Utilisation de VMware View Client pour Linux

Mai 2012

View Client pour Linux

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-000780-01

vmware®

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

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

Utilisation de VMware View Client pour Linux

1

Ce guide, *Utilisation de VMware View Client pour Linux*, fournit des informations sur l'installation et l'utilisation du logiciel VMware View™ sur un système client Linux afin de se connecter à un poste de travail View dans le datacenter.

Les informations contenues dans ce document incluent les configurations système requises et des instructions pour l'installation et l'utilisation de View Client pour Linux.

Ces informations sont conçues pour les administrateurs qui doivent configurer un déploiement VMware View comportant des systèmes client Linux. Les informations sont rédigées pour des administrateurs système expérimentés qui connaissent parfaitement la technologie des machines virtuelles et les opérations de datacenter.

Remarque Ce document se rapporte à View Client pour Linux que VMware met à disposition sur Ubuntu. De plus, plusieurs partenaires de VMware offrent des périphériques de client léger pour les déploiements de VMware View. Les fonctions disponibles pour chaque périphérique de client léger, et les systèmes d'exploitation pris en charge, sont déterminés par le fournisseur, le modèle et la configuration qu'une entreprise choisit d'utiliser. Pour plus d'informations sur les fournisseurs et les modèles de périphériques de client léger, consultez le *Guide de compatibilité VMware*, disponible sur le site Web de VMware.

Installation et configuration

La configuration d'un déploiement View pour les clients Linux implique de respecter la configuration système des clients Linux, de télécharger et d'installer View Client pour Linux et de configurer les paramètres de sécurité et de performances sur les systèmes clients Linux.

- Configuration système requise pour les clients Linux page 6

  Vous pouvez installer View Client pour Linux sur des ordinateurs de bureau qui utilisent le système d'exploitation Ubuntu Linux 10.04 ou 10.10.

- Systèmes d'exploitation de poste de travail View pris en charge page 7

  Les administrateurs créent des machines virtuelles avec un système d'exploitation client et installent View Agent sur le système d'exploitation client. Les utilisateurs finaux peuvent ouvrir une session sur ces machines virtuelles à partir d'un périphérique client.

- Préparation du Serveur de connexion View pour View Client page 7

  Les administrateurs doivent effectuer des tâches spécifiques pour permettre aux utilisateurs finaux de se connecter à des postes de travail View.

- Installer View Client pour Linux page 8

  Les utilisateurs finaux ouvrent View Client pour se connecter à des postes de travail virtuels depuis une machine physique. View Client pour Linux s'exécute sur des systèmes Ubuntu 10.04 ou 10.10. Vous l'installez à l'aide de Synaptic Package Manager.

- Configuration de la vérification des certificats pour les utilisateurs finaux page 9

  Les administrateurs peuvent configurer le mode de vérification des certificats afin que, par exemple, une vérification complète soit toujours effectuée.

- Activation du mode FIPS sur le client page 9

  Vous pouvez définir une propriété de configuration pour que le client utilise uniquement des algorithmes et des protocoles cryptographiques approuvés par FIPS (Federal Information Processing Standard) 140-2 pour établir une connexion PCoIP distante.

- Configuration du cache d'images client PCoIP page 10

  Le cache d'images client PCoIP stocke le contenu des images sur le client pour éviter la retransmission. Cette fonction est activée par défaut pour réduire l'utilisation de la bande passante.

Configuration système requise pour les clients Linux

Vous pouvez installer View Client pour Linux sur des ordinateurs de bureau qui utilisent le système d'exploitation Ubuntu Linux 10.04 ou 10.10.

L'ordinateur de bureau ou portable Linux sur lequel vous installez View Client, et les périphériques qu'il utilise, doit se conformer à une certaine configuration système.

Modèle	Poste de travail ou ordinateur de bureau avec Intel
Mémoire	Au moins 2 Go de RAM
Systèmes d'exploitation	Ubuntu Linux 10.04 ou 10.10 32 bits
Serveur de connexion View, serveur de sécurité et View Agent	4.6.1 ou version supérieure Si les systèmes clients se connectent en dehors du pare-feu d'entreprise, VMware recommande d'utiliser un serveur de sécurité. Avec un serveur de sécurité, les systèmes client ne requièrent pas de connexion VPN.

Protocole d'affichage pour VMware View	PCoIP ou RDP

Exigences matérielles pour PCoIP	■ Un processeur x86 avec extensions SSE2, avec une vitesse de processeur d'au moins 800 MHz.
	■ RAM disponible supérieure à la configuration requise pour prendre en charge plusieurs configurations d'écran. Utilisez la formule suivante comme indicateur général :
	`20 Mo + (24 * (nb d'écrans) * (largeur d'écran) * (hauteur d'écran))`
	Comme indicateur rapide, vous pouvez utiliser les calculs suivants :
	`1 écran : 1600 x 1200 : 64 Mo`
	`2 écrans : 1600 x 1200 : 128 Mo`
	`3 écrans : 1600 x 1200 : 256 Mo`

Exigences matérielles pour RDP	■ Un processeur x86 avec extensions SSE2, avec une vitesse de processeur d'au moins 800 MHz. ■ RAM de 128 Mo.

Systèmes d'exploitation de poste de travail View pris en charge

Les administrateurs créent des machines virtuelles avec un système d'exploitation client et installent View Agent sur le système d'exploitation client. Les utilisateurs finaux peuvent ouvrir une session sur ces machines virtuelles à partir d'un périphérique client.

Pour voir une liste des systèmes d'exploitation client pris en charge, reportez-vous à la rubrique « Systèmes d'exploitation pris en charge pour View Agent » dans la documentation d'installation de VMware View 4.6.x ou 5.x.

Préparation du Serveur de connexion View pour View Client

Les administrateurs doivent effectuer des tâches spécifiques pour permettre aux utilisateurs finaux de se connecter à des postes de travail View.

Pour que les utilisateurs finaux puissent se connecter à Serveur de connexion View ou à un serveur de sécurité et accéder à un poste de travail View, vous devez configurer certains paramètres de pool et des paramètres de sécurité :

- Si vous utilisez un serveur de sécurité, comme le recommande VMware, vérifiez que vous utilisez le Serveur de connexion View 4.6.1 et le serveur de sécurité View 4.6.1 ou une version supérieure. Consultez la documentation *Installation de VMware View* pour View 4.6 ou ultérieur.
- Si vous prévoyez d'utiliser une connexion sécurisée pour des périphériques client et si la connexion sécurisée est configurée avec un nom d'hôte DNS pour le Serveur de connexion View ou un serveur de sécurité, vérifiez que le périphérique client peut résoudre ce nom DNS.

  Pour activer ou désactiver le tunnel sécurisé, dans View Administrator, allez à la boîte de dialogue Modifier les paramètres du Serveur de connexion View et cochez la case **[Utiliser une connexion tunnel sécurisée vers le poste de travail]** .
- Vérifiez qu'un pool de postes de travail virtuels a été créé et que le compte d'utilisateur que vous prévoyez d'utiliser est autorisé à accéder à ce poste de travail View. Consultez les rubriques sur la création de pools de postes de travail dans la documentation *Administration de VMware View*.

- Pour pouvoir utiliser l'authentification à 2 facteurs, telle que l'authentification RSA SecurID ou RADIUS, avec View Client, vous devez activer cette fonction sur le Serveur de connexion View. L'authentification RADIUS est disponible avec View 5.1 et les versions supérieures et le Serveur de connexion View. Pour plus d'informations, consultez les rubriques relatives à l'authentification à 2 facteurs dans la documentation *Administration de VMware View*.

Installer View Client pour Linux

Les utilisateurs finaux ouvrent View Client pour se connecter à des postes de travail virtuels depuis une machine physique. View Client pour Linux s'exécute sur des systèmes Ubuntu 10.04 ou 10.10. Vous l'installez à l'aide de Synaptic Package Manager.

Prérequis

- Vérifiez que le système client utilise un système d'exploitation pris en charge. Reportez-vous à la section « Configuration système requise pour les clients Linux », page 6.
- Vérifiez que vous pouvez ouvrir une session en tant qu'administrateur sur le système client.
- Si vous prévoyez d'utiliser le protocole d'affichage RDP pour vous connecter à un poste de travail View, vérifiez que le client RDP approprié est installé. Reportez-vous à la section « Configuration système requise pour les clients Linux », page 6.

Procédure

1 Sur votre ordinateur portable ou de bureau Linux, activez Canonical Partners.

   a Dans la barre de menus Ubuntu, sélectionnez **[System (Système)] > [Administration] > [Update Manager (Gestionnaire de mises à jour)]** .

   b Cliquez sur le bouton **[Settings (Paramètres)]** et fournissez le mot de passe pour réaliser des tâches administratives.

   c Dans la boîte de dialogue Software Sources (Sources logicielles), cliquez sur l'onglet **[Other Software (Autres logiciels)]** et cochez la case **[Canonical Partners (Partenaires Canonical)]** pour sélectionner l'archive des logiciels que Canonical fournit à ses partenaires.

   d Cliquez sur **[Close (Fermer)]** et suivez les instructions pour mettre à jour la liste de packages.

2 Dans la barre de menus Ubuntu, sélectionnez **[System (Système)] > [Administration] > [Synaptic Package Manager]** .

3 Cliquez sur **[Search (Rechercher)]** et recherchez **`vmware`**.

4 Dans la liste de packages trouvés, cochez la case à côté de **[vmware-view-client]** et sélectionnez **[Mark for Installation (Marquer pour l'installation)]** .

   Ne cochez pas la case pour le client ouvert.

5 Cliquez sur **[Apply (Appliquer)]** dans la barre d'outils.

   VMware View Client pour Linux est installé.

6 Pour savoir si l'installation est réussie, vérifiez que l'icône de l'application **[VMware View]** apparaît dans le menu **[Applications] > [Internet]** .

Suivant

Démarrez View Client et vérifiez que vous pouvez ouvrir une session sur le bon poste de travail virtuel. Reportez-vous à la section « Première connexion à un poste de travail View », page 11.

Configuration de la vérification des certificats pour les utilisateurs finaux

Les administrateurs peuvent configurer le mode de vérification des certificats afin que, par exemple, une vérification complète soit toujours effectuée.

La vérification des certificats se produit pour les connexions SSL entre Serveur de connexion View et View Client. Les administrateurs peuvent configurer le mode de vérification pour utiliser l'une des stratégies suivantes :

- Les utilisateurs finaux sont autorisés à choisir le mode de vérification. Le reste de cette liste décrit les trois modes de vérification.
- (Pas de vérification) Aucune vérification de certificat n'est effectuée.
- (Avertir) Les utilisateurs sont avertis si un certificat auto-signé est présenté par le serveur. Les utilisateurs peuvent choisir d'autoriser ou pas ce type de connexion.
- (Sécurité complète) Une vérification complète est effectuée et les connexions qui ne passent pas de vérification complète sont rejetées.

Pour plus d'informations sur les types de vérifications effectuées, reportez-vous à la section « Modes de vérification des certificats pour View Client », page 13.

Utilisez la propriété `view.sslVerificationMode` pour définir le mode de vérification par défaut :

- **`1`** implémente `Vérification complète`.
- **`2`** implémente `Avertir si la connexion peut être non sécurisée`.
- **`3`** implémente `Aucune vérification effectuée`.

Pour configurer le mode afin que les utilisateurs finaux ne puissent pas modifier le mode, définissez la propriété `view.allowSslVerificationMode` sur **`"False"`** dans le fichier `/etc/vmware/view-mandatory-config` sur le système client. Reportez-vous à la section « Paramètres d'utilisation et de configuration des commandes de View Client », page 19.

Activation du mode FIPS sur le client

Vous pouvez définir une propriété de configuration pour que le client utilise uniquement des algorithmes et des protocoles cryptographiques approuvés par FIPS (Federal Information Processing Standard) 140-2 pour établir une connexion PCoIP distante.

Ce paramètre s'applique à la fois au serveur et au client. Vous pouvez configurer un ou les deux points de terminaison pour qu'ils fonctionnent en mode FIPS. La configuration d'un seul point de terminaison pour qu'il fonctionne en mode FIPS limite les algorithmes de cryptage disponibles pour la négociation de session.

IMPORTANT Si vous activez le mode FIPS sur un point de terminaison et que l'autre point de terminaison ne prenne pas en charge les algorithmes cryptographiques approuvés par FIPS 140-2, la connexion échoue.

Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, le mode FIPS n'est pas utilisé.

Définition de la propriété de configuration

Pour activer ou désactiver le mode FIPS, vous pouvez définir la propriété `pcoip.enable_fips_mode`. Affectez la valeur **`1`** à la propriété pour activer le mode FIPS, ou la valeur **`0`** pour le désactiver. Par exemple, le paramètre suivant active le mode FIPS :

```
pcoip.enable_fips_mode = 1
```

Insérez un espace avant et après le signe égal (=).

Vous pouvez définir cette propriété dans n'importe quels fichiers d'un groupe de fichiers. Lorsque View Client démarre, le paramètre est traité dans divers emplacements dans l'ordre suivant :

1 `/etc/teradici/pcoip_admin_defaults.conf`

2 `~/.pcoip.rc`

3 `/etc/teradici/pcoip_admin.conf`

Si un paramètre est défini dans plusieurs emplacements, la valeur utilisée est la valeur du dernier fichier lu.

Configuration du cache d'images client PCoIP

Le cache d'images client PCoIP stocke le contenu des images sur le client pour éviter la retransmission. Cette fonction est activée par défaut pour réduire l'utilisation de la bande passante.

IMPORTANT Cette fonction est disponible uniquement lorsque la version de View Agent et celle du Serveur de connexion View correspondent à la version View 5.0 ou une version supérieure.

Le cache d'images PCoIP capture la redondance spatiale et temporaire. Par exemple, lorsque vous faites défiler un document PDF, le nouveau contenu apparaît depuis le bas de la fenêtre et le contenu le plus ancien disparaît du haut de la fenêtre. L'autre contenu reste constant et remonte. Le cache d'images PCoIP peut détecter cette redondance spatiale et temporaire.

Comme pendant le défilement, les informations d'écran envoyées au périphérique client sont constituées principalement d'une séquence d'index de cache, utilisation du cache d'images permet d'économiser un quantité significative de bande passante. Ce défilement efficace offre des avantages dans un réseau LAN et dans un réseau WAN.

- Dans un réseau LAN, où la bande passante est relativement illimitée, le cache d'image client permet d'économiser une quantité significative de bande passante.
- Dans un réseau WAN, pour rester dans les limites de bande passante disponible, le défilement est généralement dégradé si la mise en cache client n'est pas utilisée. Dans ce cas, la mise en cache client peut économiser la bande passante et permettre de faire défiler les données d'une manière fluide et avec grande réactivité.

Cette fonction est activée par défaut pour permettre au client de stocker des parties de l'écran déjà envoyées. La taille du cache est de 250 Mo par défaut. Vous pouvez définir une taille de cache client comprise entre 50 Mo et 300 Mo. Une grande taille de cache réduit l'utilisation de la bande passante, mais nécessite plus de mémoire sur le client. Une petite taille de cache augmente l'utilisation de la bande passante. Par exemple, un client léger avec peu de mémoire nécessite un cache de petite taille.

Définition de la propriété de configuration

Pour définir la taille du cache, vous pouvez spécifier la propriété `pcoip.image_cache_size_mb`. Par exemple, le paramètre suivant définit une taille de cache de 50 Mo :

```
pcoip.image_cache_size_mb = 50
```

Insérez un espace avant et après le signe égal (=). Si vous définissez une valeur inférieure à 50, la valeur est remplacée par 50. Si vous définissez une valeur supérieure à 300, la valeur est remplacée par 300.

Vous pouvez définir cette propriété dans n'importe quels fichiers d'un groupe de fichiers. Lorsque View Client démarre, le paramètre est traité dans divers emplacements dans l'ordre suivant :

1 `/etc/teradici/pcoip_admin_defaults.conf`

2 `~/.pcoip.rc`

3 `/etc/teradici/pcoip_admin.conf`

Si un paramètre est défini dans plusieurs emplacements, la valeur utilisée est la valeur du dernier fichier lu.

Remarque Vous pouvez définir la propriété suivante pour afficher une indication graphique du fonctionnement du cache d'image :

```
pcoip.show_image_cache_hits = 1
```

Avec cette configuration, pour chaque mosaïque (32 x 32 pixels) dans une image provenant du cache d'images, un rectangle apparaît autour de la mosaïque.

Gestion des connexions de serveur et des postes de travail

Utilisez View Client pour vous connecter à View Connection Server ou à un serveur de sécurité et pour ouvrir ou fermer une session sur un poste de travail View. À des fins de dépannage, vous pouvez également réinitialiser un poste de travail View qui vous est affecté et restaurer un poste de travail que vous avez emprunté.

En fonction de la façon dont l'administrateur configure des règles pour les postes de travail View, les utilisateurs finaux peuvent être capables d'exécuter plusieurs opérations sur leurs postes de travail.

- Première connexion à un poste de travail View page 11

  Avant de laisser vos utilisateurs finaux accéder à leurs postes de travail virtuels, vérifiez que vous pouvez ouvrir une session sur un poste de travail virtuel depuis le système client.

- Modes de vérification des certificats pour View Client page 13

  Les administrateurs, et parfois les utilisateurs finaux, peuvent configurer le rejet des connexions client si une ou plusieurs vérifications de certificats de serveur échouent.

- Basculer entre postes de travail page 14

  Si vous êtes connecté à un poste de travail, vous pouvez basculer vers un autre poste de travail.

- Fermer une session ou se déconnecter d'un poste de travail page 14

  Si vous vous déconnectez d'un poste de travail View sans fermer votre session, des applications restent ouvertes.

- Restaurer un poste de travail page 15

  La restauration ignore les modifications réalisées sur un poste de travail virtuel que vous avez emprunté pour l'utiliser en mode local sur un PC ou un ordinateur portable Windows.

Première connexion à un poste de travail View

Avant de laisser vos utilisateurs finaux accéder à leurs postes de travail virtuels, vérifiez que vous pouvez ouvrir une session sur un poste de travail virtuel depuis le système client.

Prérequis

- Les informations d'identification dont vous avez besoin pour ouvrir une session, telles que le nom d'utilisateur et le mot de passe Active Directory, le nom d'utilisateur et le code secret RSA SecurID ou le nom d'utilisateur et le code secret pour l'authentification RADIUS.
- Obtenez le nom de domaine pour ouvrir une session.
- Effectuez les tâches administratives décrites dans la section « Préparation du Serveur de connexion View pour View Client », page 7.
- Si vous vous trouvez à l'extérieur du réseau d'entreprise et si vous n'utilisez pas de serveur de sécurité pour accéder au poste de travail virtuel, vérifiez que votre périphérique client est configuré pour utiliser une connexion VPN et activez cette connexion.

  Important VMware vous recommande d'utiliser un serveur de sécurité plutôt qu'un VPN.

- Vérifiez que vous possédez le nom de domaine complet (FQDN) du serveur qui fournit l'accès au poste de travail virtuel. Vous avez également besoin du numéro de port si le port n'est pas 443.
- Si vous prévoyez d'utiliser le protocole d'affichage RDP pour vous connecter à un poste de travail View, vérifiez que le paramètre de stratégie de groupe AllowDirectRDP de View Agent est activé.
- Si votre administrateur l'a autorisé, vous pouvez configurer le mode de vérification des certificats pour le certificat SSL que le serveur View server présente. Reportez-vous à la section « Modes de vérification des certificats pour View Client », page 13.

Procédure

1 Ouvrez une fenêtre de terminal et entrez **`vmware-view`** ou sélectionnez **[Applications] > [Internet] > [VMware View Client]** dans la barre de menus Ubuntu.

2 Entrez le nom de serveur et un numéro de port si nécessaire, puis cliquez sur **[Continuer]** .

Voici un exemple d'utilisation d'un port non défini comme port par défaut : **`view.company.com:1443`**.

3 Si un message demande les informations d'identification RSA SecurID ou les informations d'identification pour l'authentification RADIUS, entrez le nom d'utilisateur et le code secret et cliquez sur **[Continuer]** .

4 Entrez vos nom d'utilisateur et mot de passe, sélectionnez un domaine et cliquez sur **[OK]** .

Vous pouvez voir un message que vous devez confirmer avant que la boîte de dialogue de connexion apparaisse.

5 Si l'indicateur de sécurité de poste de travail devient rouge et qu'un message d'avertissement apparaît, répondez à l'invite.

Généralement, cet avertissement indique que le Serveur de connexion View n'a pas envoyé d'empreinte numérique de certificat au client. L'empreinte numérique est un hachage de la clé publique du certificat et elle est utilisée comme abréviation de la clé publique. Le Serveur de connexion View 4.6.1, 5.0.1 et les versions supérieures envoient des informations d'empreinte numérique, contrairement aux versions antérieures.

6 (Facultatif) Sélectionnez le protocole d'affichage et la taille de fenêtre à utiliser.

Option	Description
Protocole d'affichage	L'option par défaut est **[PCoIP]** . Pour utiliser plutôt Microsoft RDP, cliquez sur **[PCoIP]** sous le nom de poste de travail à définir et sélectionnez **[Microsoft RDP]** .
Taille de fenêtre	L'option par défaut est **[Tous les moniteurs]** . Pour choisir une autre taille de fenêtre, cliquez sur l'une des autres options sous le nom de poste de travail, telle que **[Grand écran]** ou **[Personnaliser la taille]** .

7 Double-cliquez sur un raccourci de poste de travail View pour vous connecter.

Une fois la connexion établie, la fenêtre client s'affiche. Si View Client ne peut pas se connecter au poste de travail, effectuez les tâches suivantes :

- Déterminez si le Serveur de connexion View est configuré pour ne pas utiliser SSL. View Client requiert des connexions SSL. Vérifiez si le paramètre général dans View Administrator de la case **[Use SSL for client connections (Utiliser SSL pour les connexions client)]** est désélectionné. Dans ce cas, vous devez cocher la case pour utiliser SSL ou configurer l'environnement pour que les clients puissent se connecter à un équilibreur de charge dont la fonction HTTPS est activée ou un autre périphérique intermédiaire configuré pour établir une connexion HTTP au Serveur de connexion View.
- Vérifiez que le certificat de sécurité du Serveur de connexion View fonctionne correctement. Si ce n'est pas le cas, dans View Administrator, vous pouvez également voir que View Agent sur des postes de travail n'est pas accessible.

- Vérifiez que les balises définies sur l'instance du Serveur de connexion View autorisent les connexions depuis cet utilisateur. Consultez le document *Administration de VMware View*.
- Vérifiez que l'utilisateur est autorisé à accéder à ce poste de travail. Consultez le document *Administration de VMware View*.
- Si vous utilisez le protocole d'affichage RDP pour vous connecter à un poste de travail View, vérifiez que l'ordinateur client autorise les connexions vers des postes de travail distants.

Modes de vérification des certificats pour View Client

Les administrateurs, et parfois les utilisateurs finaux, peuvent configurer le rejet des connexions client si une ou plusieurs vérifications de certificats de serveur échouent.

La vérification des certificats se produit pour les connexions SSL entre le Serveur de connexion View et View Client. La vérification de certificat inclut les vérifications suivantes :

- Le certificat a-t-il un autre but que de vérifier l'identité de l'expéditeur et de chiffrer les communications du serveur ? Autrement dit, s'agit-il du bon type de certificat ?
- Le certificat a-t-il expiré, ou est-il valide uniquement dans le futur ? Autrement dit, le certificat est-il valide en fonction de l'horloge de l'ordinateur ?
- Le nom commun sur le certificat correspond-il au nom d'hôte du serveur qui l'envoie ? Une incompatibilité peut se produire si un équilibreur de charge redirige View Client vers un serveur avec un certificat qui ne correspond pas au nom d'hôte entré dans View Client. Une incompatibilité peut également se produire si vous entrez une adresse IP plutôt qu'un nom d'hôte dans le client.
- Le certificat est-il signé par une autorité de certification inconnue ou non approuvée ? Les certificats auto-signés sont un type d'autorité de certification non approuvée.

  Pour que cette vérification aboutisse, la chaîne d'approbation du certificat doit être associée à une racine dans le magasin de certificats local du périphérique.

Remarque Pour plus d'informations sur la distribution d'un certificat racine auto-signé que les utilisateurs peuvent installer sur leurs systèmes client Linux, consultez la documentation Ubuntu.

View Client utilise les certificats de format PEM stockés dans le répertoire `/etc/ssl/certs` sur le système client. Pour plus d'informations sur l'importation d'un certificat racine stocké à cet emplacement, consultez la procédure appelée « Importing a Certificate into the System-Wide Certificate Authority Database » (Importation d'un certificat dans la base de données de l'autorité de certification à l'échelle du système) dans le document à l'adresse https://help.ubuntu.com/community/OpenSSL.

Outre la présentation d'un certificat de serveur, le Serveur de connexion View 4.6.1, 5.0.1 et les versions supérieures envoient une empreinte numérique de certificat à View Client. L'empreinte numérique est un hachage de la clé publique du certificat et elle est utilisée comme abréviation de la clé publique. Si le View server n'envoie pas d'empreinte numérique, un avertissement s'affiche pour indiquer que la connexion n'est pas autorisée.

Si votre administrateur l'a autorisé, vous pouvez définir le mode de vérification des certificats. Sélectionnez **[Fichier] > [Préférences]** dans la barre de menus de VMware View Client ou du poste de travail View. Vous avez trois possibilités :

- **[Ne jamais se connecter à des serveurs non autorisés]** . Si l'une des vérifications de certificat échoue, le client ne peut pas se connecter au serveur. Un message d'erreur répertorie les vérifications qui ont échoué.
- **[Signaler avant de se connecter à des serveurs non autorisés]** . Si une vérification de certificat échoue car le serveur utilise un certificat auto-signé, vous pouvez cliquer sur **[Continuer]** pour ignorer l'avertissement. Pour les certificats auto-signés, le nom de certificat ne doit pas être concordant au nom du serveur de connexion que vous avez saisi dans View Client.

- **[Ne pas vérifier les certificats d'identité des serveurs]** . Ce paramètre signifie que View n'effectue aucune vérification de certificat.

Basculer entre postes de travail

Si vous êtes connecté à un poste de travail, vous pouvez basculer vers un autre poste de travail.

Procédure

- Sélectionnez un poste de travail View à partir du même serveur ou d'un serveur différent.

Option	Action
Choisir un poste de travail View différent sur le même serveur	Sélectionnez **[Poste de travail]** > **[Déconnecter]** dans la barre de menus.
Choisir un poste de travail View sur un serveur différent	Sélectionnez **[Fichier]** > **[Choisir un autre serveur]** dans la barre de menus.

Fermer une session ou se déconnecter d'un poste de travail

Si vous vous déconnectez d'un poste de travail View sans fermer votre session, des applications restent ouvertes.

Si vous n'êtes pas connecté à un poste de travail View, vous pouvez fermer votre session sans vous connecter avant. Utiliser cette fonction a le même résultat que d'envoyer Ctrl+Alt+Suppr au poste de travail et de cliquer sur **[Fermer la session]** .

REMARQUE La combinaison de touches Windows Ctrl+Alt+Suppr n'est pas prise en charge sur les postes de travail View. Pour utiliser une action équivalente à la combinaison Ctrl+Alt+Suppr, sélectionnez **[Poste de travail]** > **[Envoyer Ctrl+Alt+Suppr]** dans la barre de menus.

Vous pouvez également appuyer sur Ctrl+Alt+Inser.

Procédure

- Déconnectez-vous sans fermer de session.

Option	Action
Quitter aussi View Client	Cliquez sur le bouton **[Fermer]** dans le coin de la fenêtre ou sélectionnez **[Fichier]** > **[Quitter]** dans la barre de menus.
Choisir un poste de travail View différent sur le même serveur	Sélectionnez **[Poste de travail]** > **[Déconnecter]** dans la barre de menus.
Choisir un poste de travail View sur un serveur différent	Sélectionnez **[Fichier]** > **[Choisir un autre serveur]** dans la barre de menus.

REMARQUE Votre administrateur View peut configurer votre poste de travail pour que la session soit fermée automatiquement lors de la déconnexion. Dans ce cas, tous les programmes ouverts sur votre poste de travail sont arrêtés.

- Fermez une session et déconnectez-vous.

Option	Action
À partir de l'OS du poste de travail	Utilisez le menu **[Démarrer]** de Windows pour fermer la session.
À partir de la barre de menus	Sélectionnez **[Poste de travail]** > **[Se déconnecter et fermer la session]** . Si vous utilisez cette procédure, les fichiers ouverts sur le poste de travail View seront fermés sans être enregistrés.

- Fermez une session lorsque vous n'êtes pas connecté à un poste de travail View.

  a Dans l'écran d'accueil avec les raccourcis de poste de travail, sélectionnez le poste de travail et **[Poste de travail] > [Fermer la session]** dans la barre de menus.

  b Si vous y êtes invité, entrez des informations d'identification pour accéder au poste de travail View.

  Si vous utilisez cette procédure, les fichiers ouverts sur le poste de travail View seront fermés sans être enregistrés.

Restaurer un poste de travail

La restauration ignore les modifications réalisées sur un poste de travail virtuel que vous avez emprunté pour l'utiliser en mode local sur un PC ou un ordinateur portable Windows.

Vous pouvez restaurer un poste de travail View uniquement si votre administrateur View a activé cette fonction et uniquement si vous avez emprunté le poste de travail.

AVERTISSEMENT Si des modifications ont été faites sur le poste de travail en mode local et que ces modifications n'ont pas été répliquées sur le serveur View avant la restauration, les modifications sont perdues.

Prérequis

- Les informations d'identification dont vous avez besoin pour ouvrir une session, telles que le nom d'utilisateur et le mot de passe Active Directory, le nom d'utilisateur et le code secret RSA SecurID ou le nom d'utilisateur et le code secret pour l'authentification RADIUS.
- Sauvegardez le poste de travail sur le serveur pour conserver des données ou des fichiers.

  Vous pouvez utiliser View Administrator pour répliquer des données sur le serveur ou, si la règle est définie pour l'autoriser, vous pouvez utiliser View Client with Local Mode sur le client Windows sur lequel le poste de travail est actuellement emprunté.

Procédure

1 Si l'écran d'accueil de View Client affiche l'invite de **[Serveur de connexion View]** , entrez le nom de serveur et cliquez sur **[Continuer]** .

  a Si un message demande les informations d'identification RSA SecurID ou les informations d'identification pour l'authentification RADIUS, entrez le nom d'utilisateur et le code secret et cliquez sur **[Continuer]** .

  b Saisissez votre nom d'utilisateur et votre mot de passe dans la boîte de dialogue de connexion.

2 Sur l'écran d'accueil de View Client qui affiche des raccourcis de poste de travail View, sélectionnez le poste de travail et choisissez **[Poste de travail > Restaurer le poste de travail]** dans la barre de menus.

Une fois le poste de travail View restauré, vous pouvez ouvrir une session dessus depuis le client Linux.

Utilisation d'un poste de travail Microsoft Windows sur un système Linux

View Client pour Linux prend en charge certaines fonctions incluses dans View Client pour Windows.

Matrice de prise en charge des fonctions

View Client pour Linux prend en charge un sous-ensemble des fonctions disponibles sur les autres clients, tels que View Client pour les postes de travail et les ordinateurs portables Windows.

Tableau 1-1. Fonctions prises en charge sur des postes de travail Windows pour les clients Linux

Fonction	Poste de travail View Windows 7	Poste de travail View Windows Vista	Poste de travail View Windows XP
RSA SecurID ou RADIUS	X	X	X
Authentification unique	X	X	X
Protocole d'affichage RDP	X	X	X
Protocole d'affichage PCoIP	X	X	X
Accès USB			
Wyse MMR			
Impression virtuelle			
Impression basée sur l'emplacement	X	X	X
Cartes à puce			
Plusieurs écrans	X	X	X
Mode local			

Pour des descriptions de ces fonctions et leurs limites, consultez le document *Planification de l'architecture de View*.

Remarque Cette matrice de prise en charge des fonctions s'applique à View Client pour Linux que VMware met à disposition sur Ubuntu. De plus, plusieurs partenaires de VMware offrent des périphériques de client léger pour les déploiements de VMware View. Les fonctions disponibles pour chaque périphérique de client léger sont déterminées par le fournisseur, le modèle et la configuration qu'une entreprise choisit d'utiliser. Pour plus d'informations sur les fournisseurs et les modèles de périphériques de client léger, consultez le *Guide de compatibilité VMware*, disponible sur le site Web de VMware.

Internationalisation

L'interface utilisateur et la documentation de View Client sont disponibles en anglais, japonais, français, allemand, chinois simplifié et coréen.

Si vous utilisez un système client Ubuntu 10.4 Linux et voulez afficher l'interface utilisateur View Client dans une autre langue que l'anglais, vous devez définir le système client pour utiliser un paramètre régional qui utilise le codage UTF-8.

Claviers et moniteurs

Vous pouvez utiliser plusieurs moniteurs et tous les types de claviers avec un poste de travail View. Certains paramètres permettent d'optimiser l'expérience utilisateur.

Meilleures pratiques d'utilisation de plusieurs moniteurs

Suivez les recommandations ci-dessous pour utiliser efficacement plusieurs moniteurs avec un poste de travail View :

- Avec PCoIP, vous pouvez utiliser jusqu'à quatre moniteurs si vous disposez d'une mémoire RAM vidéo suffisante.

  Pour pouvoir utiliser plus de deux moniteurs afin d'afficher le poste de travail View sur un système client Ubuntu, vous devez définir le paramètre `kernel.xhmmax` correctement. Utilisez la formule suivante :

  max horizontal resolution X *max vertical resolution* X *max number of monitors* X 4

  Par exemple, si vous affectez manuellement au paramètre `kernel.shmmax` la valeur 65536000, vous pouvez utiliser quatre moniteurs avec la résolution d'écran 2 560 x 1 600.

- Avec RDP, l'écran ne peut être affiché qu'en mode d'étirement. Pour utiliser ce mode afin d'étirer l'écran sur plusieurs moniteurs, les moniteurs doivent avoir la même hauteur.

Résolution d'écran

Suivez les instructions ci-dessous pour définir les résolutions d'écran :

- Si vous ouvrez un poste de travail View sur un moniteur secondaire et changez la résolution d'écran sur le moniteur, le poste de travail View utilise le moniteur principal.
- Avec PCoIP, si vous disposez de plusieurs moniteurs, vous pouvez régler la résolution de chaque moniteur séparément avec la résolution maximale 2 560 x 1 600 pour chaque écran.
- Avec RDP, si vous disposez de plusieurs moniteurs, vous ne pouvez pas régler la résolution de chaque moniteur séparément et l'affichage est étiré sur les moniteurs s'ils ont tous la même hauteur.

Limitations de clavier

En règle générale, les claviers fonctionnent aussi bien avec un poste de travail View qu'avec un ordinateur physique. Vous trouverez ci-dessous la liste des limitations auxquelles vous pouvez être confronté en fonction des types des périphériques et des logiciels sur le système client :

- Certaines touches multimédia sur un clavier multimédia peuvent ne pas fonctionner. Par exemple, la touche Musique et Poste de travail peuvent ne pas fonctionner.
- Si vous vous connectez à un poste de travail utilisant RDP, utilisez le gestionnaire de fenêtres Fluxbox et avez activé un écran de veille sur le poste de travail View, le clavier peut ne pas fonctionner après une période d'inactivité.

  Quel que soit le gestionnaire de fenêtres que vous utilisez, VMware recommande de désactiver l'écran de veille sur un poste de travail View et de ne pas définir de miniteur de mise en veille.

Copier et coller du texte

Vous pouvez copier et coller du texte entre votre système client et un poste de travail View distant. Si votre administrateur active la fonction, vous pouvez également copier et coller du texte entre un poste de travail View et votre système client ou entre deux postes de travail View. Certaines restrictions s'appliquent.

Si vous utilisez le protocole d'affichage PCoIP et un poste de travail View avec View 5.x ou ultérieur, votre administrateur View peut définir cette fonction pour que les opérations de copier-coller soient autorisées uniquement depuis votre système client sur un poste de travail View, ou uniquement depuis un poste de travail View vers votre système client, ou les deux, ou aucun.

Les administrateurs configurent le copier-coller à l'aide d'objets de stratégie de groupe (GPO) qui appartiennent à View Agent dans des postes de travail View. Pour plus d'informations, consultez la rubrique sur les variables de la session générale PCoIP de View dans le document *Administration de VMware View*, dans le chapitre sur la configuration des stratégies.

Vous pouvez copier du texte brut ou mis en forme entre View Client et un poste de travail View, ou l'inverse, mais le texte collé est du text brut.

Vous ne pouvez pas copier et coller des graphiques. Vous ne pouvez pas non plus copier et coller des fichiers entre un poste de travail View et le système de fichiers sur votre ordinateur client.

Dépannage de View Client

Vous pouvez résoudre la plupart des problèmes de View Client en réinitialisant le poste de travail ou en réinstallant VMware View Client.

Réinitialiser un poste de travail

La réinitialisation arrête et redémarre le poste de travail. Les données non enregistrées sont perdues.

Vous devrez peut-être réinitialiser un poste de travail si le système d'exploitation du poste de travail cesse de répondre.

La réinitialisation d'un poste de travail View a la même finalité que d'appuyer sur le bouton Réinitialiser d'un ordinateur physique pour le forcer à redémarrer. Les fichiers ouverts sur le poste de travail View seront fermés sans être enregistrés.

Vous pouvez réinitialiser le poste de travail uniquement si votre administrateur View a activé cette fonction.

Procédure

- Utilisez la commande **[Réinitialiser le poste de travail]** .

Option	Action
À partir de l'OS du poste de travail	Sélectionnez **[Poste de travail]** > **[Réinitialiser le poste de travail]** dans la barre de menus.
À partir de l'écran d'accueil avec des raccourcis de poste de travail	Sélectionnez le poste de travail et choisissez **[Poste de travail]** > **[Réinitialiser le poste de travail]** dans la barre de menus.

Le système d'exploitation dans le poste de travail View est redémarré. View Client se déconnecte du poste de travail.

Suivant

Attendez que le système démarre avant d'essayer de vous connecter au poste de travail View.

Désinstallation de View Client

Vous pouvez parfois résoudre des problèmes avec View Client en désinstallant et en réinstallant l'application VMware View Client.

Vous désinstallez View Client avec la méthode que vous utilisez habituellement pour désinstaller d'autres applications.

Par exemple, sélectionnez **[Applications] > [Logithèque Ubuntu]** , puis dans la section **[Logiciel installé]** , sélectionnez **[vmware-view-client]** et cliquez sur **[Supprimer]** .

Une fois la désinstallation terminée, vous pouvez réinstaller l'application.

Reportez-vous à la section « Installer View Client pour Linux », page 8.

Paramètres d'utilisation et de configuration des commandes de View Client

Vous pouvez configurer View Client à l'aide d'options de ligne de commande ou de propriétés équivalentes dans un fichier de configuration.

Vous pouvez utiliser l'interface de ligne de commande `vmware-view` ou des propriétés définies dans des fichiers de configuration pour définir les valeurs par défaut que vos utilisateurs voient dans View Client ou pour empêcher certaines boîtes de dialogue de demander des informations aux utilisateurs. Vous pouvez également spécifier des paramètres que vous ne voulez pas que les utilisateurs modifient.

Ordre de traitement des paramètres de configuration

Lorsque View Client démarre, des paramètres de configuration sont traités depuis plusieurs emplacements dans l'ordre suivant :

1 `/etc/vmware/view-default-config`

2 `~/.vmware/view-preferences`

3 Arguments de ligne de commande

4 `/etc/vmware/view-mandatory-config`

Si un paramètre est défini dans plusieurs emplacements, la valeur utilisée est la valeur du dernier fichier ou de la dernière option de ligne de commande lu(e). Par exemple, pour spécifier des paramètres qui remplacent les préférences des utilisateurs, définissez des propriétés dans le fichier `/etc/vmware/view-mandatory-config`.

Pour définir des valeurs par défaut que les utilisateurs peuvent modifier, utilisez le fichier `/etc/vmware/view-default-config`. Quand des utilisateurs modifient un paramètre, tous les paramètres modifiés sont enregistrés dans le fichier `~/.vmware/view-preferences` lorsqu'ils quittent View Client.

Propriétés empêchant les utilisateurs de modifier des valeurs par défaut

Pour chaque propriété, vous pouvez définir une propriété `view.allow` correspondante qui contrôle si les utilisateurs sont autorisés à modifier le paramètre. Par exemple, si vous définissez la propriété `view.allowDefaultBroker` sur « FALSE » dans le fichier `/etc/vmware/view-mandatory-config`, les utilisateurs ne pourront pas modifier le nom dans le champ **[Server Name (Nom du serveur)]** lorsqu'ils utilisent View Client.

Syntaxe à utiliser dans l'interface de ligne de commande

Utilisez la forme suivante de la commande `vmware-view` dans une fenêtre de terminal.

`vmware-view [`*`command-line-option`* `[`*`argument`*`]] ...`

Par défaut, la commande `vmware-view` se trouve dans le répertoire `/usr/bin`.

Vous pouvez utiliser la forme abrégée ou la forme longue du nom d'option, même si toutes les options n'ont pas de forme abrégée. Par exemple, pour spécifier le domaine, vous pouvez utiliser `-d` (forme abrégée) ou `--domainName=` (forme longue). Vous pouvez choisir d'utiliser la forme longue pour faire un script plus lisible.

Vous pouvez utiliser l'option `--help` pour obtenir une liste d'options de ligne de commande et des informations sur l'utilisation.

IMPORTANT Si vous devez utiliser un proxy, appliquez la syntaxe suivante :

`http_proxy=`*`proxy_server_URL:port`* `https_proxy=`*`proxy_server_URL:port`* `vmware-view` *`options`*

Cette solution palliative est nécessaire, car vous devez effacer les variables d'environnement déjà définies pour le proxy. Si vous n'exécutez pas cette action, le paramètre d'exception de proxy n'entre pas en vigueur dans View Client. Vous pouvez configurer une exception de proxy pour l'instance du Serveur de connexion View.

Paramètres de configuration de View Client

Par souci de commodité, presque tous les paramètres de configuration possèdent une propriété *key=value* et un nom d'option de ligne de commande correspondant. Pour quelques paramètres, il existe une option de ligne de commande mais pas de propriété correspondante que vous pouvez définir dans un fichier de configuration. Pour d'autres paramètres, vous devez définir une propriété car aucune option de ligne de commande n'est disponible.

IMPORTANT Certaines options de ligne de commande et clés de configuration, telles que celles de la redirection USB et de MMR, sont disponibles uniquement avec la version View Client fournie pas des fournisseurs tiers. Pour plus d'informations sur ces partenaires, voir le *Guide de compatibilité VMware*.

Tableau 1-2. Options de ligne de commande et clés du fichier de configuration de View Client

Clé de configuration	Option de ligne de commande	Description

`view.allowDefaultBroker`	`-l`, `--lockServer`
	Exemple :
	`--lockServer -s view.company.com`
		À l'aide de cette option de ligne de commande, ou en définissant la propriété sur « FALSE », désactive le champ **[Server Name (Nom du serveur)]** sauf si le client ne s'est jamais connecté à aucun serveur et si aucune adresse de serveur n'est fournie dans la ligne de commande ou le fichier de préférences.

`view.autoConnectBroker`	Aucune	Se connecte automatiquement au dernier View server utilisé sauf si la propriété de configuration `view.defaultBroker` est définie ou si l'option de ligne de commande `--serverURL=` est utilisée. Spécifiez **"TRUE"** ou **"FALSE"**. La valeur par défaut est « FALSE ». Définir cette propriété et la propriété `view.autoConnectDesktop` sur « TRUE » revient à définir la propriété `view.nonInteractive` sur « TRUE ».

Tableau 1-2. Options de ligne de commande et clés du fichier de configuration de View Client (suite)

Clé de configuration	Option de ligne de commande	Description
`view.autoConnectDesktop`	Aucune	Se connecte automatiquement au dernier poste de travail View utilisé sauf si la propriété de configuration `view.defaultDesktop` est définie ou si l'option de ligne de commande `--desktopName=` est utilisée. Spécifiez **`"TRUE"`** ou **`"FALSE"`**. La valeur par défaut est « FALSE ». Définir cette propriété et la propriété `view.autoConnectBroker` sur « TRUE » revient à définir la propriété `view.nonInteractive` sur « TRUE ».

`view.defaultBroker`	`-s, --serverURL=`
	Exemples :
	`--serverURL=https://view.company.com`
	`-s view.company.com`
	`--serverURL=view.company.com:1443`
		Ajoute le nom que vous spécifiez au champ **[Server Name (Nom du serveur)]** dans View Client. Spécifiez un nom de domaine complet. Vous pouvez également spécifier un numéro de port si vous n'utilisez pas le port par défaut 443.
		Le port par défaut est la dernière valeur utilisée.

`view.defaultDesktop`	`-n, --desktopName=`	Spécifie quel poste de travail utiliser lorsque `autoConnectDesktop` est défini sur « TRUE » et que l'utilisateur a accès à plusieurs postes de travail. Il s'agit du nom que vous voyez dans la boîte de dialogue Select Desktop (Sélectionner un poste de travail). Le nom est généralement le nom de pool.
`view.defaultDesktopHeight`	Aucune	Spécifie la hauteur par défaut de la fenêtre pour le poste de travail View, en pixels.

`view.defaultDesktopSize`	`--desktopSize=`
	Exemples :
	`--desktopSize="1280x800"`
	`--desktopSize="all"`
		Définit la taille par défaut de la fenêtre pour le poste de travail View :
		■ Pour utiliser tous les écrans, définissez la propriété sur **`"1"`** ou utilisez l'argument de ligne de commande **`"all"`**.
		■ Pour utiliser le mode plein écran sur un écran, définissez la propriété sur **`"2"`** ou utilisez l'argument de ligne de commande **`"full"`**.
		■ Pour utiliser une grande fenêtre, définissez la propriété sur **`"3"`** ou utilisez l'argument de ligne de commande **`"large"`**.
		■ Pour utiliser une petite fenêtre, définissez la propriété sur **`"4"`** ou utilisez l'argument de ligne de commande **`"small"`**.
		■ Pour définir une taille personnalisée, définissez la propriété sur **`"5"`**, puis définissez les propriétés `view.defaultDesktopWidth` et `view.defaultDesktopHeight`. Vous pouvez également spécifier la largeur et la hauteur, en pixels, dans la ligne de commande avec **`"`*`widthxheight`*`"`**.

Tableau 1-2. Options de ligne de commande et clés du fichier de configuration de View Client (suite)

Clé de configuration	Option de ligne de commande	Description
`view.defaultDesktopWidth`	Aucune	Spécifie la largeur par défaut de la fenêtre pour le poste de travail View, en pixels.
`view.defaultDomain`	`-d, --domainName=`	Définit le nom de domaine que View Client utilise pour toutes les connexions et ajoute le nom de domaine que vous spécifiez au champ **[Domain Name (Nom du domaine)]** dans la boîte de dialogue d'authentification de View Client.
`view.defaultPassword`	`-p "-", --password="-"`	Spécifiez toujours **"-"** pour lire le mot de passe à partir de `stdin`. Définit le mot de passe que View Client utilise pour toutes les connexions et ajoute le mot de passe au champ **[Password (Mot de passe)]** dans la boîte de dialogue d'authentification de View Client si le Serveur de connexion View accepte l'authentification par mot de passe. REMARQUE Vous devez définir un mot de passe, c'est-à-dire que vous ne pouvez pas définir --password=""
`view.defaultProtocol`	`--protocol=`	Spécifie quel protocole d'affichage utiliser. Spécifiez **"PCOIP"** ou **"RDP"**. Ces valeurs tiennent compte de la casse. Par exemple, si vous entrez **rdp**, le protocole par défaut est utilisé. La valeur par défaut est la valeur définie dans View Administrator dans les paramètres du pool.
`view.defaultUser`	`-u, --userName=`	Définit le nom d'utilisateur que View Client utilise pour toutes les connexions et ajoute le nom d'utilisateur que vous spécifiez au champ **[User Name (Nom d'utilisateur)]** dans la boîte de dialogue d'authentification de View Client. Pour le mode kiosque, le nom de compte peut être basé sur l'adresse MAC du client, ou il peut commencer par une chaîne de préfixe reconnue, telle que **custom-**.
`view.fullScreen`	`--fullscreen`	Masque le système d'exploitation hôte et ouvre l'interface utilisateur de View Client en mode plein écran. Cette option n'affecte pas le mode d'affichage de la session de poste de travail. Si vous définissez la clé de configuration, spécifiez **"TRUE"** ou **"FALSE"**. La valeur par défaut est « FALSE ».

`view.kbdLayout`	`-k, --kbdLayout=`
	Exemples :
	`--kbdLayout="en-us"`
	`-k "fr"`
		Spécifie quel paramètre régional utiliser pour la disposition du clavier, par code de langue.

`view.kioskLogin`	`--kioskLogin` Exemple : Reportez-vous à la section « Exemple : Exemple du mode kiosque », page 24.	Spécifie que View Client est sur le point de s'authentifier à l'aide d'un compte en mode kiosque. Si vous définissez la clé de configuration, spécifiez **"TRUE"** ou **"FALSE"**. La valeur par défaut est « FALSE ».

Tableau 1-2. Options de ligne de commande et clés du fichier de configuration de View Client (suite)

Clé de configuration	Option de ligne de commande	Description
view.mmrPath	-m, --mmrPath= Exemple : --mmrPath="/usr/lib/altmmr"	(Disponible uniquement avec les distributions de fournisseurs tiers) Définit le chemin d'accès au répertoire qui contient les bibliothèques (redirection multimédia) Wyse MMR.
view.nomenubar	--nomenubar	Supprime la barre de menus View Client lorsque View Client fonctionne en mode Plein écran pour que les utilisateurs ne puissent pas accéder aux options de menu pour fermer une session sur un poste de travail View, réinitialiser un poste de travail View ou se déconnecter d'un poste de travail View. Utilisez cette option lorsque vous configurez le mode kiosque. Si vous définissez la clé de configuration, spécifiez **"TRUE"** ou **"FALSE"**. La valeur par défaut est « FALSE ».
view.nonInteractive	-q, --nonInteractive Exemple : --nonInteractive --serverURL="https://view.company.com" --userName="user1" --password="-" --domainName="xyz" --desktopName="Windows 7"	Masque les étapes d'interface utilisateur inutiles pour les utilisateurs finaux en ignorant les écrans spécifiés dans la ligne de commande ou les propriétés de configuration. Si vous définissez la clé de configuration, spécifiez **"TRUE"** ou **"FALSE"**. La valeur par défaut est « FALSE ». Définir cette propriété sur « TRUE » revient à définir les propriétés `view.autoConnectBroker` et `view.autoConnectDesktop` sur « TRUE ».
view.once	--once	Spécifie que vous ne voulez pas que View Client essaie de nouveau de se connecter en cas d'erreur. Utilisez --once si vous voulez obtenir un flux de travail similaire vers le client View 4.6. Cette option force View Client à quitter après que l'utilisateur s'est déconnecté d'un poste de travail ou a fermé une session sur un poste de travail. Vous devez généralement spécifier cette option si vous utilisez le mode kiosque et utiliser le code de sortie pour traiter l'erreur. Sinon, il peut vous sembler difficile de tuer le processus `vmware-view` à distance. Si vous définissez la clé de configuration, spécifiez **"TRUE"** ou **"FALSE"**. La valeur par défaut est « FALSE ».
view.rdesktopOptions	--rdesktopOptions= Exemple : --rdesktopOptions="-f -m"	(Disponible si vous utilisez le protocole d'affichage Microsoft RDP) Spécifie des options de ligne de commande à transmettre à l'application rdesktop. Pour plus d'informations sur les options rdesktop, consultez la documentation sur rdesktop.

Tableau 1-2. Options de ligne de commande et clés du fichier de configuration de View Client (suite)

Clé de configuration	Option de ligne de commande	Description

Aucune	`-r`, `--redirect=`
	Exemple :
	`--redirect="sound:off"`
		(Disponible si vous utilisez le protocole d'affichage Microsoft RDP) Spécifie un périphérique local que vous voulez que rdesktop redirige vers le poste de travail View.
		Spécifiez les informations du périphérique que vous voulez transmettre à l'option `-r` de rdesktop. Vous pouvez définir plusieurs options de périphérique dans une seule commande.

`view.sslVerificationMode`	Aucune	Définit le mode de vérification des certificats de serveur. Spécifiez **"1"** pour refuser des connexions lorsque le certificat échoue des vérifications, **"2"** pour avertir mais autoriser les connexions qui utilisent un certificat auto-signé ou **"3"** pour autoriser des connexions non vérifiables. Si vous spécifiez **"3"**, aucune vérification n'est effectuée. La valeur par défaut est « 2 ».

Aucune	`--printEnvironmentInfo`
	Exemple :
	`--printEnvironmentInfo -s view.company.com`
		Affiche des informations sur l'environnement d'un périphérique client, notamment son adresse IP, son adresse MAC, le nom de la machine et le nom de domaine.
		Pour le mode kiosque, vous pouvez créer un compte pour le client basé sur l'adresse MAC. Pour afficher l'adresse MAC, vous devez utiliser cette option avec l'option `-s`.

Aucune	`--usb=`	(Disponible uniquement avec les distributions de fournisseurs tiers) Spécifie les options à utiliser pour la redirection USB. Reportez-vous à la section « Redirection d'un périphérique USB vers un poste de travail distant », page 26.
Aucune	`--version`	Affiche des informations de version sur View Client.

Exemple : Exemple du mode kiosque

Les utilisateurs de kiosque peuvent être les clients d'une station d'enregistrement pour compagnies aériennes, les étudiants dans une salle de classe ou une bibliothèque, le personnel médical utilisant une station de travail de saisie de données médicales ou les clients d'un point libre-service. Les comptes sont associés à des périphériques client plutôt qu'à des utilisateurs car les utilisateurs n'ont pas à ouvrir de session pour utiliser le périphérique client ou le poste de travail View. Il peut toujours être demandé aux utilisateurs de fournir des informations d'identification d'authentification pour certaines applications.

Pour configurer le mode kiosque, vous devez utiliser l'interface de ligne de commande `vdmadmin` sur l'instance du Serveur de connexion View et effectuer plusieurs procédures décrites dans le chapitre sur le mode kiosque dans le document *Administration de VMware View*. Une fois le mode kiosque configuré, vous pouvez utiliser la commande `vmware-view` sur un client Linux pour vous connecter à un poste de travail View en mode kiosque.

Pour vous connecter à des postes de travail View depuis des clients Linux en mode kiosque, vous devez, au minimum, inclure les clés de configuration ou options de ligne de commande suivantes.

Clé de configuration	Options de ligne de commande équivalentes
view.kioskLogin	--kioskLogin
view.nonInteractive	-q, --nonInteractive
view.fullScreen	--fullscreen
view.nomenubar	--nomenubar
view.defaultBroker	-s, --serverURL=

L'omission de l'un de ces paramètres de configuration n'est pas prise en charge en mode kiosque. Si le Serveur de connexion View est configuré pour exiger un nom d'utilisateur de kiosque non défini par défaut, vous devez également définir la propriété `view.defaultUser` ou utiliser l'option de ligne de commande `-u` ou `--userName=`. Si un nom d'utilisateur de kiosque non défini par défaut n'est pas requis et si vous ne spécifiez pas de nom d'utilisateur, View Client peut dériver et utiliser le nom d'utilisateur de kiosque par défaut.

Remarque Si vous définissez la clé de configuration `view.sslVerificationMode`, veillez à la définir dans le fichier `/etc/vmware/view-mandatory-config`. Lorsque le client est exécuté en mode kiosque, il ne regarde pas dans le fichier `view-preferences`.

La commande indiquée dans cet exemple exécute View Client sur un système client Linux et possède les caractéristiques suivantes :

- Le nom du compte d'utilisateur est basé sur l'adresse MAC du client.
- View Client s'exécute en mode plein écran sans barre de menus de View Client.
- Les utilisateurs sont automatiquement connectés à l'instance du Serveur de connexion View et au poste de travail View spécifiés et ils ne sont pas invités à fournir des informations d'identification d'ouverture de session.
- Si une erreur de connexion se produit, en fonction du code d'erreur renvoyé, un script peut s'exécuter ou un programme de surveillance du kiosque peut gérer l'erreur. Par conséquent, le système client peut, par exemple, afficher un écran hors service ou peut attendre un certain temps avant de tenter de se connecter de nouveau au Serveur de connexion View.

```
./vmware-view --kioskLogin --nonInteractive --once --fullscreen --nomenubar
--serverURL="server.mycomany.com" --userName="CM-00:11:22:33:44:55:66:77" --password="mypassword"
```

Codes de sortie de View Client

L'interface de ligne de commande pour View Client peut renvoyer des codes de sortie pour indiquer la nature des erreurs rencontrées par View Client.

Tableau 1-3 montre les codes de sortie que la commande `vmware-view` peut renvoyer. Certains codes se rapportent uniquement à View Client pour Windows.

Tableau 1-3. Codes de sortie de View Client

Code de sortie	Description
-1	Erreur fatale en mode kiosque.
0	Réussite.
1	La connexion a échoué.
2	L'ouverture de session a échoué.
3	Le poste de travail n'a pas pu démarrer.
4	RDP n'a pas pu démarrer.
5	L'opération RDP a échoué.

Tableau 1-3. Codes de sortie de View Client (suite)

Code de sortie	Description
6	Connexion par tunnel perdue.
7	Échec de transfert du poste de travail local.
8	Échec de restitution du poste de travail local.
9	Échec d'emprunt du poste de travail local.
10	Échec de restauration du poste de travail local.
11	Résultat inconnu reçu au cours de l'authentification.
12	Erreur d'authentification.
13	Demande reçue pour utiliser une méthode d'authentification inconnue.
14	Réponse du serveur non valide.
15	Le poste de travail était déconnecté.
16	Le tunnel était déconnecté.
17	Réservé pour un développement futur.
18	Réservé pour un développement futur.
19	Opération de kiosque non prise en charge.
20	Erreur de connexion de souris, clavier ou écran à distance (RMKS).
21	Erreur de code PIN.
22	Non correspondance de code PIN.
23	Non correspondance de mot de passe.
24	Erreur de View Connection Server.
25	Le poste de travail n'était pas disponible.

Redirection d'un périphérique USB vers un poste de travail distant

Utilisez l'option de ligne de commande `--usb=` de la commande `vmware-view` pour configurer les périphériques USB à rediriger vers un poste de travail View. Notez que le composant USB est disponible uniquement avec la version de View Client pour Linux fournie par des fournisseurs tiers.

Les arguments de l'option `--usb=` sont envoyés à la commande de redirection USB `vmware-view-usb`.

L' exemple suivant active la journalisation au niveau de la trace :

```
vmware-view --usb=log:trace
```

Vous pouvez définir plusieurs instances de l'option `--usb` pour chaque option `vmware-view-usb` que vous spécifiez. L'exemple suivant active la journalisation au niveau du débogage et exclut un périphérique défini pas son ID :

```
 vmware-view --usb=log:debug
--usb=exid:vid0012pid0034
```

Le tableau suivant répertorie les arguments que vous pouvez utiliser avec l'option `--usb`.

Tableau 1-4. Options de redirection USB

Option	Description
`disable-boot-fwd`	Désactive la détection et le filtrage du périphérique d'amorçage par le client USB View. L'activation de cette option, redirige tous les périphériques USB, y compris celui depuis lequel le système client est démarré.

`ex:`*device1*`[,`*device2*`]...`	Exclut une liste de périphériques nommés à rediriger. Par exemple :
	`vmware-view`
	`--usb=ex:"flash 1"`

`exfa:`*device-family1*`[,`*device-family2*`]...`	Exclut une liste de familles de périphériques nommées de la redirection. Par exemple :
	`vmware-view`
	`--usb=exfa:storage`

`exid:`*device-ID1*`[,`*device-ID2*`]...`	Exclut une liste de périphériques de la redirection où les périphériques sont définis par les valeurs hexadécimales de leurs ID de fournisseur et de produit en utilisant le format `vid`*xxxx*`pid`*xxxx* . Par exemple :
	`vmware-view`
	`--usb=exid:vid1e2fpid5a1e`

`expt:`*device-path1*`[,`*device-path2*`]...`	Exclut une liste de périphériques de la redirection où les périphériques sont définis par les valeurs décimales de leur bus et leurs valeurs de port en utilisant le format `bus`*n*`port`*n*. Par exemple : `vmware-view --usb=expt:bus1port4,bus5port3`

`in:`*device1*`[,`*device2*`]...`	Inclut une liste de périphériques nommés à rediriger. Par exemple :
	`vmware-view`
	`--usb=in:"flash 1"`

`infa:`*device-family1*`[,`*device-family2*`]...`	Inclut une liste de familles de périphériques nommées à rediriger. Par exemple :
	`vmware-view`
	`--usb=infa:storage`

`inid:`*device-ID1*`[,`*device-ID2*`]...`	Inclut une liste de périphériques à rediriger où les périphériques sont définis par les valeurs hexadecimales de leurs ID de fournisseur et de produit en utilisant le format `vid`*xxxx*`pid`*xxxx* . Par exemple :
	`vmware-view`
	`--usb=inid:vid27f8pid2a1b`

`inpt:`*device-path1*`[,`*device-path2*`]...`	Inclut une liste de périphériques à rediriger où les périphériques sont définis par les valeurs décimales de leur bus et de leurs valeurs de port en utilisant le format format `bus`*n*`port`*n*. Par exemple :
	`vmware-view`
	`--usb=inpt:bus3port1,bus4port2`

`log:{debug|error|info|trace}`	Définit le niveau de journalisation `vmware-view-usb:trace`, `debug`, `info` (par défaut) ou `error` en ordre décroissant de détail. Le fichier journal (`backendLog.txt`) est écrit dans `/tmp/vmware-`*username*`/vmware-view-usb-`*pid*`.log`. Par exemple :
	`vmware-view`
	`--usb=log:error`

L'ordre de priorité d'inclusion ou d'exclusion des périphériques est le suivant, de la priorité la plus élevée à la priorité la plus basse :

1 `expt` (exclut les périphériques identifiés par le bus et le port)

2 `inpt` (inclut les périphériques identifiés par le bus et le port)

3 `ex` (exclut une liste de périphériques nommés)

4 `in` (inclut une liste de périphériques nommés)

5 `exid` (exclut les périphériques identifiés par les ID de fournisseur et de produit)

6 `inid` (inclut les périphériques identifiés par les ID de fournisseur et de produit)

7 `exfa` (exclut une liste de familles de périphériques nommées)

8 `infa` (inclut une liste de familles de périphériques nommées)

L'exemple suivant exclut tous les périphériques des familles de stockage, sauf un périphérique défini par son ID :

```
vmware-view --usb=exfa:storage
--usb=inid:vid1812pid1492
```

La liste suivante est une liste de catégories de familles de périphériques USB que vous pouvez utiliser avec les options `infa` et `exfa`.

`audio`	`printer`
`bluetooth`	`security`
`comm`	`smart-card`
`hid`	`storage`
`hid-bootable`	`unknown`
`hub`	`vendor`
`imaging`	`video`
`other`	`wireless`
`pda`	`wusb`
`physical`	

Index