **25**