# Configuration de pools de postes de travail et d'applications dans View

VMware Horizon 7
Version 7.0

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

FR-001999-00

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

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

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

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

docfeedback@vmware.com



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

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

# Table des matières

# Configuration de pools de postes de travail et d'applications dans View .

*Configuration des pools de postes de travail et d'applications dans View* explique comment créer et provisionner des pools de machines, et comment créer des pools d'applications distantes s'exécutant sur des hôtes des services Bureau à distance (RDS) Microsoft. Ce document explique comment préparer des machines, configurer des stratégies, attribuer des droits d'accès aux utilisateurs et aux groupes, configurer des fonctionnalités de poste de travail distant et des profils d'utilisateur avec View Persona Management.

## Public cible

Ces informations sont destinées à toute personne souhaitant créer et provisionner des pools de postes de travail et d'applications. Ce document a été rédigé à l'attention des administrateurs système Windows expérimentés qui connaissent bien la technologie de machines virtuelle et les opérations de centre de données.

# Introduction aux pools de postes de travail et d'applications

1

Avec Horizon 7, vous pouvez créer des pools de postes de travail qui incluent des milliers de postes de travail virtuels. Vous pouvez déployer des postes de travail qui s'exécutent sur des machines virtuelles (VM), des machines physiques et des hôtes des services Bureau à distance Windows (RDS). Créez une VM en tant qu'image de base de sorte qu'Horizon 7 puisse générer un pool de postes de travail virtuels à partir de cette image. Vous pouvez également créer des pools d'applications qui accordent aux utilisateurs un accès distant aux applications.

Ce chapitre aborde les rubriques suivantes :



## Batteries de serveurs, hôtes RDS et pools de postes de travail et d'applications

Vous pouvez créer des pools de postes de travail et d'applications afin d'accorder aux utilisateurs un accès distant à des postes de travail basés sur une machine virtuelle, à des postes de travail basés sur une session, à des ordinateurs physiques et à des applications. Vous pouvez également choisir Microsoft Remote Desktop Services (RDS), VMware PC-over-IP (PCoIP) ou VMware Blast pour fournir un accès distant aux utilisateurs.

### Hôtes RDS

Les hôtes RDS sont des ordinateurs serveurs sur lesquels les services Bureau à distance Windows et Horizon Agent sont installés. Ces serveurs hébergent des sessions d'application et de poste de travail auxquelles les utilisateurs peuvent accéder à distance. Pour accéder à des pools de postes de travail RDS ou à des applications, Horizon Client 3.0 ou version ultérieure est requis.

### Pools de postes de travail

Il existe trois principaux types de pools de postes de travail : automatisé, manuel et RDS. Les pools de postes de travail automatisés utilisent un modèle ou un snapshot de modèle de machine virtuelle vCenter Server pour créer un pool de machines virtuelles identiques. Les pools de postes de travail manuels sont une collection de machines virtuelles vCenter Server, d'ordinateurs physiques ou de machines virtuelles tierces existantes. Dans les pools automatisés ou manuels, chaque machine est disponible pour un seul accès utilisateur à distance à la fois. Les pools de postes de travail RDS ne sont pas une collection de machines. Ils fournissent plutôt des sessions de poste de travail sur des hôtes RDS. Plusieurs utilisateurs peuvent avoir plusieurs sessions de poste de travail simultanément sur un hôte RDS.

### Pools d'applications

Les pools d'applications vous permettent de fournir des applications à plusieurs utilisateurs. Les applications contenues dans les pools d'applications s'exécutent sur une batterie de serveurs d'hôtes RDS.

### Batteries de serveurs

Les batteries de serveurs sont une collection d'hôtes RDS, et elles facilitent leur gestion. Les batteries de serveur peuvent avoir un nombre variable d'hôtes RDS et fournissent un ensemble commun d'applications ou de postes de travail RDS aux utilisateurs. Lorsque vous créez un pool de postes de travail RDS ou un pool d'applications, vous devez spécifier une batterie de serveurs. Les hôtes RDS de la batterie de serveurs fournissent des sessions de postes de travail et d'applications aux utilisateurs.

## Avantages des pools de postes de travail

Horizon 7 permet de créer et d'approvisionner des pools de postes de travail comme base de la gestion centralisée.

Vous créez un pool de postes de travail distants à partir de l'une des sources suivantes :

- Un système physique comme un PC de poste de travail physique ou un hôte RDS.
- Une machine virtuelle hébergée sur un hôte ESXi et gérée par vCenter Server
- Une machine virtuelle s'exécutant sur une plate-forme de virtualisation autre que vCenter Server qui prend en charge Horizon Agent.

Si vous utilisez une machine virtuelle vSphere comme source de postes de travail, vous pouvez automatiser le processus pour faire autant de postes de travail virtuels identiques que nécessaire. Vous pouvez définir un nombre minimum et un nombre maximum de postes de travail virtuels à générer pour le pool. La définition de ces paramètres garantit que vous possédez toujours suffisamment de postes de travail distants disponibles pour une utilisation immédiate mais pas en excès pour ne pas abuser des ressources disponibles.

L'utilisation de pools pour gérer des postes de travail vous permet d'appliquer des paramètres ou de déployer des applications sur tous les postes de travail distants dans un pool. Les exemples suivants indiquent des paramètres disponibles :

- Spécifiez le protocole d'affichage à distance à utiliser par défaut pour le poste de travail distant et si vous autorisez les utilisateurs finaux à remplacer les valeurs par défaut.
- Pour des machines virtuelles de clone lié View Composer ou des machines virtuelles de clone complet, spécifiez si vous voulez désactiver la machine virtuelle lorsqu'elle n'est pas utilisée et si vous voulez la supprimer complètement. Les machines virtuelles de clone instantané sont toujours activées.
- Pour les machines virtuelles de clone lié View Composer, vous pouvez spécifier si vous voulez utiliser une spécification de personnalisation Microsoft Sysprep ou QuickPrep de VMware. Sysprep génère un ID de sécurité et un GUID uniques pour chaque machine virtuelle dans le pool. Les clones instantanés requièrent une spécification de personnalisation différente, appelée ClonePrep, de VMware.

Vous pouvez également spécifier comment les postes de travail dans un pool sont attribués aux utilisateurs.

| | |
|---|---|
| **Pools d'affectation dédiée** | Un poste de travail distant particulier est attribué à chaque utilisateur. Les utilisateurs reviennent au même poste de travail à chaque ouverture de session. Les pools d'affectation dédiée requièrent une relation poste de travail/utilisateur un-à-un. Par exemple, un pool de 100 postes de travail est nécessaire pour un groupe de 100 utilisateurs. |
| **Pools d'affectation flottante** | Le poste de travail distant est supprimé et recréé après chaque utilisation de façon facultative, offrant ainsi un environnement hautement contrôlé. |

L'utilisation de pools d'affectation flottante vous permet également de créer un pool de postes de travail qui peut être utilisé par des groupes d'utilisateurs. Par exemple, un pool de 100 postes de travail peut être utilisé par 300 utilisateurs s'ils travaillent en groupe de 100 utilisateurs à la fois.

## Pools de postes de travail pour des types de travailleurs spécifiques

View offre de nombreuses fonctionnalités qui vous aident à conserver de l'espace de stockage et à réduire la puissance de traitement requise pour plusieurs cas d'utilisation. La plupart de ces fonctions sont disponibles en tant que paramètres de pool.

Il est fondamental de se demander si un certain type d'utilisateur a besoin d'une image de poste de travail avec état ou sans état. Les utilisateurs qui ont besoin d'une image de poste de travail avec état possèdent des données dans l'image du système d'exploitation qui doivent être préservées, conservées et sauvegardées. Par exemple, ces utilisateurs installent certaines de leurs propres applications ou possèdent des données ne pouvant pas être enregistrées en dehors de la machine virtuelle, comme sur un serveur de fichiers ou dans une base de données d'applications.

**Images de poste de travail sans état**

Également appelées postes de travail non persistants, les architectures sans état ont plusieurs avantages. Elles sont notamment plus faciles à prendre en charge et ont des coûts de stockage plus faibles. Les autres avantages comprennent un besoin limité de sauvegarder les machines virtuelles et des options de récupération d'urgence et de continuité des activités plus faciles et moins coûteuses.

**Images de poste de travail avec état**

Également appelées postes de travail persistants, ces images peuvent nécessiter des techniques traditionnelles de gestion des images. Les images avec état peuvent avoir de faibles coûts de stockage avec certaines technologies de système de stockage. Les technologies de sauvegarde et de récupération telles que VMware Consolidated Backup et VMware Site Recovery Manager sont importantes lors de la sélection de stratégies pour la sauvegarde, la récupération d'urgence et la continuité des activités.

Il existe deux façons de créer des images de poste de travail sans état dans View :

- Vous pouvez créer des pools d'affectation flottante de machines virtuelles de clone instantané. La redirection de dossiers et les profils itinérants peuvent éventuellement être utilisés pour stocker des données utilisateur.
- Vous pouvez utiliser View Composer pour créer des pools d'affectation flottante de machines virtuelles de clone lié. La redirection de dossiers et les profils itinérants peuvent éventuellement être utilisés pour stocker des données utilisateur.

Il existe plusieurs façons de créer des images de poste de travail avec état dans View :

- Vous pouvez créer des pools d'affectation flottante de machines virtuelles de clone instantané et utiliser App Volumes pour lier des données utilisateur et des applications installées par l'utilisateur. La redirection de dossiers et les profils itinérants peuvent être utilisés en option pour stocker des données utilisateur.
- Vous pouvez utiliser View Composer pour créer des pools d'affectation dédiée de machines virtuelles de clone lié. Vous pouvez configurer des disques persistants de View Composer.
- Vous pouvez créer des clones complets ou des machines virtuelles complètes. Certains fournisseurs de stockage disposent de solutions de stockage rentables pour les clones complets. Ces fournisseurs possèdent souvent leurs propres pratiques et utilitaires d'approvisionnement. Si vous faites appel à l'un de ces fournisseurs, vous devrez peut-être créer un pool d'affectation dédiée manuel.

L'utilisation de postes de travail sans état ou avec état dépend du type de travailleur spécifique.

## Pools pour travailleurs

Vous pouvez normaliser des images de poste de travail sans état pour les travailleurs afin que l'image soit toujours dans une configuration connue et facilement prise en charge et pour que les travailleurs puissent ouvrir une session sur n'importe quel poste de travail disponible.

Comme les travailleurs effectuent des tâches répétitives à l'aide d'un petit nombre d'applications, vous pouvez créer des images de poste de travail sans état, ce qui permet de conserver des exigences d'espace de stockage et de traitement. Utilisez les paramètres de pool suivants :

- Créez un pool automatisé pour que les postes de travail puissent être créés lors de la création du pool ou générés à la demande en fonction de l'utilisation du pool.
- Pour les pools de clones instantanés, pour optimiser l'utilisation des ressources, utilisez le provisionnement à la demande pour accroître ou réduire le pool en fonction de l'utilisation. Veillez à spécifier suffisamment de postes de travail de rechange pour répondre à la fréquence de connexion.
- Utilisez une affectation flottante pour que les utilisateurs ouvrent une session sur n'importe quel poste de travail disponible. Ce paramètre réduit le nombre de postes de travail requis s'il n'est pas nécessaire que tout le monde ouvre une session simultanément.
- Créez des postes de travail de clone instantané ou de clone lié View Composer pour que les postes de travail partagent la même image de base et utilisent moins d'espace de stockage dans le centre de données que des machines virtuelles complètes.
- Pour les pools de postes de travail View Composer, déterminez quelle action, le cas échéant, exécuter lorsque les utilisateurs se déconnectent. Les disques croissent avec le temps. Vous pouvez conserver l'espace disque en actualisant le poste de travail à son état d'origine lorsque des utilisateurs ferment leur session. Vous pouvez également définir un planning pour l'actualisation périodique des postes de travail. Par exemple, vous pouvez programmer l'actualisation quotidienne, hebdomadaire ou mensuelle des postes de travail.
- Pour les pools de postes de travail de clone instantané, View supprime automatiquement le clone instantané dès qu'un utilisateur se déconnecte. Un clone instantané est créé et prêt pour la connexion du prochain utilisateur, ce qui actualise effectivement le poste de travail à chaque déconnexion.
- Le cas échéant, et si vous utilisez des pools de clones liés View Composer, envisagez de stocker les postes de travail sur des banques de données ESXi locales. Cette stratégie peut offrir des avantages tels que du matériel peu coûteux, un approvisionnement de machine virtuelle rapide, des opérations d'alimentation haute performance et une gestion simple. Pour voir une liste des limites, consultez « Stockage de clones liés View Composer sur des magasins de données locaux », page 288. Les pools de clones instantanés ne sont pas pris en charge sur les banques de données locales.

---

**Remarque** Pour obtenir des informations sur les autres types d'options de stockage, reportez-vous à Chapitre 16, « Réduction et gestion des exigences de stockage », page 271.

---

- Utilisez la fonction Gestion de persona pour que les utilisateurs disposent toujours de leur apparence de poste de travail et de leurs paramètres d'application préférés, comme avec les profils d'utilisateur Windows. Si vous n'avez pas défini les postes de travail pour qu'ils soient actualisés ou supprimés lors de la fermeture de session, vous pouvez configurer le persona à supprimer lors de la fermeture de session.

---

**Important** View Persona Management facilite l'implémentation d'un pool d'affectation flottante pour les utilisateurs qui ne veulent pas conserver de paramètres entre les sessions. Précédemment, l'une des restrictions des postes de travail d'affectation flottante était que lorsque des utilisateurs finaux fermaient une session, ils perdaient tous leurs paramètres de configuration et toutes les données stockées dans le poste de travail distant.

Chaque fois que les utilisateurs finaux ouvraient une session, l'arrière-plan de leur poste de travail était défini sur le fond d'écran par défaut, et ils devaient reconfigurer les préférences de chaque application. Avec View Persona Management, l'utilisateur final d'un poste de travail d'affectation flottante ne peut pas voir de différence entre sa session et une session sur un poste de travail d'affectation dédiée.

---

## Pools pour travailleurs du savoir et utilisateurs expérimentés

Les travailleurs du savoir doivent pouvoir créer des documents complexes et les conserver sur le poste de travail. Les utilisateurs expérimentés doivent pouvoir installer leurs propres applications et les conserver. En fonction de la nature et de la quantité de données personnelles devant être conservées, le poste de travail peut être avec ou sans état.

Pour les travailleurs du savoir qui n'ont pas besoin d'applications installées par l'utilisateur sauf pour une utilisation temporaire, vous pouvez créer des images de poste de travail sans état et enregistrer toutes leurs données personnelles en dehors de la machine virtuelle, sur un serveur de fichiers ou dans une base de données d'applications. Pour les autres travailleurs du savoir et pour les utilisateurs expérimentés, vous pouvez créer des images de poste de travail avec état. Utilisez les paramètres de pool suivants :

- Certains travailleurs expérimentés et travailleurs du savoir, tels que les comptables, les directeurs commerciaux, les analystes en recherche marketing, peuvent avoir besoin de se connecter au même poste de travail à chaque fois. Créez des pools d'affectation dédiée pour eux.
- Utilisez la fonction Gestion de persona pour que les utilisateurs disposent toujours de leur apparence de poste de travail et de leurs paramètres d'application préférés, comme avec les profils d'utilisateur Windows.
- Utilisez vStorage Thin Provisioning pour que chaque poste de travail n'utilise que l'espace de stockage dont le disque a besoin pour son fonctionnement initial.
- Pour les utilisateurs expérimentés et les travailleurs du savoir qui doivent installer leurs propres applications, ce qui ajoute des données au disque du système d'exploitation, il existe deux options. La première option consiste à créer des postes de travail de machine virtuelle complète et à utiliser Mirage pour déployer et mettre à jour des applications sans remplacer les applications installées par l'utilisateur.

  La seconde option consiste à créer un pool de clones liés ou de clones instantanés et à utiliser App Volumes pour conserver les applications installées par l'utilisateur et les données utilisateur à travers les connexions.
- Si des travailleurs du savoir n'ont pas besoin d'applications installées par l'utilisateur sauf pour une utilisation temporaire, vous pouvez créer des postes de travail de clone lié ou des postes de travail de clone instantané View Composer. Les images de poste de travail partagent la même image de base et utilisent moins d'espace de stockage que des machines virtuelles complètes.

- Si vous utilisez View Composer avec des postes de travail virtuels vSphere 5.1 ou version ultérieure, activez la fonctionnalité de récupération d'espace pour vCenter Server et pour le pool de postes de travail. Avec la fonction de récupération d'espace, les données périmées ou supprimées dans un système d'exploitation client sont automatiquement récupérées avec un processus d'effacement et de réduction.
- Si vous utilisez des postes de travail de clone lié View Composer, implémentez View Persona Management, des profils itinérants ou une autre solution de gestion des profils. Vous pouvez également configurer des disques persistants pour pouvoir actualiser et recomposer les disques du système d'exploitation de clone lié tout en conservant une copie du profil d'utilisateur sur les disques persistants.
- Si vous utilisez des postes de travail de clone instantané, implémentez des profils itinérants ou une autre solution de gestion des profils. Vous n'avez pas besoin de configurer des disques persistants. Vous pouvez utiliser App Volumes pour conserver une copie des données utilisateur et du profil.

## Pools pour utilisateurs de 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 associés à des périphériques client plutôt qu'à des utilisateurs sont autorisés à utiliser ces pools de postes de travail, car les utilisateurs n'ont pas à ouvrir de session pour utiliser le périphérique client ou le poste de travail distant. Il peut toujours être demandé aux utilisateurs de fournir des informations d'identification d'authentification pour certaines applications.

Les postes de travail de machine virtuelle qui sont exécutés en mode kiosque utilisent des images de poste de travail sans état, car les données utilisateur n'ont pas à être conservées sur le disque du système d'exploitation. Les postes de travail en mode kiosque sont utilisés avec des périphériques de client léger ou des ordinateurs verrouillés. Vous devez vérifier que l'application du poste de travail implémente les mécanismes d'authentification pour des transactions sécurisées, que le réseau physique est sécurisé contre la falsification et la surveillance de trafic et que tous les périphériques connectés au réseau sont approuvés.

Il est recommandé d'utiliser des instances de Serveur de connexion View dédiées pour traiter des clients en mode kiosque, et de créer des unités d'organisation et des groupes dédiés dans Active Directory pour les comptes de ces clients. Cette pratique partitionne ces systèmes contre les intrusions injustifiées et facilite la configuration et l'administration des clients.

Pour configurer le mode kiosque, vous devez utiliser l'interface de ligne de commande `vdmadmin` et effectuer plusieurs procédures décrites dans les rubriques sur le mode kiosque du document *Administration de View*. Dans le cadre de cette configuration, vous pouvez utiliser les paramètres de pool suivants.

- Créez un pool automatisé pour que les postes de travail puissent être créés lors de la création du pool ou générés à la demande en fonction de l'utilisation du pool.
- Utilisez l'affectation flottante pour que les utilisateurs puissent accéder à n'importe quel poste de travail disponible dans le pool.
- Créez des postes de travail de clone instantané ou de clone lié View Composer pour que les postes de travail partagent la même image de base et utilisent moins d'espace de stockage dans le centre de données que des machines virtuelles complètes.
- Si vous utilisez des postes de travail de clone lié View Composer, créez une stratégie d'actualisation pour que le poste de travail soit actualisé régulièrement, comme à chaque déconnexion de l'utilisateur.
- Si vous utilisez des pools de postes de travail de clone instantané, View supprime automatiquement le clone instantané dès qu'un utilisateur se déconnecte. Un clone instantané est créé et prêt pour la connexion du prochain utilisateur, ce qui actualise effectivement le poste de travail à chaque déconnexion.

- Le cas échéant, envisagez de stocker des postes de travail sur des magasins de données ESXi locaux. Cette stratégie peut offrir des avantages tels que du matériel peu coûteux, un approvisionnement de machine virtuelle rapide, des opérations d'alimentation haute performance et une gestion simple. Pour voir une liste des limites, consultez « Stockage de clones liés View Composer sur des magasins de données locaux », page 288. Les pools de clones instantanés ne sont pas pris en charge sur les banques de données locales.

  **Remarque** Pour obtenir des informations sur les autres types d'options de stockage, reportez-vous à Chapitre 16, « Réduction et gestion des exigences de stockage », page 271.

- Utilisez un GPO Active Directory pour configurer l'impression basée sur l'emplacement afin que le poste de travail utilise l'imprimante la plus proche. Pour obtenir la liste complète et la description des paramètres disponibles dans les modèles d'administration de stratégie de groupe (ADM), reportez-vous à Chapitre 17, « Configuration de stratégies pour des pools de postes de travail et d'applications », page 297.
- Utilisez un GPO ou la fonctionnalité Stratégies de carte à puce pour contrôler si des périphériques USB locaux sont connectés au poste de travail lorsque ce dernier est lancé ou lorsque des périphériques USB sont branchés sur l'ordinateur client.

## Avantages des pools d'applications

Les pools d'applications vous permettent d'octroyer aux utilisateurs un accès aux applications qui s'exécutent sur les serveurs d'un centre de données plutôt que sur leur ordinateur personnel ou leur périphérique.

Les pools d'applications offrent plusieurs avantages importants :

- Accessibilité

  Les utilisateurs peuvent accéder à des applications depuis n'importe quel point du réseau. Vous pouvez également configurer un accès réseau sécurisé.

- Indépendance des périphériques

  Avec les pools d'applications, vous pouvez prendre en charge toute une gamme de périphériques client, comme des smartphones, des tablettes, des clients légers, des ordinateurs portables et des ordinateurs de bureau. Les périphériques client peuvent exécuter différents systèmes d'exploitation comme Windows, iOS, Mac OS ou Android.

- Contrôle d'accès

  Vous pouvez facilement et rapidement accorder ou supprimer l'accès aux applications à un utilisateur ou à un groupe d'utilisateurs.

- Déploiement accéléré

  Avec les pools d'applications, le déploiement d'applications peut être accéléré, car vous ne déployer des applications que sur des serveurs dans un centre de données et chaque serveur peut prendre en charge plusieurs utilisateurs.

- Gérabilité

  La gestion du logiciel déployé sur les ordinateurs et périphériques client nécessite généralement des ressources significatives. Les tâches de gestion incluent le déploiement, la configuration, la maintenance, la prise en charge et les mises à niveau. Avec les pools d'applications, vous pouvez simplifier la gestion de logiciel d'une entreprise, car le logiciel s'exécute sur des serveurs dans un centre de données, ce qui nécessite un nombre moindre de copies installées.

- Sécurité et conformité réglementaire

Avec les pools d'applications, vous pouvez améliorer la sécurité, car les applications et leurs données associées sont regroupées dans centre de données. La centralisation des données peut résoudre les problèmes de sécurité et de conformité réglementaire.

- Réduction du coût

  En fonction des contrats de licence logicielle, l'hébergement d'applications dans un centre de données peut être plus rentable. D'autres facteurs, notamment le déploiement accéléré et l'amélioration de la facilité de gestion, peuvent également réduire le coût du logiciel dans une entreprise.

# Préparation de machines non gérées 2

Les utilisateurs peuvent accéder à des postes de travail distants fournis par des machines qui ne sont pas gérées par vCenter Server. Ces machines non gérées peuvent inclure des ordinateurs physiques et des machines virtuelles fonctionnant sur des plates-formes de virtualisation autres que vCenter Server. Vous devez préparer une machine non gérée pour fournir un accès à un poste de travail distant.

Pour plus d'informations sur la préparation de machines qui sont utilisées en tant qu'hôtes des services Bureau à distance (Remote Desktop Services, RDS), reportez-vous à Chapitre 8, « Configuration des hôtes de services Bureau à distance », page 115.

Pour plus d'informations sur la préparation des machines virtuelles Linux pour le déploiement de postes de travail distants, consultez le guide *Configuration des postes de travail Horizon 7 for Linux*.

Ce chapitre aborde les rubriques suivantes :



## Préparer une machine non gérée pour un déploiement de postes de travail distants

Vous devez effectuer un certain nombre de tâches pour préparer une machine non gérée pour un déploiement de postes de travail distants.

### Prérequis

- Vérifiez que vous disposez des droits d'administration sur la machine non gérée.
- Pour vous assurer que les utilisateurs de postes de travail distants sont ajoutés au groupe Utilisateurs des services Bureau à distance local de la machine non gérée, créez un groupe Utilisateurs des services Bureau à distance restreint dans Active Directory. Reportez-vous au document *Installation de View* pour plus d'informations.

### Procédure

1. Mettez sous tension la machine non gérée et vérifiez qu'elle est accessible à l'instance du Serveur de connexion View.
2. Associez la machine non gérée au domaine Active Directory de vos postes de travail distants.
3. Configurez le Pare-feu Windows afin d'autoriser les connexions Bureau à distance à la machine non gérée.

### Suivant

Installez Horizon Agent sur la machine non gérée. Reportez-vous à la section « Installer Horizon Agent sur une machine non gérée », page 20.

## Installer Horizon Agent sur une machine non gérée

Vous devez installer Horizon Agent sur toutes les machines non gérées. View ne peut pas gérer une machine non gérée si Horizon Agent n'est pas installé.

Pour installer Horizon Agent sur plusieurs ordinateurs physiques Windows sans avoir à répondre à des invites d'assistant, vous pouvez installer Horizon Agent en mode silencieux. Reportez-vous à la section « Installer Horizon Agent en silence », page 37.

### Prérequis

- Vérifiez que vous disposez des droits d'administration sur la machine non gérée.
- Pour utiliser une machine virtuelle Windows Server non gérée en tant que poste de travail distant plutôt qu'en tant qu'hôte RDS, procédez de la manière décrite dans « Préparer les systèmes d'exploitation Windows Server à une utilisation comme poste de travail », page 31.
- Familiarisez-vous avec les options de configuration personnalisée d'Horizon Agent pour des machines non gérées. Reportez-vous à la section « Options d'installation personnalisée d'Horizon Agent pour des machines non gérées », page 21.
- Familiarisez-vous avec les ports TCP que le programme d'installation d'Horizon Agent ouvre sur le pare-feu. Pour plus d'informations, reportez-vous au document *Planification de l'architecture de View*.
- Si le module Microsoft Visual C++ Redistributable est installé sur la machine, vérifiez que la version du module est 2005 SP1 ou version ultérieure. Si la version du module est 2005 ou antérieure, vous pouvez effectuer la mise à niveau ou désinstaller le module.
- Téléchargez le fichier du programme d'installation d'Horizon Agent sur la page des produits VMware, à l'adresse http://www.vmware.com/go/downloadview.

### Procédure

1. Pour démarrer le programme d'installation d'Horizon Agent, double-cliquez sur le fichier du programme d'installation.

   Le nom de fichier du programme d'installation est `VMware-viewagent-y.y.y-xxxxxx.exe` ou `VMware-viewagent-x86_64-y.y.y-xxxxxx.exe`, où *y.y.y* est le numéro de version et *xxxxxx* le numéro de build.

2. Acceptez les termes de licence VMware.
3. Sélectionnez la version du protocole Internet (**IPv4** ou **IPv6**).

   Vous devez installer tous les composants View avec la même version IP.

4. Sélectionnez si le mode FIPS doit être activé ou désactivé.

   Cette option n'est disponible que si le mode FIPS est activé dans Windows.

5. Sélectionnez les options d'installation personnalisée désirées.
6. Acceptez ou modifiez le dossier de destination.
7. Dans la zone de texte **Serveur**, saisissez le nom d'hôte ou l'adresse IP d'un hôte du Serveur de connexion View.

   Lors de l'installation, le programme d'installation inscrit la machine non gérée sur cette instance du Serveur de connexion View. Après l'inscription, l'instance du Serveur de connexion View spécifiée, et toutes les instances supplémentaires du même groupe que le Serveur de connexion View, peuvent communiquer avec la machine non gérée.

8 Sélectionnez une méthode d'authentification pour inscrire la machine non gérée sur l'instance du Serveur de connexion View.

| Option | Action |
|---|---|
| **Authenticate as the currently logged in user (S'authentifier comme étant l'utilisateur actuellement connecté)** | Les zones de texte **Nom d'utilisateur** et **Mot de passe** sont désactivées et vous ouvrez une session sur l'instance du Serveur de connexion View avec vos nom d'utilisateur et mot de passe actuels. |
| **Specify administrator credentials (Spécifier des informations d'identification d'administrateur)** | Vous devez fournir le nom d'utilisateur et le mot de passe d'un administrateur du Serveur de connexion View dans les zones de texte **Nom d'utilisateur** et **Mot de passe**. |

Entrez le nom d'utilisateur dans le format suivant : `Domaine\Utilisateur`.

Le compte d'utilisateur doit être un utilisateur de domaine ayant un accès à View LDAP sur l'instance du Serveur de connexion View. Un utilisateur local ne fonctionne pas.

9 Suivez les invites dans le programme d'installation d'Horizon Agent et terminez l'installation.

10 Si vous avez sélectionné l'option Redirection USB, redémarrez la machine non gérée pour activer la prise en charge USB.

De plus, l'assistant **Nouveau matériel détecté** doit démarrer. Suivez les invites de l'assistant pour configurer le matériel avant de redémarrer la machine non gérée.

Le service VMware Horizon Horizon Agent démarre sur la machine non gérée.

### Suivant

Utilisez la machine non gérée pour créer un poste de travail distant. Reportez-vous à la section « Pools de postes de travail manuels », page 107.

## Options d'installation personnalisée d' Horizon Agent pour des machines non gérées

Lorsque vous installez Horizon Agent sur une machine non gérée, vous pouvez sélectionner ou désélectionner des options d'installation personnalisée. En outre, Horizon Agent installe automatiquement certaines fonctionnalités sur tous les systèmes d'exploitation invités sur lesquels elles sont prises en charge. Ces fonctionnalités ne sont pas facultatives.

Pour modifier des options d'installation personnalisée après avoir installé la dernière version d'Horizon Agent, vous devez désinstaller et réinstaller Horizon Agent. Pour les correctifs et les mises à niveau, vous pouvez exécuter le nouveau programme d'installation d'Horizon Agent et sélectionner un nouvel ensemble d'options sans désinstaller la version précédente.

**Tableau 2-1.** Options d'installation personnalisée d' Horizon Agent pour les machines non gérées dans un environnement IPv4 (facultatif)

| Option | Description |
|---|---|
| Redirection USB | Donne aux utilisateurs un accès à des périphériques USB connectés en local sur leurs postes de travail.<br>La fonctionnalité Redirection USB est prise en charge sur les postes de travail distants qui sont déployés sur des machines mono-utilisateur. En outre, la redirection de lecteurs flash et de disques durs USB est prise en charge sur les postes de travail et applications RDS.<br>Cette option n'est pas sélectionnée par défaut. Vous devez sélectionner l'option pour l'installer.<br>Pour obtenir des instructions sur l'utilisation de la redirection USB en toute sécurité, reportez-vous au guide *Sécurité de View*. Par exemple, vous pouvez utiliser les paramètres de stratégie de groupe pour désactiver une redirection USB pour des utilisateurs spécifiques. |
| Redirection de lecteur client | Permet aux utilisateurs d'Horizon Client de partager des lecteurs locaux avec leurs postes de travail distants.<br>Une fois cette option d'installation installée, aucune autre configuration n'est requise sur le poste de travail distant.<br>La redirection de lecteur client est également prise en charge sur les postes de travail VDI exécutés sur des machines virtuelles mono-utilisateur gérées et sur des postes de travail et applications RDS. |
| View Persona Management | Synchronise le profil d'utilisateur sur le poste de travail local avec un référentiel de profils distant, pour que les utilisateurs puissent accéder à leurs profils dès qu'ils ouvrent une session sur un poste de travail. |
| Redirection de carte à puce | Permet aux utilisateurs de s'authentifier avec des cartes à puce lorsqu'ils utilisent le protocole d'affichage PCoIP ou Blast Extreme.<br>L'option Redirection de carte à puce est prise en charge sur des postes de travail distants déployés sur des machines mono-utilisateur, mais pas sur des postes de travail distants basés sur un hôte RDS. |
| Pilote audio virtuel | Fournit un pilote audio virtuel sur le poste de travail distant. |

Dans un environnement IPv6, la redirection de carte à puce est la seule fonctionnalité facultative.

**Tableau 2-2.** Fonctionnalités Horizon Agent qui sont installées automatiquement sur des machines non gérées dans un environnement IPv4 (non facultatives)

| Fonction | Description |
|---|---|
| PCoIP Agent | Permet aux utilisateurs de se connecter au poste de travail distant à l'aide du protocole d'affichage PCoIP.<br>La fonctionnalité PCoIP Agent est prise en charge sur les machines physiques configurées avec une carte d'hôte Teradici TERA. |
| Lync | Fournit la prise en charge de Microsoft Lync 2013 Client sur les postes de travail distants. |
| Unity Touch | Permet aux utilisateurs de tablette et de smartphone d'entrer facilement en interaction avec les applications Windows qui s'exécutent sur le poste de travail distant. Les utilisateurs peuvent parcourir, rechercher et ouvrir des applications et des fichiers Windows, choisir des applications et des fichiers favoris, et basculer entre les applications en cours d'exécution, le tout sans utiliser le menu Démarrer ni la barre des tâches. |

Dans un environnement IPv6, PCoIP Agent est la seule fonctionnalité automatiquement installée.

# Création et préparation d'une machine virtuelle parente pour le clonage

# 3

Vous pouvez créer un pool de machines de poste de travail en clonant une machine virtuelle vCenter Server. Avant de créer le pool de postes de travail, vous devez préparer et configurer cette machine virtuelle, qui sera la parente des clones.

Pour plus d'informations sur la préparation de machines qui sont utilisées en tant qu'hôtes des services Bureau à distance (Remote Desktop Services, RDS), reportez-vous à Chapitre 8, « Configuration des hôtes de services Bureau à distance », page 115.

Pour plus d'informations sur la préparation de machines virtuelles Linux pour le déploiement des postes de travail distants, consultez le guide *Configuration des postes de travail Horizon 7 for Linux*.

---

**Remarque**

- À partir de la version 7.0, View Agent est renommé Horizon Agent et View Administrator devient Horizon Administrator.
- VMware Blast, le protocole d'affichage disponible à partir d'Horizon 7.0, est également appelé VMware Blast Extreme.

---

Ce chapitre aborde les rubriques suivantes :

# Création d'une machine virtuelle pour le clonage

La première étape du processus de déploiement d'un pool de postes de travail clonés consiste à créer une machine virtuelle dans vSphere, à installer et à configurer le système d'exploitation.

1 Créer une machine virtuelle dans vSphere page 26

   Vous pouvez créer une machine virtuelle dans vSphere à partir de zéro ou en clonant une machine virtuelle existante. Cette procédure décrit la création d'une machine virtuelle à partir de zéro.

2 Installer un système d'exploitation client page 28

   Après avoir créé une machine virtuelle, vous devez installer un système d'exploitation client.

3 Préparer un système d'exploitation invité pour le déploiement de postes de travail distants page 29

   Vous devez effectuer un certain nombre de tâches pour préparer un système d'exploitation invité pour le déploiement de postes de travail distants.

4 Préparer les systèmes d'exploitation Windows Server à une utilisation comme poste de travail page 31

   Pour utiliser une machine virtuelle Windows Server 2008 R2 ou Windows Server 2012 R2 en tant que poste de travail View à session unique (plutôt que comme hôte RDS), vous devez effectuer certaines étapes avant d'installer Horizon Agent sur la machine virtuelle. Vous devez également configurer View Administrator pour qu'il reconnaisse Windows Server comme un système d'exploitation pris en charge pour utiliser le poste de travail View.

5 Installer la fonctionnalité Expérience utilisateur sur Windows Server 2008 R2 page 32

   Pour les postes de travail et applications RDS, et pour les postes de travail VDI déployés sur des machines virtuelles mono-utilisateur s'exécutant sous Windows Server, la redirection de scanner requiert l'installation de la fonctionnalité Expérience de poste de travail sur les hôtes RDS et les machines virtuelles mono-utilisateur.

6 Installer la fonctionnalité Expérience utilisateur sur Windows Server 2012 ou 2012 R2 page 32

   Pour les postes de travail et applications RDS, et pour les postes de travail VDI déployés sur des machines virtuelles mono-utilisateur s'exécutant sous Windows Server, la redirection de scanner requiert l'installation de la fonctionnalité Expérience de poste de travail sur les hôtes RDS et les machines virtuelles mono-utilisateur.

7 Configurer le service Pare-feu Windows pour redémarrer après les pannes page 33

   Certaines machines Windows Server 2012 R2, Windows 8.1 et Windows 10 qui sont déployées comme postes de travail à session unique ne deviennent pas immédiatement disponibles après leur provisionnement. Ce problème se produit lorsque le service Pare-feu Windows ne redémarre pas après l'expiration de son délai d'attente. Vous pouvez configurer le service Pare-feu Windows sur la machine virtuelle parente ou le modèle de machine virtuelle pour garantir que toutes les machines d'un pool de postes de travail deviennent disponibles.

## Créer une machine virtuelle dans vSphere

Vous pouvez créer une machine virtuelle dans vSphere à partir de zéro ou en clonant une machine virtuelle existante. Cette procédure décrit la création d'une machine virtuelle à partir de zéro.

### Prérequis

- Familiarisez-vous avec les paramètres de configuration personnalisés pour les machines virtuelles. Reportez-vous à la section « Paramètres de configuration personnalisés de machine virtuelle », page 27.

### Procédure

1 Connectez-vous à vSphere Client.

2 Sélectionnez **Fichier > Nouveau > Machine virtuelle** pour démarrer l'assistant Nouvelle machine virtuelle.

3 Sélectionnez **Personnalisé** et configurez des paramètres de configuration personnalisés.

4 Sélectionnez **Modifier les paramètres de la machine virtuelle avant l'achèvement** et cliquez sur **Continuer** pour configurer des paramètres matériels.

   a Ajoutez un lecteur CD/DVD, définissez le type de support pour utiliser un fichier image ISO, sélectionnez le fichier image ISO d'un système d'exploitation approprié, puis sélectionnez **Se connecter à la mise sous tension**.

   b Définissez **Délai de démarrage d'activation** sur 10 000 millisecondes.

5 Cliquez sur **Terminer** pour créer la machine virtuelle.

### Suivant

Installez le système d'exploitation.

## Paramètres de configuration personnalisés de machine virtuelle

Vous pouvez utiliser des paramètres de configuration personnalisés de machine virtuelle comme paramètres de ligne de base lorsque vous créez une machine virtuelle pour le déploiement de postes de travail distants.

Vous pouvez modifier certains paramètres lorsque vous utilisez View Administrator pour déployer des pools de postes de travail à partir de la machine virtuelle.

**Tableau 3-1.** Paramètres de configuration personnalisés

| Paramètre | Description et recommandations |
|---|---|
| `Name and Location` | Nom et emplacement de la machine virtuelle.<br>Si vous prévoyez d'utiliser la machine virtuelle comme modèle, affectez un nom générique. L'emplacement peut être n'importe quel dossier de votre inventaire de datacenter. |
| `Host/Cluster` | Ressources du serveur ou du cluster de serveurs ESXi qui exécuteront la machine virtuelle.<br>Si vous prévoyez d'utiliser la machine virtuelle comme modèle, l'emplacement de la machine virtuelle initiale ne spécifie pas nécessairement où résideront les futures machines virtuelles créées à partir du modèle. |
| `Resource Pool` | Si les ressources du serveur ESXi physique sont divisées en pools de ressources, vous pouvez les attribuer à la machine virtuelle. |
| `Datastore` | Emplacement de fichiers associés à la machine virtuelle. |
| `Hardware Machine Version` | La version matérielle de machine qui est disponible dépend de la version d'ESXi que vous exécutez. Nous vous recommandons de sélectionner la version matérielle de machine la plus récente qui offre les meilleures performances de machine virtuelle. Certaines fonctionnalités de View nécessitent des versions matérielles de machine minimales. |
| `Guest Operating System` | Type de système d'exploitation que vous installerez sur la machine virtuelle. |
| `CPUs` | Nombre de processeurs virtuels dans la machine virtuelle.<br>Pour la plupart des systèmes d'exploitation clients, un seul processeur est suffisant. |
| `Memory` | Quantité de mémoire à allouer à la machine virtuelle.<br>Dans la plupart des cas, 512 Mo est suffisant. |

**Tableau 3-1.** Paramètres de configuration personnalisés (suite)

| Paramètre | Description et recommandations |
|---|---|
| `Network` | Nombre de cartes réseau dans la machine virtuelle.<br>Une carte réseau est normalement suffisante. Le nom de réseau doit être cohérent dans les infrastructures virtuelles. Un nom de réseau incorrect dans un modèle peut provoquer des pannes lors des phases de personnalisation d'instance.<br>Lorsque vous installez Horizon Agent sur une machine virtuelle qui possède plusieurs cartes réseau, vous devez configurer le sous-réseau qu'Horizon Agent utilise. Pour plus d'informations, reportez-vous à « Configurer une machine virtuelle avec plusieurs cartes réseau pour Horizon Agent », page 44.<br>**Important** Pour les systèmes d'exploitation Windows 7, Windows 8.*, Windows 10, Windows Server 2008 R2 et Windows Server 2012 R2, vous devez sélectionner l'adaptateur réseau VMXNET 3. L'utilisation de l'adaptateur E1000 par défaut peut entraîner des erreurs d'expiration de personnalisation sur les machines virtuelles. Pour utiliser l'adaptateur VMXNET 3, vous devez installer un correctif Microsoft :<br>■ Pour Windows 7 SP1 : http://support.microsoft.com/kb/2550978<br>Installez le correctif avant d'installer Horizon Agent. Lorsque vous installez le correctif, si vous rencontrez une erreur Windows Update 0x80070424, consultez https://support.microsoft.com/en-us/kb/968002. |
| `SCSI Controller` | Type d'adaptateur SCSI à utiliser avec la machine virtuelle.<br>Pour les systèmes d'exploitation invités Windows 8/8.1 et Windows 7, vous devez spécifier l'adaptateur LSI Logic. L'adaptateur LSI Logic a des performances améliorées et fonctionne mieux avec des périphériques SCSI génériques.<br>LSI Logic SAS est disponible uniquement pour les machines virtuelles avec la version matérielle 7 et supérieure. |
| `Select a Disk` | Disque à utiliser avec la machine virtuelle.<br>Créez un nouveau disque virtuel basé sur la quantité de stockage local que vous décidez d'allouer à chaque utilisateur. Allouez assez d'espace de stockage pour l'installation du système d'exploitation, les correctifs et les applications installées en local.<br>Pour réduire le besoin d'espace de disque et la gestion de données locales, vous devez stocker les informations, le profil et les documents de l'utilisateur sur des partages réseau plutôt que sur un disque local. |

## Installer un système d'exploitation client

Après avoir créé une machine virtuelle, vous devez installer un système d'exploitation client.

### Prérequis

- Vérifiez qu'un fichier image ISO du système d'exploitation invité se trouve dans une banque de données sur votre serveur ESXi.
- Vérifiez que le lecteur CD/DVD dans la machine virtuelle pointe vers le fichier image ISO du système d'exploitation client et que le lecteur CD/DVD est configuré pour se connecter lors de l'activation.

### Procédure

1. Dans vSphere Client, ouvrez une session sur le système vCenter Server où réside la machine virtuelle.
2. Cliquez avec le bouton droit sur la machine virtuelle, sélectionnez **Alimentation**, puis **Activer** pour démarrer la machine virtuelle.

   Comme vous avez configuré le lecteur CD/DVD pour qu'il pointe vers le fichier image ISO du système d'exploitation client et qu'il se connecte lors de l'activation, le processus d'installation du système d'exploitation client démarre automatiquement.
3. Cliquez sur l'onglet **Console** et suivez les instructions d'installation fournies par le fournisseur du système d'exploitation.

4 Activez Windows.

### Suivant

Préparez le système d'exploitation client pour le déploiement de poste de travail View.

## Préparer un système d'exploitation invité pour le déploiement de postes de travail distants

Vous devez effectuer un certain nombre de tâches pour préparer un système d'exploitation invité pour le déploiement de postes de travail distants.

### Prérequis

- Créez une machine virtuelle et installez un système d'exploitation client.
- Configurez un contrôleur de domaine Active Directory pour vos postes de travail distants. Consultez le document *Installation de View* pour plus d'informations.
- Pour vous assurer que les utilisateurs de postes de travail sont ajoutés au groupe Utilisateurs des services Bureau à distance local de la machine virtuelle, créez un groupe Utilisateurs des services Bureau à distance restreint dans Active Directory. Consultez le document *Installation de View* pour plus d'informations.
- Vérifiez que les services Bureau à distance sont démarrés sur la machine virtuelle. Les services Bureau à distance sont requis pour l'installation d'Horizon Agent, l'authentification unique et d'autres opérations de View. Vous pouvez désactiver l'accès RDP vers vos postes de travail View en configurant des paramètres de pool de postes de travail et des paramètres de stratégie de groupe. Reportez-vous à la section « Empêcher l'accès à des postes de travail View via RDP », page 183.
- Vérifiez que vous disposez de droits d'administration sur le système d'exploitation client.
- Sur les systèmes d'exploitation Windows Server, préparez le système d'exploitation pour l'utilisation d'un poste de travail. Reportez-vous à la section « Préparer les systèmes d'exploitation Windows Server à une utilisation comme poste de travail », page 31.
- Si vous prévoyez de configurer le rendu graphique 3D pour des pools de postes de travail, familiarisez-vous avec le paramètre **Activer la prise en charge 3D** pour les machines virtuelles.

  Cette paramètre est actif sur les systèmes d'exploitation Windows 7 et supérieurs. Sur les hôtes ESXi 5.1 et supérieurs, vous pouvez également sélectionner des options qui déterminent comment le convertisseur 3D est géré sur l'hôte ESXi. Pour plus d'informations, consultez le document *Administration d'une machine virtuelle vSphere*.

### Procédure

1 Dans vSphere Client, ouvrez une session sur le système vCenter Server où réside la machine virtuelle.

2 Cliquez avec le bouton droit sur la machine virtuelle, sélectionnez **Alimentation**, puis **Activer** pour démarrer la machine virtuelle.

3 Cliquez avec le bouton droit sur la machine virtuelle, sélectionnez **Invité**, puis **Installer/Mettre à niveau VMware Tools** pour installer la dernière version de VMware Tools.

   **Remarque** La fonction d'impression virtuelle n'est prise en charge que lorsque vous l'installez à partir d'Horizon Agent. Elle n'est pas prise en charge si vous l'installez avec VMware Tools.

4 Utilisez la fonction de synchronisation de l'heure de VMware Tools pour vous assurer que la machine virtuelle est synchronisée avec ESXi.

   ESXi doit se synchroniser avec une source NTP externe, par exemple, la même source d'heure qu'Active Directory.

Désactivez les autres mécanismes de synchronisation de l'heure, tels que Service de temps Windows.

L'aide en ligne de VMware Tools fournit des informations sur la configuration de la synchronisation de l'heure entre client et hôte.

5 Installez les packs de service et les mises à jour.

6 Installez un logiciel antivirus.

7 Installez d'autres applications et logiciels, tels que les pilotes de carte à puce, si vous utilisez l'authentification par carte à puce.

Si vous prévoyez d'utiliser VMware Identity Manager pour offrir un catalogue qui inclut des applications ThinApp, vous devez installer VMware Identity Manager pour Windows.

---

**Important** Si vous installez Microsoft .NET Framework, vous devez l'installer après Horizon Agent.

---

8 Si des périphériques Horizon Client se connectent à la machine virtuelle avec le protocole d'affichage PCoIP, définissez l'option d'alimentation **Éteindre l'écran** sur **Jamais**.

Si vous ne désactivez pas ce paramètre, l'écran semblera se figer dans son dernier état lorsque le mode d'économie d'énergie démarrera.

9 Si des périphériques Horizon Client se connectent à la machine virtuelle avec le protocole d'affichage PCoIP, accédez à **Panneau de configuration > Système > Paramètres système avancés > Paramètres de performances** et modifiez le paramètre **Effets visuels** sur **Ajuster afin d'obtenir les meilleures performances**.

Si vous utilisez plutôt le paramètre **Ajuster afin d'obtenir la meilleure apparence** ou **Laisser Windows choisir la meilleure configuration** et si Windows choisit l'apparence au lieu de la performance, la performance est affectée négativement.

10 Si un serveur proxy est utilisé dans votre environnement de réseau, configurez les paramètres du proxy réseau.

11 Configurez des propriétés de connexion réseau.

   a Affectez une adresse IP statique ou spécifiez qu'une adresse IP est affectée par un serveur DHCP.

   View ne prend pas en charge les adresses locales du lien (169.254.x.x) pour les postes de travail View.

   b Définissez les adresses de serveurs DNS préférentiels et alternatifs sur votre adresse de serveur Active Directory.

12 (Facultatif) Joignez la machine virtuelle au domaine Active Directory de vos postes de travail distants.

Une machine virtuelle parente pour créer des clones instantanés ou des clones liés View Composer doit appartenir au même domaine Active Directory que celui que rejoindront les machines de poste de travail ou être un membre d'un groupe de travail.

13 Configurez le pare-feu Windows pour autoriser des connexions Bureau à distance à la machine virtuelle.

14 (Facultatif) Désactivez les périphériques PCI enfichables à chaud.

Cette étape évite aux utilisateurs de déconnecter accidentellement le périphérique de réseau virtuel (vNIC) de la machine virtuelle.

15 (Facultatif) Configurez des scripts de personnalisation d'utilisateur.

## Préparer les systèmes d'exploitation Windows Server à une utilisation comme poste de travail

Pour utiliser une machine virtuelle Windows Server 2008 R2 ou Windows Server 2012 R2 en tant que poste de travail View à session unique (plutôt que comme hôte RDS), vous devez effectuer certaines étapes avant d'installer Horizon Agent sur la machine virtuelle. Vous devez également configurer View Administrator pour qu'il reconnaisse Windows Server comme un système d'exploitation pris en charge pour utiliser le poste de travail View.

### Prérequis

- Familiarisez-vous avec les étapes d'installation de la fonctionnalité Expérience de poste de travail sur Windows Server 2008 R2 ou Windows Server 2012 R2. Reportez-vous à « Installer la fonctionnalité Expérience utilisateur sur Windows Server 2008 R2 », page 32 ou à « Installer la fonctionnalité Expérience utilisateur sur Windows Server 2012 ou 2012 R2 », page 32
- Sur les machines Windows Server 2012 R2, familiarisez-vous avec les étapes de configuration du service Pare-feu Windows pour redémarrer après des pannes. Reportez-vous à la section « Configurer le service Pare-feu Windows pour redémarrer après les pannes », page 33.

### Procédure

1. Vérifiez que le rôle Services Bureau à distance n'est pas installé.

   Lorsque le rôle Services Bureau à distance n'est pas présent, le programme d'installation d' Horizon Agent vous invite à confirmer que vous souhaitez installer Horizon Agent en mode de poste de travail. Si le rôle Services Bureau à distance est présent, le programme d'installation d'Horizon Agent n'affiche pas cette invite et considère la machine Windows Server en tant qu'hôte RDS et non en tant que poste de travail View à session unique.

2. Installez Windows Server 2008 R2 Service Pack 1 (SP1) ou Windows Server 2012 R2.

   Si vous n'installez pas la version SP1 avec Windows Server 2008 R2, une erreur se produit lors de l'installation d'Horizon Agent.

3. (Facultatif) Installez la fonctionnalité Expérience de poste de travail si vous prévoyez d'utiliser les fonctionnalités suivantes.

   - HTML Access
   - Redirection de scanner
   - Windows Aero

4. (Facultatif) Pour utiliser Windows Aero sur un poste de travail Windows Server, démarrez le service Thèmes.

   Lorsque vous créez ou modifiez un pool de postes de travail, vous pouvez configurer le rendu graphique 3D pour vos postes de travail. Le paramètre Convertisseur 3D offre une option logicielle qui permet aux utilisateurs d'exécuter Windows Aero sur les postes de travail du pool.

5. Sur les machines Windows Server 2012 R2, configurez le service Pare-feu Windows pour redémarrer après des pannes.

6 Configurez View Administrator afin qu'il considère Windows Server comme un système d'exploitation de poste de travail pris en charge.

   Si vous n'exécutez pas cette étape, vous ne pourrez pas sélectionner les machines Windows Server à utiliser comme postes de travail dans View Administrator.

   a Dans View Administrator, sélectionnez **Configuration de View > Paramètres généraux**.

   b Dans le volet Général, cliquez sur **Modifier**.

   c Cochez la case **Activer les postes de travail Windows** et cliquez sur **OK**.

Lorsque vous activez des postes de travail Windows Server dans View Administrator, celui-ci affiche toutes les machines Windows Server disponibles, notamment celles sur lesquelles le Serveur de connexion View est installé, en tant que machines potentielles à utiliser comme postes de travail. Vous ne pouvez pas installer Horizon Agent sur des machines sur lesquelles d'autres composants logiciels de View sont installés.

## Installer la fonctionnalité Expérience utilisateur sur Windows Server 2008 R2

Pour les postes de travail et applications RDS, et pour les postes de travail VDI déployés sur des machines virtuelles mono-utilisateur s'exécutant sous Windows Server, la redirection de scanner requiert l'installation de la fonctionnalité Expérience de poste de travail sur les hôtes RDS et les machines virtuelles mono-utilisateur.

### Procédure

1 Connectez-vous en tant qu'administrateur.

2 Démarrez le gestionnaire de serveurs.

3 Cliquez sur **Fonctionnalités**.

4 Cliquez sur **Ajouter des fonctionnalités**.

5 Sur la page Sélectionner les fonctionnalités, cochez la case **Expérience de poste de travail**.

6 Examinez les informations relatives aux autres fonctionnalités requises par la fonctionnalité Expérience de poste de travail, puis cliquez sur **Ajouter les fonctionnalités requises**.

7 Suivez les invites et terminez l'installation.

## Installer la fonctionnalité Expérience utilisateur sur Windows Server 2012 ou 2012 R2

Pour les postes de travail et applications RDS, et pour les postes de travail VDI déployés sur des machines virtuelles mono-utilisateur s'exécutant sous Windows Server, la redirection de scanner requiert l'installation de la fonctionnalité Expérience de poste de travail sur les hôtes RDS et les machines virtuelles mono-utilisateur.

Windows Server 2012 et Windows Server 2012 R2 sont pris en charge sur les machines utilisées comme hôtes RDS. Windows Server 2012 R2 est pris en charge sur des machines mono-utilisateur :

### Procédure

1 Connectez-vous en tant qu'administrateur.

2 Démarrez le gestionnaire de serveurs.

3 Sélectionnez **Ajouter des rôles et des fonctionnalités**.

4 Sur la page Sélectionner un type d'installation, sélectionnez **Installation basée sur des rôles ou des fonctionnalités**.

5 Sur la page Sélectionner le serveur de destination, sélectionnez un serveur.

6 Sur la page Sélectionner des rôles de serveur, acceptez la sélection par défaut, puis cliquez sur **Suivant**.

7 Sur la page Sélectionner les fonctionnalités, sous **Interfaces utilisateur et infrastructure**, sélectionnez **Expérience de poste de travail**.

8 Suivez les invites et terminez l'installation.

## Configurer le service Pare-feu Windows pour redémarrer après les pannes

Certaines machines Windows Server 2012 R2, Windows 8.1 et Windows 10 qui sont déployées comme postes de travail à session unique ne deviennent pas immédiatement disponibles après leur provisionnement. Ce problème se produit lorsque le service Pare-feu Windows ne redémarre pas après l'expiration de son délai d'attente. Vous pouvez configurer le service Pare-feu Windows sur la machine virtuelle parente ou le modèle de machine virtuelle pour garantir que toutes les machines d'un pool de postes de travail deviennent disponibles.

Si vous rencontrez ce problème lors du provisionnement, les journaux d'événements Windows affichent l'erreur suivante : `Le service Pare-feu Windows s'est arrêté avec l'erreur spécifique au service suivante : Cette opération s'est terminée, car le délai d'attente a expiré.`

Ce problème se produit sur les machines Windows Server 2012 R2, Windows 8.1 et Windows 10. Les autres systèmes d'exploitation invités ne sont pas concernés.

### Procédure

1 Sur le modèle de machine virtuelle ou la machine virtuelle parente Windows Server 2012 R2, Windows 8.1 ou Windows 10 à partir de laquelle vous allez déployer un pool de postes de travail, sélectionnez **Panneau de configuration > Outils d'administration > Services**.

2 Dans la boîte de dialogue Services, cliquez avec le bouton droit sur le service **Pare-feu Windows** et sélectionnez **Propriétés**.

3 Dans la boîte de dialogue Propriétés du pare-feu Windows, cliquez sur l'onglet **Récupération**.

4 Sélectionnez les paramètres de récupération pour redémarrer le service après une panne.

| Paramètre | Option du menu déroulant |
|---|---|
| **Première panne :** | **Redémarrer le service** |
| **Deuxième panne :** | **Redémarrer le service** |
| **Pannes suivantes :** | **Redémarrer le service** |

5 Cochez la case **Activer les actions pour les arrêts avec erreurs** et cliquez sur **OK**.

6 Déployez ou redéployez le pool de postes de travail à partir de la machine virtuelle parente ou du modèle de machine virtuelle.

# Installer Horizon Agent sur une machine virtuelle

Vous devez installer Horizon Agent sur des machines virtuelles gérées par vCenter Server pour que le Serveur de connexion puisse communiquer avec elles. Installez Horizon Agent sur toutes les machines virtuelles que vous utilisez comme modèles pour des pools de postes de travail de clone complet, comme parentes pour des pools de postes de travail de clone lié, comme parentes pour des pools de postes de travail de clone instantané et comme machines dans des pools de postes de travail manuels.

Pour installer Horizon Agent sur plusieurs machines virtuelles Windows sans avoir à répondre à des invites d'assistant, vous pouvez installer Horizon Agent de manière silencieuse. Reportez-vous à la section « Installer Horizon Agent en silence », page 37.

Le logiciel Horizon Agent ne peut pas coexister sur la même machine virtuelle ou physique avec un autre composant logiciel d'Horizon, notamment un serveur de sécurité, le Serveur de connexion, View Composer ou Horizon Client.

### Prérequis

- Préparez le système d'exploitation invité pour le déploiement de postes de travail distants. Reportez-vous à la section « Préparer un système d'exploitation invité pour le déploiement de postes de travail distants », page 29.
- Pour utiliser une machine virtuelle Windows Server en tant que poste de travail distant (et non en tant qu'hôte RDS), procédez comme décrit dans « Préparer les systèmes d'exploitation Windows Server à une utilisation comme poste de travail », page 31.
- Si le module Microsoft Visual C++ Redistributable est installé sur la machine, vérifiez que la version du module est 2005 SP1 ou version ultérieure. Si la version du module est 2005 ou antérieure, vous pouvez effectuer la mise à niveau ou désinstaller le module.
- Téléchargez le fichier du programme d'installation d'Horizon Agent sur la page des produits VMware, à l'adresse http://www.vmware.com/go/downloadview.
- Vérifiez que vous disposez des droits d'administration sur la machine virtuelle.
- Familiarisez-vous avec les options de configuration personnalisée d'Horizon Agent. Reportez-vous à la section « Options d'installation personnalisée d'Horizon Agent », page 35.
- Familiarisez-vous avec les ports TCP que le programme d'installation d'Horizon Agent ouvre sur le pare-feu. Pour plus d'informations, reportez-vous au document *Planification de l'architecture de View*.

### Procédure

1. Pour démarrer le programme d'installation d'Horizon Agent, double-cliquez sur le fichier du programme d'installation.

   Le nom de fichier du programme d'installation est `VMware-viewagent-y.y.y-xxxxxx.exe` ou `VMware-viewagent-x86_64-y.y.y-xxxxxx.exe`, où *y.y.y* est le numéro de version et *xxxxxx* le numéro de build.

2. Acceptez les termes de licence VMware.
3. Si vous installez Horizon Agent sur une machine Windows Server sur laquelle le rôle Services Bureau à distance (RDS) n'est pas installé, sélectionnez **Installer VMware Horizon Agent en « mode Poste de travail »**.

   Cette option configure la machine Windows Server comme poste de travail View mono-utilisateur plutôt qu'en hôte RDS. Si vous souhaitez que la machine fonctionne comme un hôte RDS, annulez l'installation d'Horizon Agent, installez le rôle RDS sur la machine, puis redémarrez l'installation d'Horizon Agent.

4. Sélectionnez la version du protocole Internet (**IPv4** ou **IPv6**).

   Vous devez installer tous les composants View avec la même version IP.

5. Sélectionnez si le mode FIPS doit être activé ou désactivé.

   Cette option n'est disponible que si le mode FIPS est activé dans Windows.

6. Sélectionnez les options d'installation personnalisée désirées.

   Pour déployer des postes de travail de clone lié View Composer, sélectionnez l'option **VMware Horizon View Composer Agent**. Pour déployer des postes de travail de clone instantané, sélectionnez l'option **VMware Horizon Instant Clone Agent**. Vous ne pouvez pas sélectionner ces deux options.

7. Acceptez ou modifiez le dossier de destination.

8 Suivez les invites dans le programme d'installation d'Horizon Agent et terminez l'installation.

**Remarque** Si vous n'avez pas activé la prise en charge du Bureau à distance au cours de la préparation du système d'exploitation client, le programme d'installation d'Horizon Agent vous invite à l'activer. Si vous n'activez pas la prise en charge du Bureau à distance au cours de l'installation d'Horizon Agent, vous devez l'activer manuellement une fois l'installation terminée.

9 Si vous avez sélectionné l'option de redirection USB, redémarrez la machine virtuelle pour activer la prise en charge USB.

De plus, l'assistant **Nouveau matériel détecté** doit démarrer. Suivez les invites dans l'assistant pour configurer le matériel avant de redémarrer la machine virtuelle.

### Suivant

Si la machine virtuelle contient plusieurs cartes réseau, configurez le sous-réseau qu'Horizon Agent utilise. Reportez-vous à la section « Configurer une machine virtuelle avec plusieurs cartes réseau pour Horizon Agent », page 44.

## Options d'installation personnalisée d'Horizon Agent

Lorsque vous installez Horizon Agent sur une machine virtuelle, vous pouvez sélectionner ou désélectionner des options d'installation personnalisée. En outre, Horizon Agent installe automatiquement certaines fonctionnalités sur tous les systèmes d'exploitation invités sur lesquels elles sont prises en charge. Ces fonctionnalités ne sont pas facultatives.

Pour découvrir les fonctionnalités prises en charge par les différents systèmes d'exploitation invités, consultez la section « Matrice de prise en charge des fonctionnalités pour Horizon Agent » dans le document *Planification de l'architecture de View*.

Pour modifier des options d'installation personnalisée après avoir installé la dernière version d'Horizon Agent, vous devez désinstaller et réinstaller Horizon Agent. Pour les correctifs et les mises à niveau, vous pouvez exécuter le nouveau programme d'installation d'Horizon Agent et sélectionner un nouvel ensemble d'options sans désinstaller la version précédente.

Toutes les options d'installation personnalisée sont sélectionnées par défaut, sauf Redirection de port série, Redirection de scanner, Redirection USB, Redirection Flash, Redirection de carte à puce et VMware Horizon Instant Clone Agent.

**Tableau 3-2.** Options d'installation personnalisée d'Horizon Agent dans un environnement IPv4

| Option | Description |
|---|---|
| Core | Installe la fonctionnalité Core. |
| Redirection de port série | Permet de rediriger les ports COM série connectés au système client pour qu'ils puissent être utilisés sur le poste de travail distant.<br>Cette option n'est pas sélectionnée par défaut. Vous devez sélectionner l'option pour l'installer.<br>La fonctionnalité Redirection de port série est prise en charge sur les postes de travail distants qui sont déployés sur des machines mono-utilisateur.<br>La redirection de port série est disponible dans Horizon 6 version 6.1.1 et versions ultérieures. |
| Redirection de scanner | Permet de rediriger les périphériques graphiques et d'analyse connectés au système client pour qu'ils puissent être utilisés sur l'application ou le poste de travail distant.<br>Cette option n'est pas sélectionnée par défaut. Vous devez sélectionner l'option pour l'installer.<br>La redirection de scanner est disponible dans Horizon 6.0.2 et versions ultérieures. |

**Tableau 3-2.** Options d'installation personnalisée d'Horizon Agent dans un environnement IPv4 (suite)

| Option | Description |
|---|---|
| Redirection USB | Donne aux utilisateurs un accès à des périphériques USB connectés en local sur leurs postes de travail.<br>La fonctionnalité Redirection USB est prise en charge sur les postes de travail distants qui sont déployés sur des machines mono-utilisateur. En outre, la redirection de lecteurs flash et de disques durs USB est prise en charge sur les postes de travail et applications RDS.<br>Cette option n'est pas sélectionnée par défaut. Vous devez sélectionner l'option pour l'installer.<br>Pour obtenir des instructions sur l'utilisation de la redirection USB en toute sécurité, reportez-vous au guide *Sécurité de View*. Par exemple, vous pouvez utiliser les paramètres de stratégie de groupe pour désactiver une redirection USB pour des utilisateurs spécifiques. |
| VMware Horizon View Composer Agent | Permet à cette machine virtuelle d'être la machine virtuelle parente d'un pool de postes de travail de clone lié View Composer. Si vous sélectionnez cette option, vous ne pouvez pas sélectionner l'option **VMware Horizon Instant Clone Agent**. |
| VMware Horizon Instant Clone Agent | Permet à cette machine virtuelle d'être la machine virtuelle parente d'un pool de postes de travail de clone instantané. Cette option n'est pas sélectionnée par défaut. Si vous sélectionnez cette option, vous ne pouvez pas sélectionner l'option **VMware Horizon View Composer Agent**. |
| Audio/Vidéo en temps réel | Permet de rediriger la webcam et les périphériques audio connectés au système client pour qu'ils puissent être utilisés sur le poste de travail distant. |
| Redirection de lecteur client | Permet aux utilisateurs d'Horizon Client de partager des lecteurs locaux avec leurs postes de travail distants.<br>Une fois cette option installée, aucune autre configuration n'est requise sur le poste de travail distant.<br>La redirection de lecteur client est également prise en charge sur les postes de travail et les applications RDS et sur les postes de travail VDI exécutés sur des machines non gérées. |
| Impression virtuelle | Permet aux utilisateurs d'imprimer sur n'importe quelle imprimante disponible sur leurs ordinateurs clients. Les utilisateurs n'ont pas à installer des pilotes supplémentaires sur leurs postes de travail.<br>Dans Horizon 6.0.1 et version ultérieure, l'impression virtuelle est prise en charge sur les applications et les postes de travail distants suivants :<br>■ Postes de travail qui sont déployés sur des machines mono-utilisateur, notamment les machines postes de travail Windows et Windows Server<br>■ Postes de travail qui sont déployées sur des hôtes RDS, où les hôtes RDS sont des machines virtuelles<br>■ applications hébergées ;<br>■ Applications hébergées qui sont lancées à partir d'Horizon Client à l'intérieur de postes de travail distants<br>Dans Horizon 6.0 et version antérieure, l'impression virtuelle est prise en charge sur les postes de travail qui sont déployés sur des machines de poste de travail mono-utilisateur.<br>La fonction d'impression virtuelle n'est prise en charge que lorsque vous l'installez à partir d'Horizon Agent. Elle n'est pas prise en charge si vous l'installez avec VMware Tools. |
| vRealize Operations Desktop Agent | Fournit des informations qui permettent à vRealize Operations pour View de surveiller des postes de travail View. |
| View Persona Management | Synchronise le profil d'utilisateur sur le poste de travail local avec un référentiel de profils distant, pour que les utilisateurs puissent accéder à leurs profils dès qu'ils ouvrent une session sur un poste de travail. |
| Redirection de carte à puce | Permet aux utilisateurs de s'authentifier avec des cartes à puce lorsqu'ils utilisent le protocole d'affichage PCoIP ou Blast Extreme. Cette option n'est pas sélectionnée par défaut.<br>La redirection de carte à puce est prise en charge sur les postes de travail distants qui sont déployés sur des machines mono-utilisateur. |

**Tableau 3-2.** Options d'installation personnalisée d'Horizon Agent dans un environnement IPv4 (suite)

| Option | Description |
|---|---|
| VMware Audio | Fournit un pilote audio virtuel sur le poste de travail distant. |
| Redirection Flash (expérimental) | Redirige le contenu multimédia Flash dans un navigateur Internet Explorer 9, 10 ou 11 vers le client, pour l'optimisation des performances. Il s'agit d'une fonctionnalité de la version d'évaluation technique.<br>Cette option n'est pas sélectionnée par défaut. Vous devez sélectionner l'option pour l'installer.<br>La redirection Flash est disponible dans Horizon 7.0 et versions ultérieures. |

Dans un environnement IPv6, les seules fonctionnalités facultatives sont VMware Horizon View Composer Agent, VMware Horizon Instant Clone Agent et VMware Audio.

**Tableau 3-3.** Fonctionnalités d'Horizon Agent qui sont installées automatiquement (non facultatives)

| Fonction | Description |
|---|---|
| PCoIP Agent | Permet aux utilisateurs de se connecter au poste de travail View à l'aide du protocole d'affichage PCoIP.<br>L'installation de la fonctionnalité PCoIP Agent désactive le mode Veille sur les postes de travail Windows. Lorsqu'un utilisateur va dans le menu Power Options (Options d'alimentation) ou Shut Down (Arrêter), le mode veille est inactif. Les postes de travail ne passent pas en mode veille après une période par défaut d'inactivité. Les postes de travail restent en mode actif. |
| Redirection multimédia Windows Media (MMR) | Permet d'étendre la redirection multimédia pour les postes de travail et les clients Windows 7 et les versions ultérieures. Cette fonctionnalité délivre le flux multimédia directement aux ordinateurs client, permettant au flux multimédia d'être traité sur le matériel client plutôt que sur l'hôte ESXi distant. |
| Unity Touch | Permet aux utilisateurs de tablette et de smartphone d'entrer facilement en interaction avec les applications Windows qui s'exécutent sur le poste de travail distant. Les utilisateurs peuvent parcourir, rechercher et ouvrir des applications et des fichiers Windows, choisir des applications et des fichiers favoris, et basculer entre les applications en cours d'exécution, le tout sans utiliser le menu Démarrer ni la barre des tâches. |
| Pilote vidéo virtuel | Fournit un pilote vidéo virtuel sur le poste de travail distant. |

Dans un environnement IPv6, PCoIP Agent est la seule fonctionnalité automatiquement installée.

## Installer Horizon Agent en silence

Vous pouvez utiliser la fonction d'installation silencieuse de MSI (Microsoft Windows Installer) pour installer Horizon Agent sur plusieurs machines virtuelles ou ordinateurs physiques Windows. Dans une installation silencieuse, vous utilisez la ligne de commande et n'avez pas à répondre à des invites d'assistant.

L'installation silencieuse vous permet de déployer efficacement des composants View dans une entreprise de grande taille.

Si vous ne souhaitez pas installer toutes les fonctionnalités installées automatiquement ou par défaut, vous pouvez utiliser la propriété MSI `ADDLOCAL` pour sélectionner des fonctionnalités et des options de configuration individuelles à installer. Pour plus d'informations sur la propriété `ADDLOCAL`, reportez-vous à Tableau 3-5.

### Prérequis

- Préparez le système d'exploitation invité au déploiement du poste de travail. Reportez-vous à la section « Préparer un système d'exploitation invité pour le déploiement de postes de travail distants », page 29.
- Pour utiliser Windows Server en tant que poste de travail distant à session unique (et non en tant qu'hôte RDS), procédez comme décrit dans « Préparer les systèmes d'exploitation Windows Server à une utilisation comme poste de travail », page 31.
- Si le module Microsoft Visual C++ Redistributable est installé sur la machine, vérifiez que la version du module est 2005 SP1 ou version ultérieure. Si la version du module est 2005 ou antérieure, vous pouvez effectuer la mise à niveau ou désinstaller le module.
- Téléchargez le fichier du programme d'installation d'Horizon Agent sur la page des produits VMware, à l'adresse http://www.vmware.com/go/downloadview.

  Le nom de fichier du programme d'installation est `VMware-viewagent-y.y.y-xxxxxx.exe` ou `VMware-viewagent-x86_64-y.y.y-xxxxxx.exe`, où *y.y.y* est le numéro de version et *xxxxxx* le numéro de build.
- Vérifiez que vous disposez de droits d'administration sur la machine virtuelle ou l'ordinateur physique.
- Familiarisez-vous avec les options de configuration personnalisée d'Horizon Agent. Reportez-vous à la section « Options d'installation personnalisée d'Horizon Agent », page 35.
- Familiarisez-vous avec les options de ligne de commande du programme d'installation MSI. Reportez-vous à la section « Options de la ligne de commande Microsoft Windows Installer », page 39.
- Familiarisez-vous avec les propriétés d'installation silencieuse disponibles avec Horizon Agent. Reportez-vous à la section « Propriétés de l'installation silencieuse pour Horizon Agent », page 41.
- Familiarisez-vous avec les ports TCP que le programme d'installation d'Horizon Agent ouvre sur le pare-feu. Pour plus d'informations, reportez-vous au document *Planification de l'architecture de View*.
- Vérifiez que les correctifs les plus récents de Windows Update sont installés sur les systèmes d'exploitation invités sur lesquels vous prévoyez d'installer Horizon Agent de manière silencieuse. Dans certains cas, une installation interactive effectuée par un administrateur peut être nécessaire pour exécuter les correctifs en attente de Windows Update. Vérifiez que toutes les opérations du système d'exploitation et tous les redémarrages successifs sont terminés.

### Procédure

1. Ouvrez une invite de commande Windows sur la machine virtuelle ou l'ordinateur physique.
2. Saisissez la commande d'installation sur une ligne.

   L'exemple suivant installe Horizon Agent dans une machine virtuelle gérée par vCenter Server. De plus, le programme d'installation installe les composants VMware Blast, PCoIP, View Composer Agent, Impression virtuelle, Redirection USB et Audio/Vidéo en temps réel.

   ```
   VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=1
   ADDLOCAL=Core,BlastProtocol,PCoIP,SVIAgent,ThinPrint,USB,RTAV"
   ```

   L'exemple suivant installe Horizon Agent sur un ordinateur non géré et inscrit le poste de travail avec le Serveur de connexion View spécifié, `cs1.companydomain.com`. De plus, le programme d'installation installe les composants VMware Blast, PCoIP, Impression virtuelle et Redirection USB.

   ```
   VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=0
   VDM_SERVER_NAME=cs1.companydomain.com VDM_SERVER_USERNAME=admin.companydomain.com
   VDM_SERVER_PASSWORD=secret ADDLOCAL=Core,BlastProtocol,PCoIP,ThinPrint,USB"
   ```

   Si vous installez Horizon Agent sur une machine Windows Server et que vous avez l'intention de configurer la machine en tant que poste de travail View mono-utilisateur plutôt qu'en tant qu'hôte RDS, vous devez inclure la propriété `VDM_FORCE_DESKTOP_AGENT=1` dans la commande d'installation. Cette condition s'applique aux machines gérées par vCenter Server, ainsi qu'aux machines non gérées.

**Suivant**

Si la machine virtuelle contient plusieurs cartes réseau, configurez le sous-réseau qu'Horizon Agent utilise. Reportez-vous à la section « Configurer une machine virtuelle avec plusieurs cartes réseau pour Horizon Agent », page 44.

## Options de la ligne de commande Microsoft Windows Installer

Pour installer des composants View en silence, vous devez utiliser des options et des propriétés de ligne de commande de MSI (Microsoft Windows Installer). Les programmes d'installation des composants View sont des programmes MSI et utilisent des fonctions MSI standard.

Pour plus d'informations sur MSI, rendez-vous sur le site Web de Microsoft. Pour plus d'informations sur les options de la ligne de commande MSI, rendez-vous sur le site Web de la bibliothèque MSDN (Microsoft Developer Network). Pour voir comment utiliser la ligne de commande MSI, vous pouvez ouvrir une invite de commande sur l'ordinateur de composant View et saisir `msiexec /?`.

Pour exécuter un programme d'installation de composant View en mode silencieux, commencez par activer le mode silencieux sur le programme de démarrage qui extrait le programme d'installation dans un répertoire temporaire et démarre une installation interactive.

Vous devez entrer sur la ligne de commande les options qui contrôlent le programme de démarrage du programme d'installation.

**Tableau 3-4.** Options de ligne de commande du programme de démarrage d'un composant View

| Option | Description |
|---|---|
| `/s` | Désactive l'écran de démarrage et la boîte de dialogue d'extraction du programme de démarrage, qui empêche l'affichage de boîtes de dialogue interactives.<br>Par exemple : `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s`<br>L'option `/s` est obligatoire pour que l'installation soit silencieuse. |
| `/v"MSI_command_line_options"` | Demande au programme d'installation de transmettre à MSI la chaîne de caractères comprise entre guillemets, que vous avez entrée sur la ligne de commande comme un ensemble d'options à interpréter. Vous devez délimiter votre chaîne de caractères de la ligne de commande par des guillemets. Placez un guillemet après `/v` et à la fin de la ligne de commande.<br>Par exemple : `VMware-viewagent-y.y.y-xxxxxx.exe /s /v"command_line_options"`<br>Pour demander au programme d'installation MSI d'interpréter une chaîne contenant des espaces, insérez deux jeux de guillemets doubles avant et après la chaîne. Par exemple, vous voulez peut-être installer le composant View dans un nom de chemin d'installation contenant des espaces.<br>Par exemple : `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"command_line_options INSTALLDIR=""d:\abc\my folder"""`<br>Dans cet exemple, le programme d'installation MSI transmet le chemin du répertoire d'installation et n'essaie pas d'interpréter la chaîne comme deux options de ligne de commande. Notez le guillemet double final entourant toute la ligne de commande.<br>L'option `/v"command_line_options"` est obligatoire pour exécuter une installation silencieuse. |

Le contrôle de la suite de l'installation silencieuse se fait en transmettant les options de la ligne de commande et les valeurs de propriété MSI au programme d'installation MSI, `msiexec.exe`. Le programme d'installation MSI comporte le code d'installation du composant View. Le programme d'installation utilise les valeurs et les options que vous saisissez dans la ligne de commande pour interpréter des choix d'installation et des options de configuration propres au composant View.

**Tableau 3-5.** Options de la ligne de commande et propriétés MSI

| Option ou propriété MSI | Description |
|---|---|
| `/qn` | Demande au programme d'installation MSI de ne pas afficher les pages de l'assistant d'installation.<br>Par exemple, vous voulez peut-être installer Horizon Agent en silence et n'utiliser que des options et des fonctionnalités d'installation par défaut :<br>`VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn"`<br>Vous pouvez également utiliser l'option `/qb` pour afficher les pages de l'assistant d'installation dans une installation automatique non interactive. Pendant l'installation, les pages de l'assistant d'installation sont affichées, mais vous ne pouvez pas y répondre.<br>L'option `/qn` ou `/qb` est obligatoire pour que l'installation soit silencieuse. |
| `INSTALLDIR` | Spécifie un autre chemin d'installation pour le composant View.<br>Utilisez le format *`INSTALLDIR=path`* pour spécifier un chemin d'installation. Vous pouvez ignorer cette propriété MSI si vous voulez installer le composant View dans le chemin par défaut.<br>Cette propriété MSI est facultative. |
| `ADDLOCAL` | Détermine les options spécifiques du composant à installer.<br>Dans une installation interactive, le programme d'installation de View affiche des options d'installation personnalisée que vous pouvez cocher ou décocher. Dans une installation silencieuse, vous pouvez utiliser la propriété `ADDLOCAL` pour installer sélectivement des options de configuration en spécifiant les options sur la ligne de commande. Les options que vous ne spécifiez pas explicitement ne sont pas installées.<br>Dans les installations interactives et silencieuses, le programme d'installation de View installe automatiquement certaines fonctionnalités. Vous ne pouvez pas utiliser `ADDLOCAL` pour choisir d'installer ou non ces fonctionnalités non facultatives.<br>Tapez `ADDLOCAL=ALL` pour installer toutes les options de configuration personnalisées pouvant être installées au cours d'une installation interactive, notamment celles installées par défaut et celles que vous devez sélectionner, sauf NGVC. NGVC et SVIAgent s'excluent mutuellement. Pour installer NGVC, vous devez le spécifier explicitement.<br>L'exemple suivant installe Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG et toutes les fonctionnalités prises en charge sur le système d'exploitation invité : `VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=ALL"`<br>Si vous n'utilisez pas la propriété `ADDLOCAL`, les options d'installation personnalisée qui sont installées par défaut et les fonctions installées automatiquement sont installées. Les options d'installation personnalisée qui sont désactivées (non sélectionnées) par défaut ne sont pas installées.<br>L'exemple suivant installe Core, BlastProtocol, PCoIP, UnityTouch, VmVideo, PSG et les options d'installation personnalisée activées par défaut qui sont prises en charge sur le système d'exploitation invité : `VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn"`<br>Pour spécifier des options d'installation individuelles, tapez une liste séparée par des virgules de noms d'option d'installation. Ne laissez pas d'espaces entre les noms. Utilisez le format `ADDLOCAL=value,value,value....`<br>Vous devez inclure `Core` lorsque vous utilisez la propriété `ADDLOCAL=value,value,value....`<br>L'exemple suivant installe Horizon Agent avec les fonctionnalités Core, BlastProtocol, PCoIP, UnityTouch, Instant Clone Agent et Impression virtuelle :<br>`VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,BlastProtocol,PCoIP,UnityTouch,NGVC,ThinPrint"`<br>L'exemple précédent n'installe pas d'autres composants, même ceux qui sont installés par défaut de façon interactive.<br>La propriété MSI `ADDLOCAL` est facultative. |

**Tableau 3-5.** Options de la ligne de commande et propriétés MSI (suite)

| Option ou propriété MSI | Description |
|---|---|
| `REBOOT` | Vous pouvez utiliser l'option `REBOOT=ReallySuppress` pour autoriser l'exécution de tâches de configuration système avant le redémarrage du système.<br>Cette propriété MSI est facultative. |
| `/l*v` *`log_file`* | Écrit des informations de journalisation dans le fichier journal spécifié avec une sortie détaillée.<br>Par exemple : `/l*v ""%TEMP%\vmmsi.log""`<br>Cet exemple génère un fichier journal détaillé semblable à celui généré lors d'une installation interactive.<br>Vous pouvez utiliser cette option pour enregistrer des fonctions personnalisées qui s'appliquent uniquement à votre installation. Vous pouvez utiliser les informations enregistrées pour spécifier les fonctionnalités d'installation lors d'installations silencieuses ultérieures.<br>L'option `/l*v` est facultative. |

## Propriétés de l'installation silencieuse pour Horizon Agent

Vous pouvez inclure des propriétés spécifiques lorsque vous installez de façon silencieuse Horizon Agent via la ligne de commande. Vous devez utiliser le format *`PROPERTY=value`* de manière que Microsoft Windows Installer (MSI) puisse interpréter les propriétés et les valeurs.

Tableau 3-6 montre les propriétés de l'installation silencieuse d'Horizon Agent que vous pouvez utiliser dans la ligne de commande.

**Tableau 3-6.** Propriétés MSI pour l'installation silencieuse d' Horizon Agent

| Propriété MSI | Description | Valeur par défaut |
|---|---|---|
| `INSTALLDIR` | Chemin d'accès et dossier dans lequel le logiciel Horizon Agent est installé.<br>Par exemple : `INSTALLDIR=""D:\abc\my folder""`<br>Les jeux de deux guillemets doubles entourant le chemin autorisent le programme d'installation MSI à ignorer l'espace dans le chemin.<br>Cette propriété MSI est facultative. | `%ProgramFiles%\VMware\VMware View\Agent` |
| `RDP_CHOICE` | Détermine l'activation du protocole RDP (Remote Desktop Protocol) sur le poste de travail.<br>Une valeur de 1 active RDP. Une valeur de 0 laisse le paramètre RDP désactivé.<br>Cette propriété MSI est facultative. | 1 |
| `UNITY_DEFAULT_APPS` | Indique une liste d'applications préférées par défaut qui sont affichées dans la barre latérale d'Unity Touch sur un appareil portable. Cette propriété a été créée pour prendre en charge le composant Unity Touch. Il ne s'agit pas d'une propriété MSI générale.<br>Pour plus d'informations sur la configuration d'une liste d'applications préférées par défaut et sur la syntaxe et le format utilisés avec cette propriété, reportez-vous à « Configurer les applications préférées affichées par Unity Touch », page 194.<br>Cette propriété MSI est facultative. | |
| `URL_FILTERING_ENABLED` | Spécifie si la fonctionnalité de redirection de contenu URL est installée. La fonctionnalité sera installée si la valeur est égale à 1. Vous devez ensuite utiliser les paramètres de stratégie de groupe pour configurer quelles URL doivent être redirigées. Reportez-vous à la section « Configuration de la redirection de contenu URL », page 206.<br>Cette propriété MSI est facultative. | 0 |

**Tableau 3-6.** Propriétés MSI pour l'installation silencieuse d' Horizon Agent (suite)

| Propriété MSI | Description | Valeur par défaut |
|---|---|---|
| `VDM_VC_MANAGED_AGENT` | Détermine si vCenter Server gère la machine virtuelle sur laquelle Horizon Agent est installé.<br>Une valeur de 1 configure le poste de travail en tant que machine virtuelle gérée par vCenter Server.<br>Une valeur de 0 configure le poste de travail comme étant non géré par vCenter Server.<br>Cette propriété MSI est requise. | Aucune |
| `VDM_SERVER_NAME` | Nom d'hôte ou adresse IP de l'ordinateur Serveur de connexion View sur lequel le programme d'installation d'Horizon Agent inscrit un poste de travail non géré. Cette propriété s'applique uniquement à des postes de travail non gérés.<br>Par exemple : `VDM_SERVER_NAME=10.123.01.01`<br>Cette propriété MSI est requise pour les postes de travail non gérés.<br>N'utilisez pas cette propriété MSI pour les postes de travail de machine virtuelle gérés par vCenter Server. | Aucune |
| `VDM_SERVER_USERNAME` | Nom d'utilisateur de l'administrateur sur l'ordinateur Serveur de connexion View. Cette propriété MSI s'applique uniquement à des postes de travail non gérés.<br>Par exemple : `VDM_SERVER_USERNAME=domain\username`<br>Cette propriété MSI est requise pour les postes de travail non gérés.<br>N'utilisez pas cette propriété MSI pour les postes de travail de machine virtuelle gérés par vCenter Server. | Aucune |
| `VDM_SERVER_PASSWORD` | Mot de passe d'utilisateur administrateur du Serveur de connexion View.<br>Par exemple : `VDM_SERVER_PASSWORD=secret`<br>Cette propriété MSI est requise pour les postes de travail non gérés.<br>N'utilisez pas cette propriété MSI pour les postes de travail de machine virtuelle gérés par vCenter Server. | Aucune |
| `VDM_IP_PROTOCOL_USAGE` | Spécifie la version IP qu'Horizon Agent utilise. Les valeurs possibles sont IPv4 et IPv6. | IPv4 |
| `VDM_FIPS_ENABLED` | Indiquez si le mode FIPS doit être activé ou désactivé. Une valeur de 1 active le mode FIPS. Une valeur de 0 désactive le mode FIPS. Si cette propriété est définie sur 1 et que Windows n'est pas en mode FIPS, le programme d'installation échouera. | 0 |
| `VDM_FLASH_URL_REDIRECTION` | Détermine si Horizon Agent peut installer la fonctionnalité de redirection d'URL Flash. Spécifiez 1 pour activer l'installation ou 0 pour désactiver l'installation.<br>Cette propriété MSI est facultative. | 0 |

Dans une commande d'installation silencieuse, vous pouvez utiliser la propriété MSI `ADDLOCAL=` pour spécifier des options à configurer par le programme d'installation d'Horizon Agent.

Tableau 3-7 affiche les options d'Horizon Agent que vous pouvez taper sur la ligne de commande. Ces options ont des options de configuration correspondantes que vous pouvez décocher ou cocher pendant une installation interactive. Pour plus de détails sur les options d'installation personnalisées, reportez-vous à « Options d'installation personnalisée d'Horizon Agent », page 35.

Lorsque vous n'utilisez pas la propriété `ADDLOCAL` sur la ligne de commande, Horizon Agent installe toutes les options installées par défaut lors d'une installation interactive, si elles sont prises en charge sur le système d'exploitation invité. Lorsque vous utilisez `ADDLOCAL=ALL`, Horizon Agent installe toutes les options suivantes, à la fois celles activées par défaut et celles désactivées par défaut, si elles sont prises en

charge sur le système d'exploitation invité, sauf NGVC. NGVC et SVIAgent s'excluent mutuellement. Pour installer NGVC, vous devez le spécifier explicitement. Pour plus de détails, reportez-vous à l'entrée de tableau `ADDLOCAL` dans la section « Options de la ligne de commande Microsoft Windows Installer », page 39.

**Tableau 3-7.** Options de l'installation silencieuse d' Horizon Agent et options de l'installation personnalisée interactive

| Option d'installation silencieuse | Option de l'installation personnalisée dans une installation interactive | Installée par défaut de façon interactive ou lorsque `ADDLOCAL` n'est pas utilisé |
|---|---|---|
| Core | Core | Oui |
| USB | Redirection USB | Non |
| SVIAgent | View Composer Agent | Oui |
| NGVC | Agent de clone instantané | Non |
| RTAV | Audio/Vidéo en temps réel | Oui |
| ClientDriveRedirection | Redirection de lecteur client | Oui |
| SerialPortRedirection | Redirection de port série | Non |
| ScannerRedirection | Redirection de scanner | Non |
| FlashURLRedirection | Redirection d'URL Flash<br>Cette fonctionnalité est masquée sauf si vous utilisez la propriété `VDM_FLASH_URL_REDIRECTION=1` sur la ligne de commande. | Non |
| ThinPrint | Impression virtuelle | Oui |
| V4V | vRealize Operations Desktop Agent | Oui |
| VPA | View Persona Management | Oui |
| SmartCard | Carte à puce PCoIP. Cette fonctionnalité n'est pas installée par défaut dans une installation interactive. | Non |
| VmwVaudio | VMware Audio (pilote audio virtuel) | Oui |
| TSMMR | Redirection multimédia Windows Media (MMR) | Oui |
| RDP | Cette fonctionnalité active RDP dans le registre si vous utilisez la propriété `RDP_CHOICE=1` sur la ligne de commande ou si vous sélectionnez RDP comme protocole d'affichage par défaut lorsque vous créez ou modifiez un pool de postes de travail dans View Administrator.<br>Cette fonctionnalité est masquée lors des installations interactives. | Oui |

Si vous utilisez `ADDLOCAL` pour spécifier des fonctionnalités individuellement, c'est-à-dire que vous ne spécifiez pas `ADDLOCAL=ALL`, vous devez spécifier les fonctionnalités suivantes explicitement. Vous devez toujours spécifier `Core`.

| Fonction de l'installation silencieuse | Description |
|---|---|
| Core | Fonctionnalités Core d'Horizon Agent. |
| BlastProtocol | VMware Blast |
| PCoIP | Agent du protocole PCoIP |
| VmVideo | Pilote vidéo virtuel |

| Fonction de l'installation silencieuse | Description |
|---|---|
| UnityTouch | Unity Touch |
| PSG | Cette fonctionnalité définit une entrée de registre qui indique au Serveur de connexion si Horizon Agent utilise IPv4 ou IPv6. |

Vous installez la fonctionnalité Redirection d'URL Flash en utilisant la propriété `VDM_FLASH_URL_REDIRECTION=1` dans une installation silencieuse. Cette fonctionnalité n'est pas installée pendant une installation interactive ou à l'aide de la commande `ADDLOCAL=ALL` dans une installation silencieuse.

Par exemple : `VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=1 VDM_FLASH_URL_REDIRECTION=1 ADDLOCAL=Core,BlastProtocol,PCoIP,SVIAgent,ThinPrint,USB,FlashURLRedirection,RTAV"`

# Configurer une machine virtuelle avec plusieurs cartes réseau pour Horizon Agent

Lorsque vous installez Horizon Agent sur une machine virtuelle qui possède plusieurs cartes réseau, vous devez configurer le sous-réseau qu'Horizon Agent utilise. Le sous-réseau détermine quelle adresse réseau est fournie par Horizon Agent à l'instance du Serveur de connexion pour les connexions de protocole client.

### Procédure

◆ Sur la machine virtuelle sur laquelle Horizon Agent est installée, ouvrez une invite de commande, saisissez **`regedit.exe`** et créez une entrée de registre pour configurer le sous-réseau.

Par exemple, dans un réseau IPv4 :
**`HKLM\Software\VMware, Inc.\VMware VDM\IpPrefix = n.n.n.n/m (REG_SZ)`**

Dans cet exemple, *n.n.n.n* est le sous-réseau TCP/IP et *m* est le nombre de bits dans le masque de sous-réseau.

**Remarque** Dans les versions antérieures à Horizon 6 version 6.1, ce chemin de registre était **`HKLM\Software\VMware, Inc.\VMware VDM\Node Manager\subnet = n.n.n.n/m (REG_SZ)`**. L'ancien paramètre de registre n'est pas utilisé avec View Agent 6.1 ou version ultérieure. Si vous mettez à niveau View Agent à partir d'une version antérieure à la version 6.1 ou version ultérieure, assurez-vous d'utiliser le paramètre de registre actuel.

# Optimiser les performances du système d'exploitation invité

Il existe une procédure que vous pouvez exécuter pour optimiser les performances des systèmes d'exploitation invités pour le déploiement de postes de travail distants. Toutes ces étapes sont facultatives.

Ces recommandations incluent la désactivation de l'écran de veille et la non spécification d'un temporisateur de veille. Votre entreprise peut requérir l'utilisation d'écrans de veille. Par exemple, vous pouvez avoir une règle de sécurité gérée par GPO qui verrouille un poste de travail un certain temps après le démarrage de l'écran de veille. Dans ce cas, utilisez un écran noir.

### Prérequis

- Préparez un système d'exploitation invité pour le déploiement de postes de travail distants.
- Familiarisez-vous avec la procédure de désactivation du programme d'amélioration de l'expérience utilisateur Windows. Reportez-vous à la section « Désactiver le programme d'amélioration de l'expérience utilisateur Windows », page 46.

### Procédure

- Désactivez tous les ports inutiles, tels que COM1, COM2 et LPT.
- Modifiez les propriétés d'affichage.
  - a Sélectionnez un thème de base.
  - b Choisissez une couleur d'arrière-plan unie.
  - c Réglez l'écran de veille sur **Aucun**.
  - d Vérifiez que l'accélération matérielle est activée.
- Sélectionnez une option d'alimentation haute performance sans spécifier de temporisateur de veille.
- Désactivez le composant Indexing Service (Service d'indexation).

  **Remarque** L'indexation améliore les recherches en cataloguant les fichiers. Ne désactivez pas cette fonction pour les utilisateurs qui effectuent souvent des recherches.

- Supprimez ou réduisez les point de restauration du système.
- Désactivez la protection du système sur `C:\`.
- Désactivez tout service inutile.
- Réglez le son sur **Aucun son**.
- Réglez les effets visuels sur **Ajuster afin d'obtenir les meilleures performances**.
- Ouvrez Windows Media Player et utilisez les paramètres par défaut.
- Désactivez la maintenance automatique de l'ordinateur.
- Ajustez les paramètres de performance pour de meilleures performances.
- Supprimez tous les dossiers de désinstallation masqués dans `C:\Windows`, tels que `$NtUninstallKB893756$`.
- Supprimez tous les journaux d'événements.
- Exécutez un nettoyage du disque pour supprimer les fichiers temporaires, vider la Corbeille et éliminer les fichiers système et les autres éléments devenus inutiles.
- Exécutez Disk Defragmenter (Défragmenteur de disque) pour réorganiser les données fragmentées.
- Désinstallez Tablet PC Components, à moins que cette fonction soit requise.
- Désactivez IPv6, sauf si l'option est requise.
- Utilisez la commande de l'utilitaire du système de fichiers (`fsutil`) pour désactiver le paramètre qui archive l'heure du dernier accès à un fichier.

  Par exemple : `fsutil behavior set disablelastaccess 1`

- Démarrez l'éditeur de Registre (`regedit.exe`) et remplacez la valeur de la clé **TimeOutValue** REG_DWORD, dans le chemin `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Disk`, par **`0x000000be(190)`**.
- Désactivez le programme d'amélioration de l'expérience utilisateur Windows et les tâches liées du Planificateur de tâches.
- Redémarrez Windows après avoir apporté les modifications ci-dessus.

### Suivant

Consultez « Optimisation de Windows pour des machines virtuelles de clone instantané et de clone lié View Composer », page 47 pour plus d'informations sur la désactivation de certains services et tâches Windows afin de réduire la croissance des clones instantanés et des clones liés View Composer. La désactivation de certains services et tâches peut également entraîner une amélioration des performances sur les machines virtuelles complètes.

## Désactiver le programme d'amélioration de l'expérience utilisateur Windows

La désactivation du programme d'amélioration du produit Windows et des tâches du Planificateur de tâches associées qui contrôlent ce programme peut améliorer les performances des systèmes Windows 7, Windows 8/8.1 et Windows 10 dans des pools de postes de travail volumineux.

Les étapes suivantes s'appliquent à Windows 7 et Windows 8. Les étapes peuvent varier selon les différents systèmes d'exploitation Windows.

### Procédure

1. Dans le système d'exploitation invité Windows 7 ou Windows 8, démarrez le panneau de configuration et cliquez sur **Centre de maintenance > Modifier les paramètres du Centre de maintenance**.
2. Cliquez sur **Paramètres du programme d'amélioration de l'expérience utilisateur**.
3. Sélectionnez **Non, je ne veux pas participer au programme** et cliquez sur **Enregistrer les modifications**.
4. Démarrez le panneau de configuration et cliquez sur **Outils d'administration > Planificateur de tâches**.
5. Dans le volet Planificateur de tâches (local) de la boîte de dialogue Planificateur de tâches, développez les nœuds **Bibliothèque du Planificateur de tâches > Microsoft > Windows** et ouvrez le dossier **Application Experience**.
6. Désactivez les tâches **AITAgent**, **ProgramDataUpdater** et, si disponible, **Microsoft Compatibility Appraiser**.
7. Dans le nœud **Bibliothèque du Planificateur de tâches > Microsoft > Windows**, ouvrez le dossier **Customer Experience Improvement Program**.
8. Désactivez les tâches **Consolidator**, **KernelCEIPTask** et **UsbCEIP**.
9. Dans le nœud **Bibliothèque du Planificateur de tâches > Microsoft > Windows**, ouvrez le dossier **Autochk**.
10. Désactivez la tâche **Proxy**.

### Suivant

Exécutez d'autres tâches d'optimisation Windows. Reportez-vous à la section « Optimiser les performances du système d'exploitation invité », page 44.

# Optimisation de Windows pour des machines virtuelles de clone instantané et de clone lié View Composer

En désactivant certains services et tâches Windows 7, Windows 8/8.1 et Windows 10, vous pouvez réduire la croissance de l'utilisation des disques de clones instantanés et de clones liés View Composer. La désactivation de certains services et tâches peut également entraîner une amélioration des performances sur les machines virtuelles complètes.

## Avantages de la désactivation des services et tâches Windows

Windows 7, Windows 8/8.1 et Windows 10 planifient des services et des tâches qui peuvent entraîner la croissance des clones instantanés et des clones liés View Composer, même lorsque les machines sont inactives. La croissance incrémentielle du disque du système d'exploitation peut annuler les économies de stockage que vous obtenez lors de la première création de clones. Vous pouvez réduire la croissance de la taille du disque en désactivant ces services Windows.

Les systèmes d'exploitation invités Windows planifient des services tels que la défragmentation de disque pour qu'ils s'exécutent par défaut. Ces services s'exécutent dans l'arrière-plan si vous ne les désactivez pas.

Les services qui affectent la croissance du disque du système d'exploitation génèrent également des opérations d'entrée/sortie. Désactiver ces services peut réduire les IOPS (opérations d'entrée/sortie par seconde) et améliorer les performances de tout type de machines de poste de travail.

Ces meilleures pratiques pour l'optimisation de Windows s'appliquent à la plupart des environnements d'utilisateur. Toutefois, vous devez évaluer l'effet de la désactivation de chaque service sur vos utilisateurs, applications et postes de travail. Il peut être nécessaire de laisser certains services actifs.

Par exemple, il est justifié de désactiver le service Windows Update pour les clones instantanés, car le système d'exploitation est actualisé chaque fois que l'utilisateur se déconnecte, et pour les clones liés View Composer si vous actualisez ou recomposez régulièrement.

## Services et tâches Windows causant la croissance des disques dans des clones instantanés et des clones liés

Certains services et tâches dans Windows 7, Windows 8/8.1 et Windows 10 peuvent entraîner la croissance progressive du disque du système d'exploitation d'un clone instantané ou d'un clone lié View Composer, même lorsque la machine est inactive. Si vous désactivez ces services et tâches, vous pouvez contrôler la croissance du disque du système d'exploitation.

Les services qui affectent la croissance du disque du système d'exploitation génèrent également des opérations d'E/S. De même, vous pouvez évaluer les avantages de la désactivation de ces services pour des clones complets.

Avant de désactiver les services Windows présentés dans Tableau 3-8, vérifiez que vous avez suivi la procédure d'optimisation de « Optimiser les performances du système d'exploitation invité », page 44.

**Tableau 3-8.** Impact des services et tâches Windows sur la croissance du disque du système d'exploitation et l'IOPS

| Service ou tâche | Description | Occurrence par défaut ou démarrage | Impact sur le disque du système d'exploitation | Impact sur l'IOPS | Désactiver ce service ou tâche ? |
|---|---|---|---|---|---|
| Mise en veille prolongée Windows | Offre un état d'économie d'énergie en stockant des documents et des programmes ouverts dans un fichier avant que l'ordinateur ne soit désactivé. Le fichier est rechargé dans la mémoire lorsque l'ordinateur est redémarré, en restaurant l'état au moment où la mise en veille prolongée a été appelée. | Les paramètres par défaut du mode de gestion de l'alimentation désactivent la mise en veille prolongée. | Élevé.<br>Par défaut, la taille du fichier de mise en veille prolongée, `hiberfil.sys`, est la même que la RAM installée sur la machine virtuelle. Cette fonction affecte tous les systèmes d'exploitation client. | Élevé.<br>Lorsque la mise en veille prolongée est déclenchée, le système écrit un fichier `hiberfil.sys` de la taille de la RAM installée. | Oui<br>La mise en veille prolongée n'a aucun avantage dans un environnement virtuel.<br>Pour plus d'informations, reportez-vous à la section « Désactiver la mise en veille prolongée Windows sur la machine virtuelle parente », page 57. |
| Défragmentation de disque planifiée Windows | La défragmentation de disque est planifiée en tant que processus d'arrière-plan. | Une fois par semaine | Élevé.<br>Des opérations de défragmentation répétées peuvent augmenter de plusieurs Go la taille du disque du système d'exploitation et ne rendent pas l'accès au disque plus efficace. | Élevée | Oui |
| Service Windows Update | Détecte, télécharge et installe des mises à jour pour Windows et d'autres programmes. | Démarrage automatique | Moyen à élevé.<br>Entraîne des écritures fréquentes sur le disque du système d'exploitation, car des vérifications de mise à jour se produisent souvent. L'impact dépend des mises à jour téléchargées. | Moyen à élevé | Oui, pour les clones instantanés, et pour les clones liés View Composer que vous actualisez ou recomposez régulièrement. |
| Service de stratégie de diagnostic Windows | Détecte, dépanne et résout des problèmes liés aux composants Windows. Si vous arrêtez ce service, les diagnostics ne fonctionnent plus. | Démarrage automatique | Moyen à élevé.<br>Le service est déclenché à la demande. La fréquence d'écriture varie, en fonction de la demande. | Faible à moyen | Oui, si vous n'avez pas besoin que les outils de diagnostic fonctionnent sur les postes de travail. |

**Tableau 3-8.** Impact des services et tâches Windows sur la croissance du disque du système d'exploitation et l'IOPS (suite)

| Service ou tâche | Description | Occurrence par défaut ou démarrage | Impact sur le disque du système d'exploitation | Impact sur l'IOPS | Désactiver ce service ou tâche ? |
|---|---|---|---|---|---|
| Prérécupération/Superfetch | Stocke des informations spécifiques sur les applications que vous exécutez pour les aider à démarrer plus vite. | Toujours activé, sauf s'il est désactivé. | Moyenne<br>Entraîne des mises à jour périodiques de ses informations de disposition et de base de données et des fichiers de prérécupération individuels, qui sont générés à la demande. | Moyenne | Oui, si les heures de démarrage d'application sont acceptables quand vous désactivez cette fonction. |
| Sauvegarde du registre Windows (`RegIdleBackup`) | Sauvegarde automatiquement le registre Windows lorsque le système est inactif. | Tous les 10 jours à minuit | Moyen.<br>Chaque fois que cette tâche s'exécute, elle génère des fichiers de sauvegarde de registre. | Moyen. | Oui. Les clones instantanés et les clones liés View Composer vous permettent de restaurer un snapshot et de restaurer le Registre. |
| Restauration du système | Rétablit le système Windows à un état d'intégrité précédent. | Lorsque Windows démarre et ensuite une fois par jour. | Faible à moyen.<br>Capture un point de restauration système dès que le système détecte qu'il est nécessaire. | Aucun impact majeur. | Oui. Les clones instantanés et les clones liés View Composer vous permettent de revenir à un état sain. |

**Tableau 3-8.** Impact des services et tâches Windows sur la croissance du disque du système d'exploitation et l'IOPS (suite)

| Service ou tâche | Description | Occurrence par défaut ou démarrage | Impact sur le disque du système d'exploitation | Impact sur l'IOPS | Désactiver ce service ou tâche ? |
|---|---|---|---|---|---|
| Windows Defender | Offre des fonctions anti-espion. | Au démarrage de Windows. Effectue une analyse rapide une fois par jour. Recherche des mises à jour avant chaque analyse. | Moyen à élevé.<br>Effectue des mises à jour de définition, des analyses planifiées et des analyses démarrées à la demande. | Moyen à élevé. | Oui, si un autre logiciel anti-espion est installé. |
| Tâche Microsoft Feeds Synchronization (`msfeedssync.exe`) | Met à jour périodiquement des flux RSS dans les navigateurs Windows Internet Explorer. Cette tâche met à jour des flux RSS pour lesquels la synchronisation de flux RSS automatique est activée. Le processus apparaît dans le Gestionnaire des tâches de Windows uniquement quand Internet Explorer est en cours d'exécution. | Une fois par jour. | Moyen.<br>Affecte la croissance du disque du système d'exploitation si aucun disque persistant n'est configuré. Si des disques persistants sont configurés, l'impact est dévié sur les disques persistants. | Moyenne | Oui, si vos utilisateurs ne requièrent pas de mises à jour RSS automatiques sur leurs postes de travail. |

## Désactiver la défragmentation de disque planifiée sur une machine virtuelle parente Windows

Lorsque vous préparez une machine virtuelle parente pour des clones instantanés ou des clones liés View Composer, il vous est recommandé de désactiver la défragmentation planifiée. Par défaut, Windows planifie des défragmentations de disque une fois par semaine. La défragmentation augmente considérablement la taille du disque virtuel d'un clone et ne rend pas l'accès au disque plus efficace pour les clones instantanés ou les clones liés View Composer.

Les clones partagent le disque du système d'exploitation de la machine virtuelle parente, mais chaque clone conserve les modifications du système de fichiers dans son propre disque virtuel. Toutes les activités, notamment la défragmentation, augmenteront la taille du disque virtuel individuel de chaque clone ce qui, par conséquent, accroît la consommation de stockage. Il est recommandé de défragmenter la machine virtuelle parente, avant de prendre un snapshot et de créer le pool.

Les étapes suivantes s'appliquent à Windows 7 et Windows 8. Les étapes peuvent varier selon les différents systèmes d'exploitation Windows.

### Procédure

1 Dans vSphere Client, sélectionnez la machine virtuelle parente et sélectionnez **Ouvrir la console**.

2 Connectez-vous en tant qu'administrateur.

3 Cliquez sur **Démarrer** et saisissez `defrag` dans la zone **Rechercher les programmes et fichiers**.

4 Dans le volet Programmes, cliquez sur **Défragmenteur de disque**.

5 Dans la boîte de dialogue **Défragmenteur de disque**, cliquez sur **Défragmenter le disque**.

   Le Défragmenteur de disque consolide les fichiers défragmentés sur le disque dur de la machine virtuelle.

6 Dans la boîte de dialogue **Défragmenteur de disque**, cliquez sur **Configurer la planification**.

7 Décochez la case **Exécution planifiée (recommandé)** et cliquez sur **OK**.

## Désactiver Windows Update

La désactivation de la fonctionnalité Windows Update évite certaines opérations d'E/S sur le système de fichiers et peut réduire la croissance du disque virtuel d'un clone instantané ou d'un clone lié View Composer.

Évaluez les besoins de votre environnement avant de désactiver Windows Update. Si vous désactivez cette fonctionnalité, vous pouvez télécharger manuellement les mises à jour sur la machine virtuelle parente et utiliser l'opération d'image de transfert pour les clones instantanés ou de recomposition pour les clones liés View Composer afin d'appliquer les mises à jour sur tous les clones.

Les étapes suivantes s'appliquent à Windows 7 et Windows 8. Les étapes peuvent varier selon les différents systèmes d'exploitation Windows.

### Procédure

1 Dans vSphere Client, sélectionnez la machine virtuelle parente et sélectionnez **Ouvrir la console**.

2 Connectez-vous en tant qu'administrateur.

3 Cliquez sur **Démarrer > Panneau de configuration > Système et sécurité > Activer ou désactiver la mise à jour automatique**.

4 Dans le menu Mises à jour importantes, sélectionnez **Ne jamais rechercher de mises à jour**.

5 Décochez la case **Recevoir les mises à jour recommandées de la même façon que vous recevez les mises à jour importantes**.

6 Décochez la case **Autoriser tous les utilisateurs à installer les mises à jour sur cet ordinateur** et cliquez sur **OK**.

## Désactiver le service de stratégie de diagnostic sur des machines virtuelles Windows

La désactivation du service de stratégie de diagnostic Windows évite certaines opérations d'E/S sur le système de fichiers et peut réduire la croissance du disque virtuel d'un clone instantané ou d'un clone lié View Composer.

Ne désactivez pas le service de stratégie de diagnostic Windows si vos utilisateurs ont besoin des outils de diagnostic sur leurs postes de travail.

Les étapes suivantes s'appliquent à Windows 7 et Windows 8. Les étapes peuvent varier selon les différents systèmes d'exploitation Windows.

### Procédure

1 Dans vSphere Client, sélectionnez la machine virtuelle parente et sélectionnez **Ouvrir la console**.

2 Connectez-vous en tant qu'administrateur.

3 Cliquez sur **Démarrer > Panneau de configuration > Système et sécurité > Outils d'administration**.

4 Sélectionnez **Services** et cliquez sur **Ouvrir**.

5 Double-cliquez sur **Service de stratégie de diagnostic**.

6 Dans la boîte de dialogue Propriétés du service de stratégie de diagnostic (Ordinateur local), cliquez sur **Arrêter**.

7 Dans le menu Type de démarrage, sélectionnez **Désactivé**.

8 Cliquez sur **OK**.

## Désactiver les fonctions de prérécupération et Superfetch sur des machines virtuelles Windows

La désactivation de ces fonctionnalités évite certaines opérations d'E/S sur le système de fichiers et peut réduire la croissance du disque virtuel d'un clone instantané ou d'un clone lié View Composer.

Pour désactiver les fonctions de prérécupération et Superfetch, vous devez modifier une clé de Registre Windows et désactiver le service de prérécupération sur la machine virtuelle.

Les étapes suivantes s'appliquent à Windows 7 et Windows 8. Les étapes peuvent varier selon les différents systèmes d'exploitation Windows.

### Prérequis

Pour plus d'informations sur l'utilisation de l'éditeur de Registre Windows, consultez le site Web Microsoft TechNet.

### Procédure

1 Démarrez l'éditeur de Registre Windows sur la machine virtuelle Windows locale.

2 Allez à la clé de Registre appelée **PrefetchParameters**.

La clé de registre se trouve à l'emplacement suivant : `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters`.

3 Définissez les valeurs **EnablePrefetcher** et **EnableSuperfetch** sur `0`.

4 Cliquez sur **Démarrer > Panneau de configuration > Système et sécurité > Outils d'administration**.

5 Sélectionnez **Services** et cliquez sur **Ouvrir**.

6 Double-cliquez sur le service **Superfetch**.

7 Dans la boîte de dialogue Propriétés de Superfetch (Ordinateur local), cliquez sur **Arrêter**.

8 Dans le menu Type de démarrage, sélectionnez **Désactivé**.

9 Cliquez sur **OK**.

## Désactiver la sauvegarde du Registre Windows sur des machines virtuelles Windows

La désactivation de la fonctionnalité de sauvegarde du Registre Windows, `RegIdleBackup`, évite certaines opérations d'E/S sur le système de fichiers et peut réduire la croissance du disque virtuel d'un clone instantané ou d'un clone lié View Composer.

Les étapes suivantes s'appliquent à Windows 7 et Windows 8. Les étapes peuvent varier selon les différents systèmes d'exploitation Windows.

### Procédure

1 Dans vSphere Client, sélectionnez la machine virtuelle parente et sélectionnez **Ouvrir la console**.

2 Connectez-vous en tant qu'administrateur.

3 Cliquez sur **Démarrer > Panneau de configuration > Système et sécurité > Outils d'administration**.

4 Sélectionnez **Planificateur de tâches** et cliquez sur **Ouvrir**.

5 Dans le volet de gauche, développez **Bibliothèque du Planificateur de tâches**, **Microsoft**, **Windows**.

6 Double-cliquez sur **Registre** et sélectionnez **RegIdleBackup**.

7 Dans le volet Actions, cliquez sur **Désactiver**.

## Désactiver la Restauration du système sur des machines virtuelles Windows

La désactivation de la fonctionnalité Restauration du système Windows évite certaines opérations d'E/S sur le système de fichiers et peut réduire la croissance du disque virtuel d'un clone instantané ou d'un clone lié View Composer.

Avec la Restauration du système, vous pouvez rétablir l'état d'une machine à un point passé. Vous pouvez obtenir le même résultat avec l'opération d'image de transfert pour des clones instantanés et l'opération de recomposition ou d'actualisation pour les clones liés View Composer. De plus, avec les clones instantanés, lorsqu'un utilisateur se déconnecte, la machine est recréée, ce qui rend inutile la restauration du système.

Les étapes suivantes s'appliquent à Windows 7 et Windows 8. Les étapes peuvent varier selon les différents systèmes d'exploitation Windows.

### Procédure

1 Dans vSphere Client, sélectionnez la machine virtuelle parente et sélectionnez **Ouvrir la console**.

2 Connectez-vous en tant qu'administrateur.

3 Cliquez sur **Démarrer > Panneau de configuration > Système et sécurité > Outils d'administration**.

4 Sélectionnez **Planificateur de tâches** et cliquez sur **Ouvrir**.

5 Dans le volet de gauche, développez **Bibliothèque du Planificateur de tâches**, **Microsoft**, **Windows**.

6 Double-cliquez sur **SystemRestore** et sélectionnez **SR**.

7 Dans le volet Actions, cliquez sur **Désactiver**.

## Désactiver Windows Defender sur des machines virtuelles Windows

La désactivation de Windows Defender évite certaines opérations d'E/S sur le système de fichiers et peut réduire la croissance du disque virtuel d'un clone instantané ou d'un clone lié View Composer.

Si Windows Defender est le seul anti-espion installé sur la machine virtuelle, vous pouvez préférer laisser Windows Defender actif sur les postes de travail dans votre environnement.

Les étapes suivantes s'appliquent à Windows 7 et Windows 8. Les étapes peuvent varier selon les différents systèmes d'exploitation Windows.

### Procédure

1 Dans vSphere Client, sélectionnez la machine virtuelle parente et sélectionnez **Ouvrir la console**.

2 Connectez-vous en tant qu'administrateur.

3 Cliquez sur **Démarrer** et saisissez `Windows Defender` dans la zone Rechercher les programmes et fichiers.

4 Cliquez sur **Outils > Options > Administrateur**.

5 Décochez la case **Utiliser ce programme** et cliquez sur **Enregistrer**.

### Désactiver la tâche Microsoft Feeds Synchronization sur des machines virtuelles Windows

Windows Internet Explorer utilise la tâche Microsoft Feeds Synchronization pour mettre à jour des flux RSS dans les navigateurs Web des utilisateurs. La désactivation de cette tâche évite certaines opérations d'E/S sur le système de fichiers et peut réduire la croissance du disque virtuel d'un clone instantané ou d'un clone lié View Composer.

#### Procédure

1 Dans vSphere Client, sélectionnez la machine virtuelle parente et sélectionnez **Ouvrir la console**.

2 Connectez-vous en tant qu'administrateur.

3 Cliquez sur **Démarrer > Panneau de configuration > Réseau et Internet > Options Internet**.

4 Cliquez sur l'onglet **Contenu**.

5 Flux et composants Web Slice, cliquez sur **Paramètres**.

6 Décochez la case **Rechercher automatiquement les mises à jour des flux et des composants Web Slice** et cliquez sur **OK**.

7 Dans la boîte de dialogue Propriétés Internet, cliquez sur **OK**.

## Préparation d'une machine virtuelle parente

Pour déployer un pool de postes de travail de clone instantané ou de clone lié View Composer, vous devez d'abord préparer une machine virtuelle parente.

- Configurer une machine virtuelle parente page 55

  Après avoir créé une machine virtuelle que vous prévoyez d'utiliser comme parent, configurez l'environnement Windows.

- Activation de Windows sur des clones instantanés et des clones liés View Composer page 57

  Pour vous assurer que les clones Windows 7, Windows 8/8.1, Windows 10 et Windows Server sont correctement activés lorsqu'ils sont créés, vous devez utiliser l'activation du volume Microsoft sur la machine virtuelle parente. La technologie d'activation du volume requiert une clé de licence en volume.

- Désactiver la mise en veille prolongée Windows sur la machine virtuelle parente page 57

  La fonctionnalité de mise en veille prolongée Windows crée un fichier système masqué, `Hiberfil.sys`, et utilise ce fichier pour stocker des informations nécessaires pour la veille hybride. La désactivation de la mise en veille prolongée réduit la taille du disque virtuel d'un clone instantané ou d'un clone lié View Composer.

- Configurer le stockage local des clones liés View Composer page 58

  Pour un pool de postes de travail de clone lié View Composer, vous pouvez configurer la machine virtuelle parente afin de stocker les fichiers d'échange de machine virtuelle sur un magasin de données local. Les fichiers d'échange des clones liés résideront sur le stockage local. Cette fonctionnalité n'est pas disponible pour les clones instantanés.

- Enregistrer la taille du fichier de pagination d'une machine virtuelle parente View Composer page 58

  Lorsque vous créez un pool de postes de travail de clone lié View Composer, vous pouvez rediriger les fichiers de pagination et temporaires des clones vers un disque séparé. Vous devez configurer ce disque pour que sa taille soit supérieure à celle du fichier de pagination sur la machine virtuelle parente.

- Augmenter la limite du délai d'expiration des scripts de personnalisation ClonePrep et QuickPrep page 59

  Les scripts de post-synchronisation ou de désactivation ClonePrep et QuickPrep ont une limite du délai d'expiration de 20 secondes. Vous pouvez augmenter cette limite en modifiant la valeur de Registre Windows `ExecScriptTimeout` sur la machine virtuelle parente.

## Configurer une machine virtuelle parente

Après avoir créé une machine virtuelle que vous prévoyez d'utiliser comme parent, configurez l'environnement Windows.

### Prérequis

- Vérifiez que vous avez préparé une machine virtuelle à utiliser pour le déploiement de postes de travail distants. Reportez-vous à la section « Création d'une machine virtuelle pour le clonage », page 26.

  La machine virtuelle parente peut appartenir au même domaine Active Directory que celui que rejoindront les machines de poste de travail ou être un membre d'un groupe de travail.

- Vérifiez que la machine virtuelle n'a pas été convertie depuis un clone instantané ou un clone lié View Composer.

  **Important** De même, vous ne pouvez pas utiliser un clone instantané ou un clone lié View Composer comme machine virtuelle parente.

- Lorsque vous installez Horizon Agent sur la machine virtuelle parente, sélectionnez l'option **VMware Horizon Instant Clone Agent** pour les clones instantanés ou l'option **VMware Horizon View Composer Agent**. Reportez-vous à la section « Installer Horizon Agent sur une machine virtuelle », page 33.

  Pour mettre à jour Horizon Agent dans un environnement volumineux, vous pouvez utiliser des mécanismes de mise à jour Windows standard comme Altiris, SMS, LanDesk, BMC ou d'autres logiciels de gestion des systèmes. Vous pouvez également utiliser l'image de transfert ou l'opération de recomposition pour mettre à jour Horizon Agent.

  **Remarque** Pour les clones liés View Composer, ne modifiez pas le compte d'ouverture de session pour le service VMware View Composer Guest Agent Server dans une machine virtuelle parente. Par défaut, il s'agit du compte de système local. Si vous modifiez ce compte, les clones liés créés à partir du parent ne démarreront pas.

- Pour déployer des machines Windows, configurez une clé de licence en volume et activez le système d'exploitation de la machine virtuelle parente avec l'activation en volume. Reportez-vous à la section « Activation de Windows sur des clones instantanés et des clones liés View Composer », page 57.

- Vérifiez que vous avez suivi les meilleures pratiques pour optimiser le système d'exploitation. Reportez-vous à la section « Optimisation de Windows pour des machines virtuelles de clone instantané et de clone lié View Composer », page 47.

- Familiarisez-vous avec la procédure de désactivation de la recherche de pilotes de périphérique de Windows Update. Consultez l'article de Microsoft Technet « Désactiver la recherche de pilotes de périphérique de Windows Update » à l'adresse http://technet.microsoft.com/en-us/library/cc730606(v=ws.10).aspx.

### Procédure

- Désactivez le bail DHCP sur la machine virtuelle parente pour empêcher la copie d'une adresse IP avec bail vers les clones liés du pool.

  a Sur la machine virtuelle parente, ouvrez une invite de commande.

  b Saisissez la commande **`ipconfig /release`**.

- Vérifiez que le disque système contient un seul volume.

  Vous ne pouvez pas déployer de clones liés à partir d'une machine virtuelle parente contenant plusieurs volumes. Plusieurs disques virtuels sont pris en charge.

  **Remarque** Pour les clones liés View Composer, si la machine virtuelle parente contient plusieurs disques virtuels, lorsque vous créez un pool de postes de travail, ne sélectionnez pas une lettre de lecteur pour le disque persistant de View Composer ou le disque de données supprimable qui existe déjà sur la machine virtuelle parente ou qui entre en conflit avec une lettre de lecteur utilisée pour un lecteur monté en réseau.

- Vérifiez que la machine virtuelle ne contient pas de disque indépendant.

  Un disque indépendant est exclu lorsque vous prenez un snapshot de la machine virtuelle. Les clones sont basés sur un snapshot et ils ne contiendront donc pas le disque indépendant.

- Pour les clones liés View Composer, si vous prévoyez de configurer des disques de données supprimables lorsque vous créez des machines de clone lié, supprimez les variables utilisateur `TEMP` et `TMP` par défaut de la machine virtuelle parente.

  Vous pouvez également supprimer le fichier `pagefile.sys` pour éviter la duplication du fichier sur tous les clones liés. Si vous laissez le fichier `pagefile.sys` sur la machine virtuelle parente, une version en lecture seule du fichier est héritée par les clones liés, alors qu'une deuxième version du fichier est utilisée sur le disque de données supprimable.

- Désactivez l'option de veille prolongée pour réduire la taille du disque virtuel de chaque clone.

- Avant de prendre un snapshot de la machine virtuelle parente, désactivez la recherche de pilotes de périphérique de Windows Update.

  Cette fonctionnalité Windows peut interférer avec le processus de personnalisation. À chaque fois qu'un clone est personnalisé, Windows peut rechercher les meilleurs pilotes sur Internet pour ce clone, ce qui entraîne des retards.

- Dans vSphere Client, désactivez le paramètre vApp Options (Options vApp) sur la machine virtuelle parente.

- Sur les machines Windows 8.1, Windows Server 2008 R2 et Windows Server 2012 R2, désactivez la tâche de maintenance planifiée qui récupère de l'espace disque en supprimant des fonctionnalités inutilisées.

  Par exemple : `Schtasks.exe /change /disable /tn "\Microsoft\Windows\AppxDeploymentClient\Pre-staged app cleanup"`

  Par exemple, dans le cas de clones liés View Composer, cette tâche de maintenance peut supprimer le script de personnalisation Sysprep après la création des clones liés, ce qui entraînerait l'échec des opérations de recomposition suivantes avec des erreurs d'expiration de délai de l'opération de personnalisation. Pour plus d'informations, reportez-vous à l'article de base de connaissances Microsoft disponible à l'adresse http://support.microsoft.com/kb/2928948.

### Suivant

Utilisez vSphere Client ou vSphere Web Client pour prendre un snapshot de la machine virtuelle parente dans son état hors tension. Ce snapshot fournit l'image de base pour les clones.

**Important** Avant de prendre un snapshot, arrêtez la machine virtuelle parente.

## Activation de Windows sur des clones instantanés et des clones liés View Composer

Pour vous assurer que les clones Windows 7, Windows 8/8.1, Windows 10 et Windows Server sont correctement activés lorsqu'ils sont créés, vous devez utiliser l'activation du volume Microsoft sur la machine virtuelle parente. La technologie d'activation du volume requiert une clé de licence en volume.

Pour activer Windows avec l'activation en volume, vous devez utiliser le service de gestion des clés (KMS, Key Management Service) qui nécessite une clé de licence KMS. Contactez votre revendeur Microsoft pour acquérir une clé de licence en volume et configurer l'activation du volume.

**Remarque** La licence de clé d'activation multiple (MAK, Multiple Activation Key) n'est pas prise en charge.

Avant de créer un pool de postes de travail de clone instantané ou de clone lié View Composer, vous devez utiliser l'activation du volume pour activer Windows sur la machine virtuelle parente.

Les étapes suivantes décrivent comment se déroule l'activation :

1 Appelez un script pour supprimer la licence existante.

2 Redémarrez Windows.

3 Appelez un script qui utilise la licence KMS pour activer Windows.

KMS traite chaque clone activé en tant qu'ordinateur avec une nouvelle licence émise.

## Désactiver la mise en veille prolongée Windows sur la machine virtuelle parente

La fonctionnalité de mise en veille prolongée Windows crée un fichier système masqué, `Hiberfil.sys`, et utilise ce fichier pour stocker des informations nécessaires pour la veille hybride. La désactivation de la mise en veille prolongée réduit la taille du disque virtuel d'un clone instantané ou d'un clone lié View Composer.

**Avertissement** Lorsque vous désactivez la mise en veille prolongée, la veille hybride ne fonctionne pas. Les utilisateurs peuvent perdre des données en cas de perte de puissance.

### Procédure

1 Dans vSphere Client, sélectionnez la machine virtuelle parente et sélectionnez **Ouvrir la console**.

2 Connectez-vous en tant qu'administrateur.

3 Désactivez l'option de mise en veille prolongée.

   a Cliquez sur **Démarrer** et saisissez **`cmd`** dans la zone **Rechercher**.

   b Dans la liste de résultats de la recherche, cliquez avec le bouton droit sur **Invite de commandes** et cliquez sur **Exécuter en tant qu'administrateur**.

   c À l'invite Contrôle de compte d'utilisateur, cliquez sur **Continuer**.

   d À l'invite de commande, saisissez **`powercfg.exe /hibernate off`** et appuyez sur Entrée.

   e Saisissez **`exit`** et appuyez sur Entrée.

## Configurer le stockage local des clones liés View Composer

Pour un pool de postes de travail de clone lié View Composer, vous pouvez configurer la machine virtuelle parente afin de stocker les fichiers d'échange de machine virtuelle sur un magasin de données local. Les fichiers d'échange des clones liés résideront sur le stockage local. Cette fonctionnalité n'est pas disponible pour les clones instantanés.

Dans cette procédure, vous configurez le stockage local pour les fichiers d'échange de machine virtuelle, pas les fichiers d'échange et temporaires dans le système d'exploitation client. Lorsque vous créez un pool de clone lié, vous pouvez également rediriger les fichiers d'échange et temporaires du système d'exploitation client vers un disque séparé. Reportez-vous à la section « Feuille de calcul pour créer un pool de postes de travail de clone lié », page 71.

### Procédure

1 Configurez une banque de données de fichier d'échange sur l'hôte ou le cluster ESXi sur lequel vous allez déployer le pool de clone lié.

2 Lorsque vous créez la machine virtuelle parente dans vCenter Server, stockez les fichiers d'échange de machine virtuelle dans la banque de données de fichiers d'échange sur l'hôte ou le cluster ESXi local :

   a Dans vSphere Client, sélectionnez la machine virtuelle parente.

   b Cliquez sur **Modifier les paramètres** et cliquez sur l'onglet **Options**.

   c Cliquez sur **Emplacement du fichier d'échange**, puis sur **Stocker dans le magasin de données de fichier d'échange de l'hôte**.

   Pour plus d'instructions, consultez la documentation de VMware vSphere.

## Enregistrer la taille du fichier de pagination d'une machine virtuelle parente View Composer

Lorsque vous créez un pool de postes de travail de clone lié View Composer, vous pouvez rediriger les fichiers de pagination et temporaires des clones vers un disque séparé. Vous devez configurer ce disque pour que sa taille soit supérieure à celle du fichier de pagination sur la machine virtuelle parente.

Lorsqu'un clone lié configuré avec un disque séparé pour les fichiers supprimables est désactivé, le disque est recréé. Cette fonctionnalité peut ralentir la croissance de la taille d'un clone lié. Toutefois, cette fonctionnalité ne peut agir que si vous configurez le disque de fichier supprimable pour qu'il soit suffisamment volumineux pour contenir le fichier de pagination du clone.

Avant de configurer le disque de fichier supprimable, enregistrez la taille maximale de fichier de pagination dans la machine virtuelle parente. Les clones liés ont la même taille de fichier de pagination que la machine virtuelle parente.

Il est recommandé de supprimer le fichier `pagefile.sys` de la machine virtuelle parente avant de prendre un snapshot pour éviter la duplication du fichier sur tous les clones liés. Reportez-vous à la section « Configurer une machine virtuelle parente », page 55.

---

**Remarque** Cette fonctionnalité n'est pas la même que la configuration du stockage local pour les fichiers d'échange de machine virtuelle. Reportez-vous à la section « Configurer le stockage local des clones liés View Composer », page 58.

---

### Procédure

1 Dans vSphere Client, cliquez avec le bouton droit sur la machine virtuelle parente et cliquez sur **Ouvrir la console**.

2 Sélectionnez **Démarrer > Paramètres > Panneau de configuration > Système**.

3 Cliquez sur l'onglet **Avancé**.

4 Dans le volet Performances, cliquez sur **Paramètres**.

5 Cliquez sur l'onglet **Avancé**.

6 Dans le volet Mémoire virtuelle, cliquez sur **Modifier**.

La page Mémoire virtuelle apparaît.

7 Définissez la taille du fichier d'échange sur une valeur supérieure à celle de la mémoire affectée à la machine virtuelle.

---

**Important** Si le paramètre **Taille maximale (Mo)** est inférieur à la taille de la mémoire de la machine virtuelle, saisissez une valeur supérieure et enregistrez la nouvelle valeur.

---

8 Conservez une trace du paramètre **Taille maximale (Mo)** configuré dans le volet Taille du fichier d'échange pour le lecteur sélectionné.

### Suivant

Lorsque vous configurez un pool de clone lié à partir de cette machine virtuelle parente, configurez un disque de fichier supprimable dont la taille est supérieure à celle du fichier d'échange.

## Augmenter la limite du délai d'expiration des scripts de personnalisation ClonePrep et QuickPrep

Les scripts de post-synchronisation ou de désactivation ClonePrep et QuickPrep ont une limite du délai d'expiration de 20 secondes. Vous pouvez augmenter cette limite en modifiant la valeur de Registre Windows `ExecScriptTimeout` sur la machine virtuelle parente.

Au lieu d'augmenter la limite du délai d'expiration, vous pouvez également utiliser votre script de personnalisation pour lancer un autre script ou processus qui effectue la tâche de longue durée.

---

**Remarque** La plupart des scripts de personnalisation QuickPrep peuvent arrêter leur exécution dans la limite de 20 secondes. Testez vos scripts avant d'augmenter la limite.

---

### Procédure

1 Sur la machine virtuelle parente, démarrez l'Éditeur du Registre Windows.

   a Sélectionnez **Démarrer > Invite de commande**.

   b À l'invite de commande, saisissez **regedit**.

2 Dans le Registre Windows, recherchez la clé de registre `vmware-viewcomposer-ga`.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\vmware-viewcomposer-ga
```

3 Cliquez sur **Modifier** et modifiez la valeur de registre.

```
Value Name: ExecScriptTimeout
Value Type: REG_DWORD
Value unit: milliseconds
```

La valeur par défaut est de 20 000 millisecondes.

## Création de modèles de machine virtuelle

Vous devez créer un modèle de machine virtuelle avant de pouvoir créer un pool automatisé qui contient des machines virtuelles complètes.

Un modèle de machine virtuelle est une copie principale d'une machine virtuelle pouvant être utilisée pour créer et approvisionner de nouvelles machines virtuelles. En général, un modèle inclut un système d'exploitation client installé et un jeu d'applications.

Vous créez des modèles de machines virtuelles dans vSphere Client. Vous pouvez créer un modèle de machine virtuelle depuis une machine virtuelle configurée précédemment, ou vous pouvez convertir une machine virtuelle configurée précédemment en modèle de machine virtuelle.

Pour plus d'informations sur l'utilisation de vSphere Client pour créer des modèles de machines virtuelles, consultez le guide *vSphere Basic System Administration (Administration de système de base vSphere)*. Pour plus d'informations sur la création de pools automatisés, reportez-vous à la section « Pools automatisés contenant des machines virtuelles complètes », page 61.

---

**Remarque** Un modèle de machine virtuelle n'est pas conçu pour créer un pool de postes de travail de clone instantané ou de clone lié View Composer.

---

## Création de spécifications de personnalisation

Lorsque vous personnalisez un clone à l'aide de Sysprep, vous devez fournir une spécification de personnalisation.

Sysprep est disponible pour les pools de postes de travail de clone lié View Composer et les pools de postes de travail de clone complet automatisés, mais pas les pools de postes de travail de clone instantané. Vous créez des spécifications de personnalisation en utilisant l'assistant Spécification de personnalisation dans vSphere. Pour plus d'informations sur l'utilisation de l'assistant Customization Specification (Spécification de personnalisation), consultez le document *vSphere Virtual Machine Administration (Administration de machine virtuelle vSphere)*.

Il vous est recommandé de tester une spécification de personnalisation dans vSphere avant de l'utiliser pour créer un pool de postes de travail. Lorsque vous utilisez une spécification de personnalisation Sysprep pour associer un poste de travail Windows à un domaine, vous devez utiliser le nom de domaine complet (FQDN) du domaine Active Directory. Vous ne pouvez pas utiliser le nom NetBIOS.

# Création de pools de postes de travail automatisés contenant des machines virtuelles complètes

# 4

Avec un pool de postes de travail automatisé qui contient des machines virtuelles complètes, vous créez un modèle de machine virtuelle et View utilise ce modèle pour créer des machines virtuelles pour chaque poste de travail. Vous pouvez facultativement créer des spécifications de personnalisation pour accélérer les déploiements de pools automatisés.

Ce chapitre aborde les rubriques suivantes :



## Pools automatisés contenant des machines virtuelles complètes

Pour créer un pool de postes de travail automatisé, View provisionne des machines de manière dynamique en fonction de paramètres que vous appliquez au pool. View utilise un modèle de machine virtuelle en tant que base pour le pool. À partir du modèle, View crée une machine virtuelle dans vCenter Server pour chaque poste de travail.

## Feuille de calcul pour créer un pool automatisé contenant des machines virtuelles complètes

Lorsque vous créez un pool de postes de travail automatisé, l'assistant Ajouter un pool de postes de travail de View Administrator vous invite à configurer certaines options. Utilisez cette feuille de calcul pour préparer vos options de configuration avant de créer le pool.

Vous pouvez imprimer cette feuille de calcul et noter les valeurs que vous souhaitez spécifier quand vous exécutez l'assistant Ajouter un pool de postes de travail.

**Tableau 4-1.** Feuille de calcul : options de configuration pour créer un pool automatisé contenant des machines virtuelles complètes

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| Affectation d'utilisateur | Choisissez le type d'affectation d'utilisateur :<br>■ Dans un pool à attribution dédiée, une machine est attribuée à chaque utilisateur. Les utilisateurs reçoivent la même machine chaque fois qu'ils ouvrent une session sur le pool.<br>■ Dans un pool à attribution flottante, les utilisateurs reçoivent des machines différentes chaque fois qu'ils ouvrent une session.<br>Pour plus d'informations, reportez-vous à « Affectation d'utilisateur dans des pools de postes de travail », page 151. | |
| Activer l'affectation automatique | Dans un pool à attribution dédiée, une machine est attribuée à un utilisateur lorsque celui-ci se connecte pour la première fois au pool. Vous pouvez également attribuer des machines aux utilisateurs de manière explicite.<br>Si vous n'activez pas l'attribution automatique, vous devez attribuer une machine à chaque utilisateur de manière explicite.<br>Vous pouvez attribuer des machines manuellement, même lorsque l'attribution automatique est activée. | |
| vCenter Server | Sélectionnez le serveur vCenter Server qui gère les machines virtuelles dans le pool. | |
| ID du pool de postes de travail | Nom unique qui identifie le pool dans View Administrator.<br>Si plusieurs serveurs vCenter Server sont exécutés dans votre environnement, assurez-vous qu'aucun autre serveur vCenter Server n'utilise le même ID de pool.<br>Une configuration du Serveur de connexion View peut être une instance autonome du Serveur de connexion View ou un espace d'instances répliquées partageant une configuration commune de View LDAP. | |
| Nom d'affichage | Nom du pool que les utilisateurs voient lorsqu'ils se connectent à partir d'un périphérique client. Si vous ne spécifiez pas de nom d'affichage, l'ID de pool est affiché aux utilisateurs. | |
| Groupe d'accès | Sélectionnez un groupe d'accès dans lequel placer le pool ou laissez ce dernier dans le groupe d'accès racine par défaut.<br>Si vous utilisez un groupe d'accès, vous pouvez déléguer la gestion du pool à un administrateur avec un rôle spécifique. Pour plus d'informations, reportez-vous au chapitre consacré à l'administration déléguée basée sur des rôles du document *Administration de View*.<br>**Remarque** Les groupes d'accès sont différents des dossiers vCenter Server qui stockent des machines virtuelles de poste de travail. Vous sélectionnez un dossier vCenter Server plus tard dans l'assistant avec d'autres paramètres de vCenter Server. | |

**Tableau 4-1.** Feuille de calcul : options de configuration pour créer un pool automatisé contenant des machines virtuelles complètes (suite)

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| Supprimer la machine après la fermeture de session | Si vous sélectionnez une attribution flottante à des utilisateurs, choisissez si vous voulez supprimer des machines quand les utilisateurs ferment leur session.<br>REMARQUE Vous définissez cette option sur la page Paramètres de pool de postes de travail. | |
| Paramètres du pool de postes de travail | Paramètres qui déterminent l'état du poste de travail, l'état d'alimentation quand une machine virtuelle n'est pas utilisée, le protocole d'affichage, la qualité Adobe Flash, etc.<br>Pour obtenir une description, reportez-vous à « Paramètres de pools de postes de travail pour tous les types de pools de postes de travail », page 160.<br>Pour consulter la liste des paramètres qui s'appliquent à des pools automatisés, reportez-vous à la section « Paramètres de poste de travail pour des pools automatisés contenant des machines virtuelles complètes », page 68<br>Pour plus d'informations sur les stratégies d'alimentation et les pools automatisés, reportez-vous à « Définition de règles d'alimentation pour des pools de postes de travail », page 165. | |
| Arrêter l'approvisionnement en cas d'erreur | Vous pouvez faire en sorte qu'View arrête ou continue le provisionnement des machines virtuelles dans un pool de postes de travail suite à une erreur survenue au cours du provisionnement d'une machine virtuelle. Si vous laissez ce paramètre sélectionné, vous pouvez empêcher qu'une erreur de provisionnement se répète sur plusieurs machines virtuelles. | |
| Attribution de nom aux machines virtuelles | Indiquez si vous souhaitez provisionner des machines en spécifiant manuellement la liste des noms de machines ou en indiquant un mode d'attribution de nom et le nombre total de machines.<br>Pour plus d'informations, reportez-vous à « Dénomination manuelle de machines ou fourniture d'un mode d'attribution de nom », page 152. | |
| Spécifier des noms manuellement | Si vous spécifiez les noms manuellement, préparez la liste des noms de machines et, éventuellement, les noms d'utilisateurs associés. | |
| Mode d'attribution de nom | Si vous utilisez cette méthode de nommage, fournissez le mode.<br>Le modèle que vous spécifiez est utilisé en tant que préfixe dans tous les noms de machines, suivi d'un numéro unique identifiant chaque machine.<br>Pour plus d'informations, reportez-vous à « Utilisation d'un mode d'attribution de nom pour des pools de postes de travail automatisés », page 155. | |

**Tableau 4-1.** Feuille de calcul : options de configuration pour créer un pool automatisé contenant des machines virtuelles complètes (suite)

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| Nombre maximal de machines | Si vous utilisez un mode d'attribution de nom, spécifiez le nombre total de machines dans le pool.<br>Vous pouvez également spécifier un nombre minimal de machines à provisionner lorsque vous créez le pool. | |
| Nombre de machines de rechange (sous tension) | Si vous spécifiez les noms manuellement ou si vous utilisez un mode d'attribution de nom, indiquez un nombre de machines à garder à disposition et sous tension pour les nouveaux utilisateurs. Pour plus d'informations, reportez-vous à « Dénomination manuelle de machines ou fourniture d'un mode d'attribution de nom », page 152.<br>Lorsque vous spécifiez les noms manuellement, cette option est appelée **Nb de machines non affectées maintenues sous tension**. | |
| Nombre minimal de machines | Si vous utilisez un mode d'attribution de nom et que vous provisionnez des machines à la demande, spécifiez un nombre minimal de machines dans le pool.<br>Le nombre minimal de machines est créé lorsque vous créez le pool.<br>Si vous provisionnez des machines à la demande, des machines supplémentaires sont créées à mesure que les utilisateurs se connectent au pool pour la première fois ou à mesure que vous attribuez des machines à des utilisateurs. | |
| Utiliser vSphere Virtual SAN | Spécifiez s'il convient d'utiliser Virtual SAN, le cas échéant. Virtual SAN est une couche de stockage définie par logiciel qui virtualise les disques de stockage physique locaux disponibles sur un cluster d'hôtes ESXi. Pour plus d'informations, reportez-vous à la section « Utilisation de Virtual SAN pour un stockage haute performance et une gestion basée sur les stratégies », page 273. | |
| Modèle | Sélectionnez le modèle de machine virtuelle à utiliser pour créer le pool. | |
| vCenter Server folder (Dossier vCenter Server) | Sélectionnez le dossier dans vCenter Server dans lequel réside le pool de postes de travail. | |
| Host or cluster (Hôte ou cluster) | Sélectionnez l'hôte ou le cluster ESXi sur lequel les machines virtuelles s'exécutent.<br>Dans vSphere 5.1 ou supérieur, vous pouvez sélectionner un cluster avec 32 hôtes ESXi maximum. | |
| Resource pool (Pool de ressources) | Sélectionnez le pool de ressources de vCenter Server dans lequel le pool de postes de travail réside. | |

**Tableau 4-1.** Feuille de calcul : options de configuration pour créer un pool automatisé contenant des machines virtuelles complètes (suite)

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| Magasins de données | Sélectionnez un ou plusieurs magasins de données sur lesquels stocker le pool de postes de travail.<br>Pour les clusters, vous pouvez utiliser des magasins des données partagés ou locaux.<br>**Remarque** Si vous utilisez Virtual SAN, sélectionnez une seule banque de données. | |
| Utiliser View Storage Accelerator | Déterminez si les hôtes ESXi mettent en cache des données de disque de machine virtuelle communes. View Storage Accelerator peut améliorer les performances et réduire le besoin de bande passante d'E/S de stockage supplémentaire pour gérer des tempêtes de démarrage et des tempêtes d'E/S d'analyse antivirus.<br>Cette fonction est prise en charge sur vSphere 5.0 et supérieur.<br>Cette fonction est activée par défaut.<br>Pour plus d'informations, reportez-vous à « Configurer View Storage Accelerator des clones liés View Composer », page 290. | |
| Portée du partage de page transparente (Transparent Page Sharing) | Sélectionnez le niveau auquel autoriser le partage de page transparente (TPS). Les choix sont **Machine virtuelle** (par défaut), **Pool**, **Espace** ou **Global**. Si vous activez le partage de page transparente pour les machines du pool, de l'espace ou globalement, l'hôte ESXi élimine les copies redondantes des pages mémoire obtenues si les machines utilisent le même système d'exploitation invité ou les mêmes applications.<br>Le partage de page se produit sur l'hôte ESXi. Par exemple, si vous activez le partage de page transparente au niveau du pool alors que le pool couvre plusieurs hôtes ESXi, seules les machines virtuelles sur le même hôte et à l'intérieur du même pool partageront des pages. Au niveau global, toutes les machines gérées par View sur le même hôte ESXi peuvent partager des pages de mémoire, quel que soit le pool sur lequel résident les machines.<br>**Remarque** Par défaut, les pages de mémoire ne sont pas partagées entre plusieurs machines, car le partage de page transparente (TPS) peut créer un risque. Les recherches indiquent que le partage de page transparente peut être exploité de façon abusive pour obtenir un accès non autorisé à des données dans des scénarios de configuration très limités. | |
| Guest customization (Personnalisation client) | Sélectionnez une spécification de personnalisation (SYSPREP) dans la liste pour configurer des paramètres de licence, d'association de domaine, de protocole DHCP et d'autres propriétés sur les machines.<br>Vous pouvez également personnaliser les machines manuellement après leur création. | |

# Créer un pool automatisé contenant des machines virtuelles complètes

Vous pouvez créer un pool de postes de travail automatisé basé sur un modèle de machine virtuelle que vous sélectionnez. View déploie dynamiquement les postes de travail, en créant une nouvelle machine virtuelle dans vCenter Server pour chaque poste de travail.

### Prérequis

- Préparez un modèle de machine virtuelle que View utilisera pour créer les machines. Horizon Agent doit être installé sur le modèle. Reportez-vous à la section Chapitre 3, « Création et préparation d'une machine virtuelle parente pour le clonage », page 25.
- Si vous prévoyez d'utiliser une spécification de personnalisation, assurez-vous que les spécifications sont exactes. Dans vSphere Client, déployez et personnalisez une machine virtuelle depuis votre modèle à l'aide de la spécification de personnalisation. Testez entièrement la machine virtuelle résultante, notamment DHCP et l'authentification.
- Vérifiez que vous disposez d'un nombre suffisant de ports sur le commutateur virtuel ESXi utilisé pour les machines virtuelles servant de postes de travail distants. La valeur par défaut peut ne pas être suffisante si vous créez des pools de postes de travail volumineux. Le nombre de ports de commutateur virtuel sur l'hôte ESXi doit être égal ou supérieur au nombre de machines virtuelles multiplié par le nombre de cartes réseau virtuelles par machine virtuelle.
- Collectez les informations de configuration que vous devez fournir pour créer le pool. Reportez-vous à la section « Feuille de calcul pour créer un pool automatisé contenant des machines virtuelles complètes », page 61.
- Décidez comment configurer les paramètres d'alimentation, le protocole d'affichage, la qualité Adobe Flash et d'autres paramètres. Reportez-vous à la section « Paramètres de pools de postes de travail pour tous les types de pools de postes de travail », page 160.
- Si vous prévoyez de fournir un accès à vos applications et postes de travail via VMware Identity Manager, assurez-vous de créer les pools d'applications et de postes de travail en tant qu'utilisateur disposant du rôle Administrateurs sur le groupe d'accès racine dans View Administrator. Si vous attribuez à l'utilisateur le rôle Administrateurs sur un groupe d'accès autre que le groupe d'accès racine, VMware Identity Manager ne reconnaîtra pas l'authentificateur SAML que vous configurez dans View et vous ne pourrez pas configurer le pool dans VMware Identity Manager.

### Procédure

1. Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.
2. Cliquez sur **Ajouter**.
3. Sélectionnez **Pool de postes de travail automatisé**.
4. Sur la page vCenter Server, choisissez **Machines virtuelles complètes**.
5. Suivez les invites de l'assistant pour créer le pool.

   Utilisez les informations de configuration que vous avez collectées dans la feuille de calcul. Vous pouvez revenir directement à n'importe quelle page de l'assistant en cliquant sur le nom de page dans le volet de navigation.

Dans View Administrator, vous pouvez afficher les machines à mesure de leur ajout au pool en sélectionnant **Catalogue > Pools de postes de travail**.

### Suivant

Autorisez les utilisateurs à accéder au pool. Reportez-vous à la section « Ajouter des droits d'accès à un pool de postes de travail ou d'applications », page 187.

## Cloner un pool de postes de travail automatisé

Vous pouvez cloner un pool de postes de travail automatisé à partir d'un pool existant. Lorsque vous clonez un pool, les paramètres du pool de postes de travail existant sont copiés dans l'assistant Ajouter un pool de postes de travail, ce qui vous permet de créer un pool sans avoir à remplir chaque paramètre manuellement.

Avec cette fonction, vous pouvez rationaliser la création de pool car vous n'avez pas à saisir chaque option dans l'assistant Ajouter un pool de postes de travail. Vous pouvez vous assurer que les attributs du pool de postes de travail sont normalisés en utilisant les valeurs préremplies dans l'assistant.

Vous pouvez cloner des pools de postes de travail automatisés qui contiennent des machines virtuelles complètes ou des clones liés View Composer. Vous ne pouvez pas cloner des pools de postes de travail automatisés de clones instantanés, des pools de postes de travail manuels ou des pools de postes de travail RDS.

Lorsque vous clonez un pool de postes de travail, vous ne pouvez pas modifier certains paramètres :

- Type de pool de postes de travail
- Type de clone : clone lié ou machine virtuelle complète
- Affectation d'utilisateur : dédiée ou flottante
- Instance de vCenter Server

### Prérequis

- Vérifiez que les conditions préalables pour créer le pool de postes de travail d'origine sont toujours valides.

  Par exemple, pour un pool qui contient des machines virtuelles complètes, vérifiez qu'un modèle de machine virtuelle a été préparé.

  Pour un pool de clone lié, vérifiez qu'une machine virtuelle parente a été préparée et qu'un snapshot a été pris après la désactivation de la machine virtuelle.

  Lorsque vous clonez un pool, vous pouvez utiliser le même modèle de machine virtuelle ou la même machine virtuelle parente, ou vous pouvez en sélectionner un ou une autre.
- Pour connaître les conditions préalables pour cloner un pool de clone complet automatisé, reportez-vous à la section « Créer un pool automatisé contenant des machines virtuelles complètes », page 66.
- Pour connaître les conditions préalables pour cloner un pool de clone lié, reportez-vous à la section « Créer un pool de postes de travail de clone lié », page 82.

### Procédure

1. Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.
2. Sélectionnez le pool de postes de travail que vous voulez cloner et cliquez sur **Cloner**.

   L'assistant Ajouter un pool de postes de travail s'affiche.
3. Sur la page Ajouter un pool de postes de travail, saisissez un ID de pool unique.

4 Sur la page Paramètres d'approvisionnement, fournissez des noms uniques pour les machines virtuelles.

| Option | Description |
|---|---|
| **Utiliser un mode d'attribution de nom** | Saisissez un mode d'attribution de nom aux machines virtuelles. |
| **Spécifier des noms manuellement** | Fournissez une liste de noms uniques pour les machines virtuelles. |

5 Suivez les autres invites de l'assistant pour créer le pool.

Modifiez les paramètres et les valeurs du pool de postes de travail si nécessaire.

Dans View Administrator, vous pouvez afficher les machines à mesure de leur ajout au pool en sélectionnant **Catalogue > Pools de postes de travail**.

### Suivant

Autorisez les utilisateurs à accéder au pool. Reportez-vous à la section « Ajouter des droits d'accès à un pool de postes de travail ou d'applications », page 187.

## Paramètres de poste de travail pour des pools automatisés contenant des machines virtuelles complètes

Vous devez spécifier des paramètres de pool de postes de travail lorsque vous configurez des pools automatisés contenant des machines virtuelles complètes. Différents paramètres s'appliquent à des pools avec des affectations d'utilisateur dédiées et flottantes.

Tableau 4-2 répertorie les paramètres qui s'appliquent à des pools automatisés avec des affectations dédiées et flottantes.

Pour voir des descriptions de chaque paramètre de pools de postes de travail, reportez-vous à la section « Paramètres de pools de postes de travail pour tous les types de pools de postes de travail », page 160

**Tableau 4-2.** Paramètres des pools automatisés contenant des machines virtuelles complètes

| Paramètre | Pool automatisé, affectation dédiée | Pool automatisé, affectation flottante |
|---|---|---|
| État | Oui | Oui |
| Restrictions du serveur de connexion | Oui | Oui |
| Stratégie d'alimentation de machine distante | Oui | Oui |
| Automatic logoff after disconnect (Fermeture de session automatique après la déconnexion) | Oui | Oui |
| Autoriser les utilisateurs à réinitialiser leurs machines | Oui | Oui |
| Autoriser l'utilisateur à ouvrir des sessions séparées depuis différents périphériques clients | | Oui |
| Supprimer la machine après la fermeture de session | | Oui |
| Protocole d'affichage par défaut | Oui | Oui |
| Autoriser les utilisateurs à choisir un protocole | Oui | Oui |
| Convertisseur 3D | Oui | Oui |

**Tableau 4-2.** Paramètres des pools automatisés contenant des machines virtuelles complètes (suite)

| Paramètre | Pool automatisé, affectation dédiée | Pool automatisé, affectation flottante |
|---|---|---|
| Max number of monitors (Nombre max. d'écrans) | Oui | Oui |
| Max resolution of any one monitor (Résolution max. d'un écran) | Oui | Oui |
| Adobe Flash quality (Qualité Adobe Flash) | Oui | Oui |
| Adobe Flash throttling (Limitation d'Adobe Flash) | Oui | Oui |
| Remplacer les paramètres de Mirage | Oui | Oui |
| Configuration du serveur Mirage | Oui | Oui |

# Création de pools de postes de travail de clone lié

5

Avec un pool de postes de travail de clone lié, View crée un pool de postes de travail basé sur une machine virtuelle parente que vous sélectionnez. Le service View Composer crée dynamiquement une nouvelle machine virtuelle de clone lié dans vCenter Server pour chaque poste de travail.

Ce chapitre aborde les rubriques suivantes :



## Pools de postes de travail de clone lié

Pour créer un pool de postes de travail de clone lié, View Composer génère des machines virtuelles de clone lié depuis un snapshot d'une machine virtuelle parente. View provisionne dynamiquement les postes de travail de clone lié en fonction des paramètres que vous appliquez au pool.

Comme les postes de travail de clone lié partagent une image du disque système de base, ils utilisent moins de stockage que les machines virtuelles complètes.

## Feuille de calcul pour créer un pool de postes de travail de clone lié

Lorsque vous créez un pool de postes de travail de clone lié, l'assistant Ajouter un pool de postes de travail de View Administrator vous invite à configurer certaines options. Utilisez cette feuille de calcul pour préparer vos options de configuration avant de créer le pool.

Vous pouvez imprimer cette feuille de calcul et noter les valeurs que vous souhaitez spécifier quand vous exécutez l'assistant Ajouter un pool de postes de travail.

Avant de créer un pool de clone lié, vous devez utiliser vCenter Server pour prendre un snapshot de la machine virtuelle parente que vous préparez pour le pool. Vous devez éteindre la machine virtuelle parente avant de prendre le snapshot. View Composer utilise le snapshot comme image de base depuis laquelle les clones sont créés.

**Remarque** Vous ne pouvez pas créer de pool de clone lié depuis un modèle de machine virtuelle.

**Tableau 5-1.** Feuille de calcul : options de configuration pour la création d'un pool de postes de travail de clone lié

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| Affectation d'utilisateur | Choisissez le type d'affectation d'utilisateur :<br>■ Dans un pool à attribution dédiée, une machine est attribuée à chaque utilisateur. Les utilisateurs reçoivent la même machine chaque fois qu'ils ouvrent une session.<br>■ Dans un pool à attribution flottante, les utilisateurs reçoivent des machines différentes chaque fois qu'ils ouvrent une session.<br>Pour plus d'informations, reportez-vous à « Affectation d'utilisateur dans des pools de postes de travail », page 151. | |
| Activer l'affectation automatique | Dans un pool à attribution dédiée, une machine est attribuée à un utilisateur lorsque celui-ci se connecte pour la première fois au pool. Vous pouvez également attribuer des machines aux utilisateurs de manière explicite.<br>Si vous n'activez pas l'attribution automatique, vous devez attribuer une machine à chaque utilisateur de manière explicite. | |
| vCenter Server | Sélectionnez le serveur vCenter Server qui gère les machines virtuelles dans le pool. | |
| ID du pool de postes de travail | Nom unique qui identifie le pool dans View Administrator.<br>Si plusieurs configurations du Serveur de connexion View sont exécutées dans votre environnement, assurez-vous qu'aucune autre configuration du Serveur de connexion View n'utilise le même ID de pool.<br>Une configuration du Serveur de connexion View peut être une instance autonome du Serveur de connexion View ou un espace d'instances répliquées partageant une configuration commune de View LDAP. | |
| Nom d'affichage | Nom du pool que les utilisateurs voient lorsqu'ils se connectent à partir d'un périphérique client. Si vous ne spécifiez pas de nom d'affichage, l'ID de pool est affiché aux utilisateurs. | |

**Tableau 5-1.** Feuille de calcul : options de configuration pour la création d'un pool de postes de travail de clone lié (suite)

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| Groupe d'accès | Sélectionnez un groupe d'accès dans lequel placer le pool ou laissez ce dernier dans le groupe d'accès racine par défaut.<br>Si vous utilisez un groupe d'accès, vous pouvez déléguer la gestion du pool à un administrateur avec un rôle spécifique. Pour plus d'informations, reportez-vous au chapitre consacré à l'administration déléguée basée sur des rôles du document *Administration de View*.<br>**Remarque** Les groupes d'accès sont différents des dossiers vCenter Server qui stockent les machines virtuelles utilisées en tant que postes de travail. Vous sélectionnez un dossier vCenter Server plus tard dans l'assistant avec d'autres paramètres de vCenter Server. | |
| Supprimer ou actualiser la machine à la fermeture de session | Si vous sélectionnez l'attribution d'utilisateurs flottante, indiquez s'il convient d'actualiser les machines, de les supprimer ou de ne rien faire après que les utilisateurs se déconnectent.<br>**Remarque** Vous définissez cette option sur la page Paramètres de pool de postes de travail. | |
| Paramètres du pool de postes de travail | Paramètres qui déterminent l'état de la machine, l'état d'alimentation lorsqu'une machine virtuelle n'est pas utilisée, le protocole d'affichage, la qualité Adobe Flash, etc.<br>Pour obtenir une description, reportez-vous à « Paramètres de pools de postes de travail pour tous les types de pools de postes de travail », page 160.<br>Pour obtenir la liste des paramètres s'appliquant aux pools de clone lié, reportez-vous à « Paramètres de pool de postes de travail pour des pools de postes de travail de clone lié », page 85.<br>Pour plus d'informations sur les stratégies d'alimentation et les pools automatisés, reportez-vous à « Définition de règles d'alimentation pour des pools de postes de travail », page 165. | |
| Arrêter l'approvisionnement en cas d'erreur | Vous pouvez faire en sorte qu'View arrête ou continue le provisionnement des machines virtuelles dans un pool de postes de travail suite à une erreur survenue au cours du provisionnement d'une machine virtuelle. Si vous laissez ce paramètre sélectionné, vous pouvez empêcher qu'une erreur de provisionnement se répète sur plusieurs machines virtuelles. | |
| Virtual machine naming (Attribution de nom aux machines virtuelles) | Indiquez si vous souhaitez provisionner des machines en spécifiant manuellement la liste des noms de machines ou en indiquant un mode d'attribution de nom et le nombre total de machines.<br>Pour plus d'informations, reportez-vous à « Dénomination manuelle de machines ou fourniture d'un mode d'attribution de nom », page 152. | |
| Spécifier des noms manuellement | Si vous spécifiez les noms manuellement, préparez la liste des noms de machines et, éventuellement, les noms d'utilisateurs associés. | |

**Tableau 5-1.** Feuille de calcul : options de configuration pour la création d'un pool de postes de travail de clone lié (suite)

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| Mode d'attribution de nom | Si vous utilisez cette méthode de nommage, fournissez le mode.<br>Le modèle que vous spécifiez est utilisé en tant que préfixe dans tous les noms de machines, suivi d'un numéro unique identifiant chaque machine.<br>Pour plus d'informations, reportez-vous à « Utilisation d'un mode d'attribution de nom pour des pools de postes de travail automatisés », page 155. | |
| Nombre max. de machines | Si vous utilisez un mode d'attribution de nom, spécifiez le nombre total de machines dans le pool.<br>Vous pouvez également spécifier un nombre minimal de machines à provisionner lorsque vous créez le pool. | |
| Nombre de machines de rechange (sous tension) | Si vous spécifiez les noms manuellement ou si vous utilisez un mode d'attribution de nom, indiquez un nombre de machines à garder à disposition et sous tension pour les nouveaux utilisateurs. Pour plus d'informations, reportez-vous à « Dénomination manuelle de machines ou fourniture d'un mode d'attribution de nom », page 152.<br>Lorsque vous spécifiez les noms manuellement, cette option est appelée **Nb de machines non affectées maintenues sous tension**. | |
| Nombre minimal de machines prêtes (provisionnées) pendant les opérations de maintenance de View Composer | Si vous spécifiez les noms manuellement ou si vous utilisez un mode d'attribution de nom, spécifiez un nombre minimal de machines provisionnées pour une utilisation dans des sessions de poste de travail distant pendant l'exécution des opérations de maintenance de View Composer.<br>Ce paramètre permet aux utilisateurs de maintenir des connexions existantes ou de faire de nouvelles demandes de connexion pendant que View Composer actualise, recompose ou rééquilibre les machines dans le pool. Le paramètre ne fait pas la différence entre les machines de rechange qui sont prêtes à accepter les nouvelles connexions et les machines qui sont déjà connectées dans des sessions de poste de travail existantes.<br>Cette valeur doit être inférieure au **Nombre max. de machines** que vous spécifiez si vous provisionnez des machines à la demande.<br>Reportez-vous à la section « Maintien des machines de clone lié provisionnées pour une utilisation dans des sessions de poste de travail distant au cours d'opérations de View Composer », page 91. | |

**Tableau 5-1.** Feuille de calcul : options de configuration pour la création d'un pool de postes de travail de clone lié (suite)

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| Provisionner des machines à la demande<br>ou<br>Provisionner toutes les machines à l'avance | Si vous utilisez un mode d'attribution de nom, indiquez s'il convient de provisionner toutes les machines lors de la création du pool ou en fonction des besoins.<br>■ **Provisionner toutes les machines à l'avance**. À la création du pool, le système provisionne le nombre de machines que vous spécifiez dans **Nombre max. de machines**.<br>■ **Provisionner des machines à la demande**. À la création du pool, le système crée le nombre de machines que vous spécifiez dans **Nombre min. de machines**. Des machines supplémentaires sont créées lorsque les utilisateurs se connectent au pool pour la première fois ou lorsque vous leur attribuez des machines. | |
| Nombre min. de machines | Si vous utilisez un mode d'attribution de nom et que vous provisionnez les postes de travail à la demande, spécifiez un nombre minimal de machines dans le pool.<br>Le système crée le nombre minimal de machines lorsque vous créez le pool. Ce nombre est conservé même si d'autres paramètres, comme **Supprimer ou actualiser la machine à la fermeture de session**, entraînent la suppression de machines. | |
| Rediriger un profil Windows vers un disque persistant | Si vous sélectionnez des affectations d'utilisateur dédiées, choisissez si vous voulez stocker des données de profil d'utilisateur Windows sur un disque persistant séparé de View Composer ou sur le même disque que les données du système d'exploitation.<br>Les disques persistants séparés vous permettent de conserver des données et des paramètres d'utilisateur. Les opérations d'actualisation, de recomposition et de rééquilibrage de View Composer n'affectent pas les disques persistants. Vous pouvez détacher un disque persistant d'un clone lié et recréer la machine virtuelle de clone lié à partir du disque détaché. Par exemple, lorsqu'une machine ou un pool est supprimé, vous pouvez détacher le disque persistant et recréer le poste de travail, préservant ainsi les données et les paramètres de l'utilisateur d'origine.<br>Si vous stockez le profil Windows sur le disque du système d'exploitation, les données et les paramètres d'utilisateur sont supprimés au cours des opérations d'actualisation, de recomposition et de rééquilibrage. | |
| Disk size and drive letter for persistent disk (Taille et lettre des disques persistants) | Si vous stockez des données de profil d'utilisateur sur un disque persistant séparé de View Composer, fournissez la taille du disque en mégaoctets et la lettre du lecteur.<br>**Remarque** Ne sélectionnez pas de lettre de lecteur qui existe déjà sur la machine virtuelle parente ou qui entre en conflit avec une lettre de lecteur utilisée pour un lecteur monté en réseau. | |

**Tableau 5-1.** Feuille de calcul : options de configuration pour la création d'un pool de postes de travail de clone lié (suite)

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| Redirection de fichier supprimable | Choisissez si vous voulez rediriger les fichiers d'échange et temporaires du système d'exploitation client sur un disque non persistant séparé. Si vous le faites, fournissez la taille de disque en mégaoctets.<br>Avec cette configuration, lorsqu'un clone lié est hors tension, le disque de fichier supprimable est remplacé par une copie du disque d'origine qui a été créée avec le pool de clone lié. La taille des clones liés peut augmenter à mesure que les utilisateurs interagissent avec leurs postes de travail. La redirection du fichier supprimable peut économiser de l'espace de stockage en ralentissant la croissance des clones liés. | |
| Taille et lettre des disques de fichier supprimables | Si vous redirigez des fichiers supprimables vers un disque non persistant, fournissez la taille du disque en mégaoctets et la lettre du lecteur.<br>La taille de disque doit être supérieure à la taille du fichier d'échange du système d'exploitation client. Pour déterminer la taille du fichier d'échange, reportez-vous à « Enregistrer la taille du fichier de pagination d'une machine virtuelle parente View Composer », page 58.<br>Lorsque vous configurez la taille du disque de fichier supprimable, prenez bien en considération que la taille réelle d'une partition de disque formaté est légèrement plus petite que la valeur que vous fournissez dans View Administrator.<br>Vous pouvez sélectionner une lettre de lecteur pour le disque de fichier supprimable. La valeur par défaut, **Auto**, demande à View d'affecter la lettre de lecteur.<br>**Remarque** Ne sélectionnez pas de lettre de lecteur qui existe déjà sur la machine virtuelle parente ou qui entre en conflit avec une lettre de lecteur utilisée pour un lecteur monté en réseau. | |
| Utiliser vSphere Virtual SAN | Spécifiez si vous souhaitez utiliser VMware Virtual SAN, le cas échéant. Virtual SAN est une couche de stockage définie par logiciel qui virtualise les disques de stockage physique locaux disponibles sur un cluster d'hôtes ESXi. Pour plus d'informations, reportez-vous à la section « Utilisation de Virtual SAN pour un stockage haute performance et une gestion basée sur les stratégies », page 273. | |
| Sélectionner des magasins de données séparés pour les disques persistants et du système d'exploitation | (Disponible uniquement si vous n'utilisez pas Virtual SAN) Si vous redirigez les profils utilisateurs vers des disques persistants distincts, vous pouvez stocker ceux-ci, ainsi que les disques du système d'exploitation, sur des banques de données distinctes. | |

**Tableau 5-1.** Feuille de calcul : options de configuration pour la création d'un pool de postes de travail de clone lié (suite)

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| Sélectionner des magasins de données séparés pour les disques de réplication et du système d'exploitation | (Disponible uniquement si vous n'utilisez pas Virtual SAN ou Virtual Volumes) Vous pouvez stocker le disque de machine virtuelle de réplication (maître) sur une banque de données haute performance et les clones liés sur des banques de données distinctes.<br>Pour plus d'informations, reportez-vous à « Stockage de réplicas et de clones sur des magasins de données séparés pour des clones instantanés et des clones liés View Composer », page 289.<br>Si vous stockez des réplicas et des disques du système d'exploitation sur des magasins de données séparés, des snapshots NFS natifs ne peuvent pas être utilisés. Le clonage natif sur un périphérique NAS ne peut avoir lieu que si les disques de réplica et du système d'exploitation sont stockés sur les mêmes magasins de données. | |
| Machine virtuelle parente | Sélectionnez la machine virtuelle parente du pool. | |
| Snapshot (image par défaut) | Sélectionnez le snapshot de la machine virtuelle parente à utiliser comme image de base pour le pool.<br>Ne supprimez pas le snapshot et la machine virtuelle parente de vCenter Server, sauf si aucun clone lié dans le pool n'utilise l'image par défaut, et si aucun autre clone lié ne sera créé à partir de cette image par défaut. Le système requiert que la machine virtuelle parente et le snapshot provisionnent les nouveaux clones liés dans le pool, conformément aux stratégies du pool. La machine virtuelle parente et le snapshot sont également requis pour les opérations de maintenance de View Composer. | |
| Emplacement du dossier de machine virtuelle | Sélectionnez le dossier dans vCenter Server dans lequel réside le pool de postes de travail. | |
| Host or cluster (Hôte ou cluster) | Sélectionnez l'hôte ou le cluster ESXi sur lequel les machines virtuelles de poste de travail s'exécutent.<br>Avec des banques de données Virtual SAN (fonctionnalité de vSphere 5.5 Update 1), vous pouvez sélectionner un cluster contenant jusqu'à 20 hôtes ESXi. Avec des banques de données Virtual Volumes (fonctionnalité de vSphere 6.0), vous pouvez sélectionner un cluster contenant jusqu'à 32 hôtes ESXi.<br>Dans vSphere 5.1 ou supérieur, vous pouvez sélectionner un cluster contenant jusqu'à 32 hôtes ESXi si les réplicas sont stockés sur des magasins de données VMFS5 ou supérieur ou sur des magasins de données NFS. Si vous stockez les réplicas sur une version VMFS antérieure à VMFS5, un cluster peut contenir 8 hôtes au maximum.<br>Dans vSphere 5.0, vous pouvez sélectionner un cluster avec plus de 8 hôtes ESXi si les réplicas sont stockés sur des magasins de données NFS. Si vous stockez les réplicas sur des magasins de données VMFS, un cluster peut contenir au maximum 8 hôtes. Reportez-vous à la section « Configuration de pools de postes de travail sur des clusters comportant plus de huit hôtes », page 184. | |
| Resource pool (Pool de ressources) | Sélectionnez le pool de ressources de vCenter Server dans lequel le pool de postes de travail réside. | |

**Tableau 5-1.** Feuille de calcul : options de configuration pour la création d'un pool de postes de travail de clone lié (suite)

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| Magasins de données | Sélectionnez un ou plusieurs magasins de données sur lesquels stocker le pool de postes de travail.<br>Sur la page Sélectionner des banques de données de clone lié de l'assistant Ajouter un pool de postes de travail, un tableau fournit des recommandations pour estimer les besoins en stockage du pool. Ces recommandations peuvent vous aider à déterminer les magasins de données assez volumineux pour stocker les disques de clone lié. Pour plus d'informations, reportez-vous à « Dimensionnement du stockage pour des pools de postes de travail de clone instantané et de clone lié View Composer », page 280.<br>Vous pouvez utiliser des magasins de données partagés ou locaux pour un hôte ESXi individuel ou pour des clusters ESXi. Si vous utilisez des magasins de données locaux dans un cluster ESXi, vous devez prendre en compte les contraintes de l'infrastructure vSphere qui sont imposées sur votre déploiement de poste de travail. Reportez-vous à la section « Stockage de clones liés View Composer sur des magasins de données locaux », page 288.<br>Avec des banques de données Virtual SAN (fonctionnalité de vSphere 5.5 Update 1), vous pouvez sélectionner un cluster contenant jusqu'à 20 hôtes ESXi. Avec des banques de données Virtual Volumes (fonctionnalité de vSphere 6.0), vous pouvez sélectionner un cluster contenant jusqu'à 32 hôtes ESXi.<br>Dans vSphere 5.1 ou supérieur, un cluster peut contenir plus de huit hôtes ESXi si les réplicas sont stockés sur des magasins de données VMFS5 ou supérieur ou NFS. Dans vSphere 5.0, un cluster peut contenir plus de huit hôtes ESXi uniquement si les réplicas sont stockés sur des magasins de données NFS. Reportez-vous à la section « Configuration de pools de postes de travail sur des clusters comportant plus de huit hôtes », page 184.<br>Pour plus d'informations sur les disques créés pour des clones liés, reportez-vous à « Disques de données de clone lié View Composer », page 287.<br>**Remarque** Si vous utilisez Virtual SAN, sélectionnez une seule banque de données. | |
| Surcharge du stockage | Déterminez le niveau de surcharge du stockage auquel les clones liés sont créés sur chaque banque de données.<br>À mesure que le niveau augmente, plus de clones liés sont placés sur le magasin de données et moins d'espace est réservé pour la croissance des clones individuels. Un niveau de surcharge du stockage élevé vous permet de créer des clones liés ayant une taille logique totale supérieure à la limite de stockage physique du magasin de données. Pour plus d'informations, reportez-vous à « Définir le niveau de surcharge du stockage pour des machines virtuelles de clone lié », page 286.<br>**Remarque** Ce paramètre n'a aucun effet si vous utilisez Virtual SAN. | |

**Tableau 5-1.** Feuille de calcul : options de configuration pour la création d'un pool de postes de travail de clone lié (suite)

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| Utiliser View Storage Accelerator | Déterminez si vous voulez utiliser View Storage Accelerator, ce qui permet aux hôtes ESXi de mettre en cache des données de disque de machine virtuelle communes. View Storage Accelerator peut améliorer les performances et réduire le besoin de bande passante d'E/S de stockage supplémentaire pour gérer des tempêtes de démarrage et des tempêtes d'E/S d'analyse antivirus.<br>Cette fonction est prise en charge sur vSphere 5.0 et supérieur.<br>Cette fonction est activée par défaut.<br>Pour plus d'informations, reportez-vous à « Configurer View Storage Accelerator des clones liés View Composer », page 290. | |
| Utiliser des snapshots NFS natifs (VAAI) | (Disponible uniquement si vous n'utilisez pas Virtual SAN) Si votre déploiement inclut des périphériques NAS prenant en charge la technologie VAAI (vStorage APIs for Array Integration), vous pouvez utiliser la technologie de snapshot native pour cloner des machines virtuelles.<br>Vous pouvez utiliser cette fonction uniquement si vous sélectionnez des magasins de données résidant sur des périphériques NAS prenant en charge les opérations de clonage natif via VAAI.<br>Vous ne pouvez pas utiliser cette fonction si vous stockez des réplicas et des disques du système d'exploitation sur des magasins de données séparés. Vous ne pouvez pas utiliser cette fonctionnalité sur les machines virtuelles intégrant des disques à optimisation d'espace.<br>Cette fonction est prise en charge sur vSphere 5.0 et supérieur.<br>Pour plus d'informations, reportez-vous à « Utilisation du stockage VAAI des clones liés View Composer », page 294. | |
| Récupérer l'espace disque de machine virtuelle | (Disponible uniquement si vous n'utilisez pas Virtual SAN ou Virtual Volumes) Déterminez si vous souhaitez autoriser des hôtes ESXi à récupérer l'espace disque non utilisé sur les clones liés qui sont créés au format de disque à optimisation d'espace. La fonction de récupération d'espace réduit l'espace de stockage total requis pour les postes de travail de clone lié.<br>Cette fonction est prise en charge sur vSphere 5.1 et supérieur. Les machines virtuelles de clone lié doivent avoir la version matérielle virtuelle 9 ou supérieure.<br>Pour plus d'informations, reportez-vous à « Récupérer l'espace disque sur des clones liés View Composer », page 292. | |

**Tableau 5-1.** Feuille de calcul : options de configuration pour la création d'un pool de postes de travail de clone lié (suite)

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| Initier la récupération lorsque l'espace inutilisé de la machine virtuelle dépasse : | (Disponible uniquement si vous n'utilisez pas Virtual SAN ou Virtual Volumes) Tapez le volume minimal d'espace disque inutilisé, en giga-octets, qui doit s'accumuler sur un disque du système d'exploitation de clone lié pour déclencher la récupération d'espace. Lorsque l'espace disque inutilisé dépasse ce seuil, View initie l'opération qui demande à l'hôte ESXi de récupérer l'espace sur le disque du système d'exploitation.<br>Cette valeur est mesurée par machine virtuelle. L'espace disque inutilisé doit dépasser le seuil spécifié sur une machine virtuelle individuelle pour que View démarre le processus de récupération d'espace sur cette machine.<br>Par exemple : **2** Go.<br>La valeur par défaut est 1 Go. | |
| Durée d'interruption | Configurez les jours et les heures auxquels la régénération View Storage Accelerator et la récupération de l'espace disque de machine virtuelle n'ont pas lieu.<br>Pour vous assurer que des ressources ESXi sont dédiées à des tâches de premier plan lorsque cela est nécessaire, vous pouvez empêcher les hôtes ESXi d'exécuter ces opérations pendant des périodes de temps spécifiées certains jours.<br>Pour plus d'informations, reportez-vous à « Définir les durées d'interruption de Storage Accelerator et de récupération d'espace des clones liés View Composer », page 295. | |
| Portée du partage de page transparente (Transparent Page Sharing) | Sélectionnez le niveau auquel autoriser le partage de page transparente (TPS). Les choix sont **Machine virtuelle** (par défaut), **Pool**, **Espace** ou **Global**. Si vous activez le partage de page transparente pour les machines du pool, de l'espace ou globalement, l'hôte ESXi élimine les copies redondantes des pages mémoire obtenues si les machines utilisent le même système d'exploitation invité ou les mêmes applications.<br>Le partage de page se produit sur l'hôte ESXi. Par exemple, si vous activez le partage de page transparente au niveau du pool alors que le pool couvre plusieurs hôtes ESXi, seules les machines virtuelles sur le même hôte et à l'intérieur du même pool partageront des pages. Au niveau global, toutes les machines gérées par View sur le même hôte ESXi peuvent partager des pages de mémoire, quel que soit le pool sur lequel résident les machines.<br>**Remarque** Par défaut, les pages de mémoire ne sont pas partagées entre plusieurs machines, car le partage de page transparente (TPS) peut créer un risque. Les recherches indiquent que le partage de page transparente peut être exploité de façon abusive pour obtenir un accès non autorisé à des données dans des scénarios de configuration très limités. | |

**Tableau 5-1.** Feuille de calcul : options de configuration pour la création d'un pool de postes de travail de clone lié (suite)

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| Domaine | Sélectionnez le domaine Active Directory et le nom d'utilisateur.<br>View Composer requiert certains privilèges d'utilisateur pour créer un pool de clone lié. Domaine et compte d'utilisateur utilisés par QuickPrep ou Sysprep pour personnaliser les machines de clone lié.<br>Vous spécifiez cet utilisateur lorsque vous configurez des paramètres de View Composer pour vCenter Server. Vous pouvez spécifier plusieurs domaines et utilisateurs lorsque vous configurez les paramètres de View Composer. Lorsque vous utilisez l'assistant Ajouter un pool de postes de travail pour créer un pool, vous devez sélectionner un domaine et un utilisateur dans la liste.<br>Pour plus d'informations sur la configuration de View Composer, reportez-vous au document *Administration de View*. | |
| Conteneur Active Directory | Fournissez le nom unique relatif du conteneur Active Directory.<br>Par exemple : **`CN=Ordinateurs`**<br>Lorsque vous exécutez l'assistant Ajouter un pool de postes de travail, vous pouvez parcourir l'arborescence d'Active Directory à la recherche du conteneur. | |
| Autoriser la réutilisation de comptes d'ordinateur pré-existants | Sélectionnez cette option pour utiliser des comptes d'ordinateur existants dans Active Directory pour des clones liés qui sont approvisionnés par View Composer. Cette option vous permet de contrôler les comptes d'ordinateur qui sont créés dans Active Directory.<br>Lorsqu'un clone lié est provisionné, si le nom d'un compte d'ordinateur Active Directory existant correspond au nom de la machine de clone lié, View Composer utilise le compte d'ordinateur existant. Sinon, un nouveau compte d'ordinateur est créé.<br>Les comptes d'ordinateur existants doivent être situés dans le conteneur Active Directory que vous spécifiez avec le paramètre **Conteneur Active Directory**.<br>Lorsque cette option est désactivée, un nouveau compte d'ordinateur AD est créé lorsque View Composer approvisionne un clone lié. Par défaut, cette option est désactivée.<br>Pour plus d'informations, reportez-vous à « Utiliser des comptes d'ordinateur Active Directory existants pour des clones liés », page 92. | |

**Tableau 5-1.** Feuille de calcul : options de configuration pour la création d'un pool de postes de travail de clone lié (suite)

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| Use QuickPrep or a customization specification (Sysprep) (Utiliser QuickPrep ou une spécification de personnalisation (Sysprep)) | Indiquez si vous souhaitez utiliser QuickPrep ou sélectionnez une spécification de personnalisation (Sysprep) pour configurer les paramètres de licence, d'association de domaine, de protocole DHCP et d'autres propriétés sur les machines.<br>Sysprep est pris en charge pour les clones liés uniquement sur le logiciel vSphere 4.1 ou supérieur.<br>Si vous avez utilisé QuickPrep ou Sysprep lors de la création d'un pool, vous ne pourrez pas passer à l'autre méthode de personnalisation ultérieurement lorsque vous créerez ou recomposerez des machines dans le pool.<br>Pour plus d'informations, reportez-vous à « Choisir QuickPrep ou Sysprep pour personnaliser des machines de clone lié », page 87. | |
| Power-off script (Script de désactivation) | QuickPrep peut exécuter un script de personnalisation sur les machines de clone lié avant qu'elles soient mises hors tension.<br>Fournissez le chemin d'accès au script sur la machine virtuelle parente et aux paramètres de script. | |
| Script de post-synchronisation | QuickPrep peut exécuter un script de personnalisation sur les machines de clone lié après leur création, leur recomposition et leur actualisation.<br>Fournissez le chemin d'accès au script sur la machine virtuelle parente et aux paramètres de script. | |

## Créer un pool de postes de travail de clone lié

Vous pouvez créer un pool de postes de travail de clone lié automatisé basé sur une machine virtuelle parente que vous sélectionnez. Le service View Composer crée dynamiquement une nouvelle machine virtuelle de clone lié dans vCenter Server pour chaque poste de travail.

Pour créer un pool automatisé contenant des machines virtuelles complètes, reportez-vous à la section « Pools automatisés contenant des machines virtuelles complètes », page 61

### Prérequis

- Vérifiez que le service View Composer est installé, sur le même hôte que vCenter Server ou sur un hôte séparé, et qu'une base de données View Composer est configurée. Reportez-vous au document *Installation de View*.
- Vérifiez que les paramètres de View Composer pour vCenter Server sont configurés dans View Administrator. Reportez-vous au document *Administration de View*.
- Vérifiez que vous disposez d'un nombre suffisant de ports sur le commutateur virtuel ESXi utilisé pour les machines virtuelles servant de postes de travail distants. La valeur par défaut peut ne pas être suffisante si vous créez des pools de postes de travail volumineux. Le nombre de ports de commutateur virtuel sur l'hôte ESXi doit être égal ou supérieur au nombre de machines virtuelles multiplié par le nombre de cartes réseau virtuelles par machine virtuelle.
- Vérifiez que vous avez préparé une machine virtuelle parente. Horizon Agent doit être installé sur la machine virtuelle parente. Reportez-vous à la section Chapitre 3, « Création et préparation d'une machine virtuelle parente pour le clonage », page 25.

- Prenez un snapshot de la machine virtuelle parente dans vCenter Server. Vous devez éteindre la machine virtuelle parente avant de prendre le snapshot. View Composer utilise le snapshot comme image de base depuis laquelle les clones sont créés.

  **Remarque** Vous ne pouvez pas créer de pool de clone lié depuis un modèle de machine virtuelle.

- Collectez les informations de configuration que vous devez fournir pour créer le pool. Reportez-vous à la section « Feuille de calcul pour créer un pool de postes de travail de clone lié », page 71.
- Décidez comment configurer les paramètres d'alimentation, le protocole d'affichage, la qualité Adobe Flash et d'autres paramètres. Reportez-vous à la section « Paramètres de pools de postes de travail pour tous les types de pools de postes de travail », page 160.
- Si vous prévoyez de fournir un accès à vos applications et postes de travail via VMware Identity Manager, assurez-vous de créer les pools d'applications et de postes de travail en tant qu'utilisateur disposant du rôle Administrateurs sur le groupe d'accès racine dans View Administrator. Si vous attribuez à l'utilisateur le rôle Administrateurs sur un groupe d'accès autre que le groupe d'accès racine, VMware Identity Manager ne reconnaîtra pas l'authentificateur SAML que vous configurez dans View et vous ne pourrez pas configurer le pool dans VMware Identity Manager.

**Important** Lors de la création d'un pool de clone lié, ne modifiez pas la machine virtuelle parente dans vCenter Server. Par exemple, ne convertissez pas la machine virtuelle parente en modèle. Le service View Composer requiert que la machine virtuelle parente reste dans un état statique et inchangé lors de la création du pool.

### Procédure

1. Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.
2. Cliquez sur **Ajouter**.
3. Sélectionnez **Pool de postes de travail automatisé**.
4. Sur la page vCenter Server, choisissez **Clones liés View Composer**.
5. Suivez les invites de l'assistant pour créer le pool.

   Utilisez les informations de configuration que vous avez collectées dans la feuille de calcul. Vous pouvez revenir directement à n'importe quelle page de l'assistant en cliquant sur le nom de page dans le volet de navigation.

   Sur la page **Paramètres de vCenter**, vous devez cliquer sur **Parcourir** et sélectionner les paramètres de vCenter Server en séquence. Vous ne pouvez pas ignorer un paramètre de vCenter Server :

   a. Machine virtuelle parente
   b. Snapshot
   c. Emplacement du dossier de machine virtuelle
   d. Host or cluster (Hôte ou cluster)
   e. Resource pool (Pool de ressources)
   f. Magasins de données

Dans View Administrator, vous pouvez afficher les machines à mesure de leur ajout au pool en sélectionnant **Catalogue > Pools de postes de travail**.

Les clones liés peuvent redémarrer une ou plusieurs fois lors de leur approvisionnement. Si un clone lié est dans un état d'erreur, le mécanisme de récupération automatique de View tente d'activer, ou d'arrêter et de redémarrer, le clone lié. Si des tentatives de récupération répétées échouent, le clone lié est supprimé.

View Composer crée également une machine virtuelle réplica qui sert d'image maître pour l'approvisionnement des clones liés. Pour réduire la consommation d'espace, le réplica est créé en tant que disque fin. Si toutes les machines virtuelles sont recomposées ou supprimées, et qu'aucun clone n'est lié au réplica, la machine virtuelle réplica est supprimée de vCenter Server.

Si vous ne stockez pas le réplica sur un magasin de données séparé, View Composer crée un réplica sur chaque magasin de données sur lequel des clones liés sont créés.

Si vous stockez le réplica sur un magasin de données séparé, un réplica est créé pour le pool entier, même lorsque des clones liés sont créés sur plusieurs magasins de données.

### Suivant

Autorisez les utilisateurs à accéder au pool. Reportez-vous à la section « Ajouter des droits d'accès à un pool de postes de travail ou d'applications », page 187.

## Cloner un pool de postes de travail automatisé

Vous pouvez cloner un pool de postes de travail automatisé à partir d'un pool existant. Lorsque vous clonez un pool, les paramètres du pool de postes de travail existant sont copiés dans l'assistant Ajouter un pool de postes de travail, ce qui vous permet de créer un pool sans avoir à remplir chaque paramètre manuellement.

Avec cette fonction, vous pouvez rationaliser la création de pool car vous n'avez pas à saisir chaque option dans l'assistant Ajouter un pool de postes de travail. Vous pouvez vous assurer que les attributs du pool de postes de travail sont normalisés en utilisant les valeurs préremplies dans l'assistant.

Vous pouvez cloner des pools de postes de travail automatisés qui contiennent des machines virtuelles complètes ou des clones liés View Composer. Vous ne pouvez pas cloner des pools de postes de travail automatisés de clones instantanés, des pools de postes de travail manuels ou des pools de postes de travail RDS.

Lorsque vous clonez un pool de postes de travail, vous ne pouvez pas modifier certains paramètres :

- Type de pool de postes de travail
- Type de clone : clone lié ou machine virtuelle complète
- Affectation d'utilisateur : dédiée ou flottante
- Instance de vCenter Server

### Prérequis

- Vérifiez que les conditions préalables pour créer le pool de postes de travail d'origine sont toujours valides.

  Par exemple, pour un pool qui contient des machines virtuelles complètes, vérifiez qu'un modèle de machine virtuelle a été préparé.

  Pour un pool de clone lié, vérifiez qu'une machine virtuelle parente a été préparée et qu'un snapshot a été pris après la désactivation de la machine virtuelle.

  Lorsque vous clonez un pool, vous pouvez utiliser le même modèle de machine virtuelle ou la même machine virtuelle parente, ou vous pouvez en sélectionner un ou une autre.
- Pour connaître les conditions préalables pour cloner un pool de clone complet automatisé, reportez-vous à la section « Créer un pool automatisé contenant des machines virtuelles complètes », page 66.
- Pour connaître les conditions préalables pour cloner un pool de clone lié, reportez-vous à la section « Créer un pool de postes de travail de clone lié », page 82.

### Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

2 Sélectionnez le pool de postes de travail que vous voulez cloner et cliquez sur **Cloner**.

L'assistant Ajouter un pool de postes de travail s'affiche.

3 Sur la page Ajouter un pool de postes de travail, saisissez un ID de pool unique.

4 Sur la page Paramètres d'approvisionnement, fournissez des noms uniques pour les machines virtuelles.

| Option | Description |
|---|---|
| **Utiliser un mode d'attribution de nom** | Saisissez un mode d'attribution de nom aux machines virtuelles. |
| **Spécifier des noms manuellement** | Fournissez une liste de noms uniques pour les machines virtuelles. |

5 Suivez les autres invites de l'assistant pour créer le pool.

Modifiez les paramètres et les valeurs du pool de postes de travail si nécessaire.

Dans View Administrator, vous pouvez afficher les machines à mesure de leur ajout au pool en sélectionnant **Catalogue > Pools de postes de travail**.

### Suivant

Autorisez les utilisateurs à accéder au pool. Reportez-vous à la section « Ajouter des droits d'accès à un pool de postes de travail ou d'applications », page 187.

## Paramètres de pool de postes de travail pour des pools de postes de travail de clone lié

Vous devez spécifier des paramètres de machine et de pool de postes de travail lorsque vous configurez des pools automatisés contenant des clones liés créés par View Composer. Différents paramètres s'appliquent à des pools avec des affectations d'utilisateur dédiées et flottantes.

Tableau 5-2 répertorie les paramètres qui s'appliquent à des pools de clone lié avec des affectations dédiées et flottantes.

Pour voir une description de chaque paramètre, reportez-vous à « Paramètres de pools de postes de travail pour tous les types de pools de postes de travail », page 160.

**Tableau 5-2.** Paramètres de pools de postes de travail de clone lié automatisés

| Paramètre | Pool de clone lié, affectation dédiée | Pool de clone lié, affectation flottante |
|---|---|---|
| État | Oui | Oui |
| Restrictions du serveur de connexion | Oui | Oui |
| Stratégie d'alimentation de machine distante | Oui | Oui |
| Automatically logoff after disconnect (Fermeture de session automatique après la déconnexion) | Oui | Oui |
| Autoriser les utilisateurs à réinitialiser leurs machines | Oui | Oui |
| Autoriser l'utilisateur à ouvrir des sessions séparées depuis différents périphériques clients | | Oui |
| Supprimer ou actualiser la machine à la fermeture de session | | Oui |

**Tableau 5-2.** Paramètres de pools de postes de travail de clone lié automatisés (suite)

| Paramètre | Pool de clone lié, affectation dédiée | Pool de clone lié, affectation flottante |
|---|---|---|
| Actualiser le disque du système d'exploitation après la fermeture de session | Oui | |
| Protocole d'affichage par défaut | Oui | Oui |
| Autoriser les utilisateurs à choisir un protocole | Oui | Oui |
| Convertisseur 3D | Oui | Oui |
| Max number of monitors (Nombre max. d'écrans) | Oui | Oui |
| Max resolution of any one monitor (Résolution max. d'un écran) | Oui | Oui |
| Adobe Flash quality (Qualité Adobe Flash) | Oui | Oui |
| Adobe Flash throttling (Limitation d'Adobe Flash) | Oui | Oui |
| Remplacer les paramètres de Mirage | Oui | Oui |
| Configuration du serveur Mirage | Oui | Oui |

## Prise en charge de View Composer pour les SID de clone lié et les applications tierces

View Composer peut générer et conserver des ID de sécurité (SID) d'ordinateur local pour des machines virtuelles de clone lié dans certaines situations. View Composer peut conserver des identificateurs globaux uniques (GUID) d'applications tierces, en fonction de la façon dont les applications génèrent des GUID.

Pour comprendre comment les opérations de View Composer affectent les SID et les GUID des applications, vous devez comprendre comment les machines de clone lié sont créées et provisionnées :

1. View Composer crée un clone lié en effectuant ces actions :
   a. Il crée le réplica en clonant le snapshot de machine virtuelle parente.
   b. Il crée le clone lié pour faire référence au réplica comme son disque parent.
2. View Composer et View personnalisent le clone lié avec QuickPrep ou une spécification de personnalisation Sysprep, en fonction de l'outil de personnalisation que vous sélectionnez lors de la création du pool.
   - Si vous utilisez Sysprep, un SID unique est généré pour chaque clone.
   - Si vous utilisez QuickPrep, aucun nouveau SID n'est généré. Le SID de la machine virtuelle parente est répliqué sur toutes les machines de clone lié provisionnées du pool.
   - Certaines applications génèrent un GUID au cours de la personnalisation.
3. View crée un snapshot du clone lié.

   Le snapshot contient le SID unique généré avec Sysprep ou un SID commun généré avec QuickPrep.
4. View met sous tension la machine en fonction des paramètres que vous sélectionnez lors de la création du pool.

   Certaines applications génèrent un GUID lors de la première mise sous tension de la machine.

Pour voir une comparaison des personnalisations QuickPrep et Sysprep, reportez-vous à « Choisir QuickPrep ou Sysprep pour personnaliser des machines de clone lié », page 87.

Lorsque vous actualisez le clone lié, View Composer utilise le snapshot pour restaurer le clone à son état initial. Son SID est conservé.

Si vous utilisez QuickPrep, lorsque vous recomposez le clone lié, le SID de la machine virtuelle parente est conservé sur le clone lié tant que vous sélectionnez la même machine virtuelle parente pour l'opération de recomposition. Si vous sélectionnez une machine virtuelle parente différente pour la recomposition, le SID du nouveau parent est répliqué sur le clone.

Si vous utilisez Sysprep, un nouveau SID est toujours généré sur le clone. Pour plus d'informations, reportez-vous à « Recomposition de clones liés personnalisés avec Sysprep », page 90.

Tableau 5-3 montre l'effet des opérations de View Composer sur les SID de clones liés et les GUID d'applications tierces.

**Tableau 5-3.** Opérations de View Composer, SID de clone lié et GUID d'application

| Prise en charge de SID ou de GUID | Création de clone | Actualiser | Recomposer |
|---|---|---|---|
| Sysprep : SID uniques pour clones liés | Avec la personnalisation Sysprep, des SID uniques sont générés pour des clones liés. | Les SID uniques sont conservés. | Les SID uniques ne sont pas conservés. |
| QuickPrep : SID communs pour clones liés | Avec la personnalisation QuickPrep, un SID commun est généré pour tous les clones d'un pool. | Le SID commun est conservé. | Le SID commun est conservé. |
| GUID d'application tierce | Chaque application se comporte différemment.<br>REMARQUE Sysprep et QuickPrep ont le même effet sur la conservation de GUID. | Le GUID est conservé si une application génère le GUID avant la prise du snapshot initial.<br>Le GUID n'est pas conservé si une application génère le GUID après la prise du snapshot initial. | Les opérations de recomposition ne conservent pas de GUID d'application sauf si l'application inscrit le GUID sur le lecteur spécifié en tant que disque persistant de View Composer. |

## Choisir QuickPrep ou Sysprep pour personnaliser des machines de clone lié

QuickPrep et Microsoft Sysprep offrent différentes méthodes pour personnaliser des machines de clone lié. QuickPrep est conçu pour fonctionner efficacement avec View Composer. Microsoft Sysprep offre des outils de personnalisation standard.

Lorsque vous créez des machines de clone lié, vous devez modifier chaque machine virtuelle pour qu'elle puisse fonctionner en tant qu'ordinateur unique sur le réseau. View Manager et View Composer offrent deux méthodes pour personnaliser des machines de clone lié.

Tableau 5-4 compare QuickPrep avec des spécifications de personnalisation créées avec Microsoft Sysprep.

**Tableau 5-4.** Comparaison de QuickPrep et Microsoft Sysprep

| QuickPrep | Spécification de personnalisation (Sysprep) |
|---|---|
| Conçu pour fonctionner avec View Composer.<br>Pour plus d'informations, reportez-vous à « Personnalisation de machines de clone lié avec QuickPrep », page 88. | Peut être créée avec les outils Microsoft Sysprep standard. |
| Utilise le même ID de sécurité (SID) de l'ordinateur local pour tous les clones liés du pool. | Génère un SID d'ordinateur local unique pour chaque clone lié du pool. |
| Peut exécuter des scripts de personnalisation supplémentaires avant la désactivation de clones liés et après la création, l'actualisation ou la recomposition de clones liés. | Peut exécuter un script supplémentaire après la première ouverture de session de l'utilisateur. |

**Tableau 5-4.** Comparaison de QuickPrep et Microsoft Sysprep (suite)

| QuickPrep | Spécification de personnalisation (Sysprep) |
|---|---|
| Associe l'ordinateur de clone lié au domaine Active Directory. | Associe l'ordinateur de clone lié au domaine Active Directory.<br>Les informations de domaine et d'administrateur dans la spécification de personnalisation Sysprep ne sont pas utilisées. La machine virtuelle est jointe au domaine utilisant les informations de personnalisation client que vous entrez dans View Administrator lorsque vous créez le pool. |
| Pour chaque clone lié, ajoute un ID unique au compte de domaine Active Directory. | Pour chaque clone lié, ajoute un ID unique au compte de domaine Active Directory. |
| Ne génère pas de nouveau SID après l'actualisation des clones liés. Le SID commun est conservé. | Génère un nouveau SID lors de la personnalisation de chaque clone lié. Conserve les SID uniques au cours d'une opération d'actualisation, mais pas au cours d'une opération de recomposition ou de rééquilibrage. |
| Ne génère pas de nouveau SID après la recomposition des clones liés. Le SID commun est conservé. | S'exécute de nouveau après la recomposition des clones liés, en générant de nouveaux SID pour les machines virtuelles.<br>Pour plus d'informations, reportez-vous à « Recomposition de clones liés personnalisés avec Sysprep », page 90. |
| S'exécute plus rapidement que Sysprep. | Peut prendre plus de temps que QuickPrep. |

Si vous avez personnalisé un pool de clone lié avec QuickPrep ou Sysprep, vous ne pourrez pas passer à l'autre méthode de personnalisation lorsque vous créerez ou recomposerez des machines dans le pool.

## Personnalisation de machines de clone lié avec QuickPrep

Vous pouvez personnaliser les machines de clone lié qui sont créées à partir d'une machine virtuelle parente à l'aide de l'outil système QuickPrep. View Composer exécute QuickPrep lors de la création ou de la recomposition d'une machine de clone lié.

QuickPrep personnalise une machine de clone lié de plusieurs manières :

- Il donne à l'ordinateur un nom que vous spécifiez lorsque vous créez le pool de clone lié.
- Il crée un compte d'ordinateur dans Active Directory, en associant l'ordinateur au domaine approprié.
- Il monte le disque persistant de View Composer. Le profil d'utilisateur Windows est redirigé vers ce disque.
- Il redirige des fichiers temporaires et d'échange vers un disque séparé.

Ces étapes peuvent requérir un ou plusieurs redémarrages des clones liés.

QuickPrep utilise des clés de licence de volume KMS pour activer des machines de clone lié Windows. Pour obtenir des informations détaillées, reportez-vous au document *Administration de View*.

Vous pouvez créer vos propres scripts pour personnaliser davantage les clones liés. QuickPrep peut exécuter deux types de scripts à des heures prédéfinies :

- après la création ou la recomposition des clones liés ;
- immédiatement avant la désactivation des clones liés.

Pour connaître les instructions et les règles d'utilisation des scripts de personnalisation QuickPrep, reportez-vous à « Exécution de scripts de personnalisation QuickPrep », page 89

**Remarque** View Composer nécessite les informations d'identification d'un utilisateur de domaine pour joindre des machines de clone lié à un domaine Active Directory. Pour obtenir des informations détaillées, reportez-vous au document *Administration de View*.

## Exécution de scripts de personnalisation QuickPrep

L'outil QuickPrep vous permet de créer des scripts pour personnaliser les machines de clone lié d'un pool. Vous pouvez configurer QuickPrep pour exécuter des scripts de personnalisation à deux moments prédéfinis.

### Lors de l'exécution de scripts QuickPrep

Le script de post-synchronisation s'exécute après la création, la recomposition ou le rééquilibrage des clones liés, et l'état du clone est **Prêt**. Le script de désactivation s'exécute avant la désactivation de clones liés. Les scripts s'exécutent dans les systèmes d'exploitation client des clones liés.

### Comment QuickPrep exécute des scripts

Le processus de QuickPrep utilise l'appel API `CreateProcess` de Windows pour exécuter des scripts. Votre script peut appeler n'importe quel processus pouvant être créé avec l'API `CreateProcess`. Par exemple, les processus `cmd`, `vbscript`, `exe` et de fichier de commandes fonctionnent avec l'API.

En particulier, QuickPrep transmet le chemin d'accès spécifié pour le script en tant que deuxième paramètre à l'API `CreateProcess` et définit le premier paramètre sur `NULL`.

Par exemple, si le chemin du script est `c:\myscript.cmd`, le chemin apparaît en tant que deuxième paramètre dans la fonction dans le fichier journal de View Composer : `CreateProcess(NULL,c:\myscript.cmd,...)`.

### Fournir des chemins à des scripts QuickPrep

Vous fournissez des chemins d'accès aux scripts de personnalisation QuickPrep lorsque vous créez un pool de machines de clone lié ou lorsque vous modifiez les paramètres de personnalisation invités d'un pool. Les scripts doivent résider sur la machine virtuelle parente. Vous ne pouvez pas utiliser de chemin d'accès UNC vers un partage de réseau.

Si vous utilisez un langage de script qui a besoin d'un interprète pour exécuter le script, le chemin du script doit démarrer par le binaire de l'interprète.

Par exemple, si vous spécifiez le chemin d'accès `C:\script\myvb.vbs` en tant que script de personnalisation QuickPrep, View Composer Agent ne peut pas exécuter le script. Vous devez spécifier un chemin qui démarre par le chemin du binaire de l'interprète :

```
C:\windows\system32\cscript.exe c:\script\myvb.vbs
```

---

**Important** Empêchez les utilisateurs normaux d'accéder aux scripts de personnalisation QuickPrep. Placez les scripts dans un dossier sécurisé.

---

### Délai d'expiration du script QuickPrep

View Composer termine un script de post-synchronisation ou de désactivation qui prend plus de 20 secondes. Si votre script dure plus de 20 secondes, vous pouvez augmenter la limite d'expiration. Pour plus d'informations, reportez-vous à « Augmenter la limite du délai d'expiration des scripts de personnalisation ClonePrep et QuickPrep », page 59.

Vous pouvez également utiliser votre script pour lancer un autre script ou processus exécutant la longue tâche.

### Compte de script QuickPrep

QuickPrep exécute les scripts sous le compte dans lequel le service VMware View Composer Guest Agent Server est configuré pour être exécuté. Par défaut, ce compte est `système local`.

Ne modifiez pas ce compte d'ouverture de session. Si vous le faites, les clones liés ne démarrent pas.

### Privilèges du processus QuickPrep

Pour des raisons de sécurité, certains privilèges du système d'exploitation Windows sont supprimés du processus View Composer Guest Agent qui appelle des scripts de personnalisation QuickPrep.

Un script de personnalisation QuickPrep ne peut effectuer aucune action nécessitant un privilège qui est supprimé du processus View Composer Guest Agent.

Les privilèges suivants sont supprimés du processus qui appelle les scripts QuickPrep :

```
SeCreateTokenPrivilege
SeTakeOwnershipPrivilege
SeSecurityPrivilege
SeSystemEnvironmentPrivilege
SeLoadDriverPrivilege
SeSystemtimePrivilege
SeUndockPrivilege
SeManageVolumePrivilege
SeLockMemoryPrivilege
SeIncreaseBasePriorityPrivilege
SeCreatePermanentPrivilege
SeDebugPrivilege
SeAuditPrivilege
```

### Journaux de script QuickPrep

Les journaux de View Composer contiennent des informations sur l'exécution du script QuickPrep. Le journal enregistre le début et la fin de l'exécution et journalise des messages de sortie ou d'erreur. Le journal se trouve dans le répertoire `temp` de Windows :

```
C:\Windows\Temp\vmware-viewcomposer-ga-new.log
```

## Recomposition de clones liés personnalisés avec Sysprep

Si vous recomposez une machine de clone lié personnalisée avec Sysprep, View exécute à nouveau la spécification de personnalisation Sysprep, une fois le disque du système d'exploitation recomposé. Cette opération génère un nouveau SID pour la machine virtuelle de clone lié.

Si un nouveau SID est généré, le clone lié recomposé fonctionne comme un nouvel ordinateur sur le réseau. Certains programmes logiciels, tels que des outils de gestion système, dépendent du SID pour identifier les ordinateurs qu'ils gèrent. Ces programmes peuvent ne pas pouvoir identifier ou rechercher la machine virtuelle de clone lié.

De plus, si un logiciel tiers est installé sur le disque système, la spécification de personnalisation peut regénérer les GUID de ce logiciel après la recomposition.

Une recomposition restaure le clone lié à son état d'origine, avant la première exécution de la spécification de personnalisation. Dans cet état, le clone lié ne possède pas de SID d'ordinateur local ou le GUID des logiciels tiers installés sur le lecteur système. View doit exécuter la spécification de personnalisation Sysprep après la recomposition du clone lié.

## Maintien des machines de clone lié provisionnées pour une utilisation dans des sessions de poste de travail distant au cours d'opérations de View Composer

Si vos utilisateurs doivent pouvoir accéder à des postes de travail distants à tout moment, vous devez maintenir un certain nombre de machines provisionnées pour une utilisation dans des sessions de poste de travail distant, même lorsque des opérations de maintenance de View Composer sont en cours. Vous pouvez définir un nombre minimal de machines qui ne sont pas placées en mode de maintenance alors que View Composer actualise, recompose ou rééquilibre les machines virtuelles de clone lié dans un pool.

Lorsque vous définissez **Nombre minimal de machines prêtes (provisionnées) lors d'opérations de maintenance de View Composer**, View s'assure que des machines au nombre spécifié restent provisionnées, et qu'elles ne sont pas placées en mode de maintenance, pendant que View Composer exécute l'opération de maintenance.

Ce paramètre permet aux utilisateurs de maintenir des connexions existantes ou de faire de nouvelles demandes de connexion lors de l'opération de maintenance de View Composer. Le paramètre ne fait pas la différence entre les machines de rechange qui sont prêtes à accepter les nouvelles connexions et les machines qui sont déjà connectées dans des sessions de poste de travail existantes.

Vous pouvez spécifier ce paramètre lorsque vous créez ou modifiez un pool de clone lié.

Les recommandations suivantes s'appliquent à ce paramètre :

- Pour permettre à plusieurs utilisateurs de maintenir leurs connexions de poste de travail existantes et de garder un nombre minimal de machines de rechange (sous tension) pouvant accepter les nouvelles demandes de connexion, définissez **Nombre minimal de machines prêtes (provisionnées) lors d'opérations de maintenance de View Composer** sur une valeur suffisamment importante pour inclure les deux jeux de machines.
- Si vous utilisez un mode d'attribution de nom pour provisionner des machines et pour provisionner des machines à la demande, définissez le nombre de machines provisionnées lors des opérations de View Composer sur une valeur inférieure à la valeur **Nombre max. de machines**. Si le nombre maximal est inférieur, votre pool peut se retrouver avec un nombre total de machines inférieur au nombre minimal de machines que vous voulez maintenir provisionnées lors des opérations de View Composer. Dans ce cas, les opérations de maintenance de View Composer ne pourraient pas avoir lieu.
- Si vous provisionnez des machines en spécifiant manuellement une liste de noms de machines, ne réduisez pas la taille de pool totale (en supprimant des noms de machines) à un nombre inférieur au nombre minimal de machines provisionnées. Dans ce cas, les opérations de maintenance de View Composer ne pourraient pas avoir lieu.
- Si vous définissez un nombre minimal important de machines provisionnées par rapport à la taille du pool, les opérations de maintenance de View Composer peuvent durer plus longtemps. Pendant que View maintient le nombre minimal de machines provisionnées lors d'une opération de maintenance, l'opération peut ne pas atteindre la limite de simultanéité spécifiée dans le paramètre **Nombre max. d'opérations de maintenance View Composer simultanées**.

  Par exemple, si un pool contient 20 machines et que le nombre minimal de machines provisionnées est de 15, View Composer peut fonctionner sur 5 machines maximum à la fois. Si la limite de simultanéité des opérations de maintenance de View Composer est de 12, elle n'est jamais atteinte.
- Dans ce nom de paramètre, le terme « prêt » s'applique à l'état de la machine virtuelle de clone lié, pas à l'état de la machine qui est affiché dans View Administrator. Une machine virtuelle est prête lorsqu'elle est approvisionnée et prête à être activée. L'état de la machine reflète la condition gérée par View de la machine. Par exemple, une machine peut présenter l'état `Connecté`, `Déconnecté`, `Agent inaccessible`, `Suppression`, etc. et toujours être considérée comme étant « prête ».

# Utiliser des comptes d'ordinateur Active Directory existants pour des clones liés

Lorsque vous créez ou modifiez un pool de postes de travail ou une batterie de serveurs automatisée, vous pouvez configurer View Composer afin qu'il utilise des comptes d'ordinateur existants dans Active Directory pour les clones liés qui viennent d'être provisionnés.

Par défaut, View Composer génère un nouveau compte d'ordinateur Active Directory pour chaque clone lié qu'il approvisionne. L'option **Autoriser la réutilisation de comptes d'ordinateur pré-existants** vous permet de contrôler les comptes d'ordinateur qui sont créés dans Active Directory en garantissant que View Composer utilise des comptes d'ordinateur AD existants.

Si cette option est activée et qu'un clone lié est provisionné, View Composer vérifie si un nom de compte d'ordinateur AD existant correspond au nom de la machine de clones liés. Si une correspondance existe, View Composer utilise le compte d'ordinateur AD existant. Si View Composer ne trouve pas de nom de compte d'ordinateur AD correspondant, il génère un nouveau compte d'ordinateur AD pour le clone lié.

Vous pouvez définir l'option **Autoriser la réutilisation de comptes d'ordinateur pré-existants** lorsque vous créez ou modifiez un pool de postes de travail ou une batterie de serveurs automatisée. Si vous modifiez un pool ou une batterie de serveurs et définissez cette option, le paramètre affecte les machines de clone lié qui sont provisionnées dans le futur. Les clones liés qui sont déjà approvisionnés ne sont pas affectés.

Lorsque vous définissez l'option **Autoriser la réutilisation de comptes d'ordinateur pré-existants**, vous pouvez limiter les autorisations Active Directory affectées au compte d'utilisateur View Composer qui génère le pool de postes de travail ou la batterie de serveurs. Seules les autorisations Active Directory suivantes sont requises :

- Lister le contenu
- Lire toutes les propriétés
- Autorisations de lecture
- Réinitialiser le mot de passe

Vous ne pouvez limiter les autorisations Active Directory que si vous êtes certain que tous les machines que vous prévoyez de provisionner disposent de comptes d'ordinateur existants alloués dans Active Directory. View Composer génère un nouveau compte d'ordinateur AD si aucun nom correspondant n'est trouvé. Des autorisations supplémentaires, telles que Créer des objets ordinateur, sont requises pour créer de nouveaux comptes d'ordinateur. Pour obtenir la liste complète des autorisations requises pour le compte d'utilisateur View Composer, consultez le document *Administration de View*.

Cette option ne peut pas être désactivée si View Composer utilise actuellement au moins un compte d'ordinateur AD existant.

La procédure suivante s'applique à des pools de postes de travail de clone lié. Les étapes sont semblables pour les batteries de serveurs automatisées.

### Prérequis

Vérifiez que les comptes d'ordinateur existants sont situés dans le conteneur Active Directory que vous spécifiez avec le paramètre **Conteneur Active Directory**. Si les comptes existants se trouvent dans un conteneur différent, l'approvisionnement échoue pour les clones liés avec ces noms de compte et un message d'erreur indique que les comptes d'ordinateur existants existent déjà dans Active Directory.

Par exemple, si vous sélectionnez l'option **Autoriser la réutilisation de comptes d'ordinateur pré-existants** et spécifiez que le **Conteneur Active Directory** est la valeur par défaut, `CN=Computers`, et si les comptes d'ordinateur existants se trouvent dans `OU=mydesktops`, l'approvisionnement échoue pour ces comptes.

### Procédure

1 Dans Active Directory, créez les comptes d'ordinateur à utiliser pour les machines de clone lié.

   Par exemple : `machine1, machine2, machine3`

   Les noms de compte d'ordinateur doivent utiliser des entiers consécutifs afin de correspondre aux noms qui sont générés lors du provisionnement de machines dans View.

2 Dans View Administrator, créez un pool avec l'assistant Ajouter un pool de postes de travail ou modifiez le pool dans la boîte de dialogue Modifier.

3 Sur la page ou l'onglet Paramètres d'approvisionnement, sélectionnez **Utiliser un mode d'attribution de nom**.

4 Dans la zone de texte **Mode d'attribution de nom**, tapez un nom de machine qui correspond au nom de compte d'ordinateur Active Directory.

   Par exemple : `machine`

   View ajoute des numéros uniques au modèle pour fournir un nom unique pour chaque machine.

   Par exemple : `machine1, machine2, machine3`

5 Sur la page ou l'onglet Personnalisation client, sélectionnez l'option **Autoriser la réutilisation de comptes d'ordinateur pré-existants**.

# Création de pools de postes de travail de clone instantané

6

Pour fournir aux utilisateurs un accès à des postes de travail de clone instantané, vous devez d'abord créer un pool de postes de travail de clone instantané.

Ce chapitre aborde les rubriques suivantes :



## Pools de postes de travail de clone instantané

Un pool de postes de travail de clone instantané est un pool de postes de travail automatisé. vCenter Server crée les machines virtuelles de poste de travail en fonction des paramètres que vous spécifiez lorsque vous créez le pool.

Comme les clones liés View Composer, les clones instantanés partagent un disque virtuel d'une machine virtuelle et ils consomment donc moins de stockage que des machines virtuelles complètes. De plus, les clones instantanés partagent également la mémoire d'une machine virtuelle parente. Les clones instantanés sont créés à l'aide de la technologie vmFork. Un pool de postes de travail de clone instantané dispose des propriétés de clé suivantes :

- Le provisionnement de clones instantanés est beaucoup plus rapide que les clones liés View Composer.
- Les clones instantanés sont toujours créés dans un état sous tension, prêts pour la connexion de l'utilisateur. La personnalisation de l'invité et la jonction de domaine AD sont réalisées dans le cadre du workflow initial de mise sous tension.
- Lorsqu'un utilisateur se déconnecte, la machine virtuelle de poste de travail est supprimée. De nouveaux clones sont créés en fonction de la stratégie de provisionnement, qui peut être à la demande ou à l'avance.
- Avec l'opération d'image de transfert, vous pouvez recréer le pool à partir de n'importe quel snapshot de n'importe quelle machine virtuelle parente. Vous pouvez utiliser une image de transfert pour déployer des correctifs de système d'exploitation et d'application.
- Des clones sont automatiquement rééquilibrés sur des magasins de données disponibles lorsque les clones sont créés.
- View Storage Accelerator est automatiquement activé.

- Le partage de page transparente est automatiquement activé.

Comme View peut créer des clones instantanés très rapidement, vous n'avez généralement pas besoin de provisionner un grand nombre de postes de travail à l'avance ou d'avoir un grand nombre de postes de travail prêts. Pour cette raison, par rapport aux clones liés View Composer, les clones instantanés peuvent faciliter la tâche de gestion d'un grand nombre de postes de travail et également réduire la quantité de ressources matérielles nécessaire.

Les clones instantanés ont les exigences de compatibilité suivantes :

- vSphere 6.0 Update 1 ou version ultérieure.
- Machine virtuelle version 11 ou ultérieure.

Il vous est recommandé de configurer des commutateurs virtuels distribués dans l'environnement vSphere.

Dans Horizon 7.0, les clones instantanés ont certaines restrictions :

- Postes de travail mono-utilisateur uniquement. Les hôtes RDS ne sont pas pris en charge.
- Affectation d'utilisateur flottante uniquement. Des postes de travail aléatoires du pool sont attribués aux utilisateurs.
- Des postes de travail de clone instantané ne peuvent pas disposer de disques persistants. Les utilisateurs peuvent utiliser VMware App Volumes pour stocker des données persistantes. Pour plus d'informations sur App Volumes, consultez https://www.vmware.com/products/appvolumes.
- Les snapshots NFS natifs Virtual Volumes et VAAI (vStorage APIs for Array Integration) ne sont pas pris en charge.
- Sysprep n'est pas disponible pour la personnalisation de poste de travail.
- Windows 7 et Windows 10 sont pris en charge, mais pas Windows 8 ou Windows 8.1.
- PowerCLI n'est pas pris en charge.
- Les magasins de données locaux ne sont pas pris en charge.
- IPv6 n'est pas pris en charge.
- Les clones instantanés ne peuvent pas réutiliser des comptes d'ordinateur préexistants dans Active Directory.
- Persona Management n'est pas disponible.
- Le rendu 3D n'est pas disponible.
- Vous ne pouvez pas spécifier un nombre minimal de machines prêtes (provisionnées) lors d'opérations de maintenance de clone instantané. Cette fonctionnalité n'est pas nécessaire, car la vitesse élevée de création des clones instantanés signifie que certaines machines sont toujours disponibles même lors des opérations de maintenance.

La fonctionnalité de récupération d'espace disque qui est disponible pour les clones liés View Composer n'est pas nécessaire, car les clones instantanés sont recréés lorsque les utilisateurs se déconnectent. Ainsi, la récupération de l'espace disque inutilisé dans une machine virtuelle n'a plus un impact important sur la consommation de stockage.

Chaque pool de postes de travail de clone instantané est associé à une image. Une image est le snapshot d'une machine virtuelle parente. La création d'un pool de postes de travail de clone instantané implique deux opérations :

1 View publie l'image que vous avez sélectionnée. Dans vCenter Server, quatre dossiers (`ClonePrepInternalTemplateFolder`, `ClonePrepParentVmFolder`, `ClonePrepReplicaVmFolder` et `ClonePrepResyncVmFolder`) sont créés s'ils n'existent pas, et plusieurs machines virtuelles internes requises pour le clonage sont créées. Dans View Administrator, vous pouvez voir la progression de cette opération sur la page de résumé du pool de postes de travail. Lors de la publication, le volet Image en attente indique l'image et son état.

   **Remarque** Ne modifiez pas les quatre dossiers ou les machines virtuelles internes qui se trouvent à l'intérieur. Si vous le faites, des erreurs peuvent se produire. Les machines virtuelles internes sont automatiquement supprimées lorsqu'elles ne sont plus nécessaires. Normalement, les machines virtuelles sont supprimées dans les 5 minutes qui suivent la suppression du pool ou une opération d'image de transfert. Cependant, il peut arriver que la suppression prenne jusqu'à 30 minutes.

2 Les clones sont créés. Ce processus est très rapide. En général, un clone peut être créé en moins de deux secondes. Lors de ce processus, le volet Image actuelle indique l'image et son état.

Une fois le pool créé, vous pouvez modifier l'image via l'opération d'image de transfert. Consultez « Modifier l'image d'un pool de postes de travail de clone instantané » dans le document *Administration de View*. De nouveau, la nouvelle image est d'abord publiée. Ensuite, les clones sont recréés.

Si vous modifiez un pool pour ajouter ou supprimer des magasins de données, le rééquilibrage des machines virtuelles se produit automatiquement lorsqu'un nouveau clone doit être créé, par exemple, lorsqu'un utilisateur se déconnecte ou que vous augmentez la taille du pool. Si vous voulez que le rééquilibrage arrive plus vite, procédez comme suit :

- Si vous supprimez une banque de données, supprimez manuellement les postes de travail sur cette banque de données pour que les nouveaux postes de travail soient créés sur les banques de données restantes.
- Si vous ajoutez une banque de données, supprimez manuellement quelques postes de travail des banques de données d'origine pour que les nouveaux postes de travail soient créés sur la nouvelle banque de données. Vous pouvez également supprimer tous les postes de travail ou simplement effectuer une image de transfert avec la même image pour que, lorsque les postes de travail sont recréés, ils soient distribués équitablement parmi les magasins de données.

Pour plus d'informations sur tous les paramètres disponibles pour un pool de clone instantané, reportez-vous à la section « Feuille de calcul pour créer un pool de postes de travail de clone instantané », page 98.

## Ajouter un administrateur de domaine de clone instantané

Avant de pouvoir créer un pool de postes de travail de clone instantané, vous devez ajouter un administrateur de domaine de clone instantané à View.

L'administrateur de domaine de clone instantané doit disposer de certains privilèges de domaine Active Directory. Pour plus d'informations, consultez la section « Créer un compte d'utilisateur pour des opérations de clone instantané » dans le document *Installation de View*.

### Procédure

1 Dans View Administrator, sélectionnez **Configuration de View > Administrateurs de domaine Instant Clone**.

2 Cliquez sur **Ajouter**.

3 Entrez le nom de connexion et le mot de passe de l'administrateur.

# Feuille de calcul pour créer un pool de postes de travail de clone instantané

Lorsque vous créez un pool de postes de travail de clone instantané, l'assistant Ajouter un pool de postes de travail d'Horizon Administrator vous invite à configurer certaines options. Utilisez cette feuille de calcul pour préparer vos options de configuration avant de créer le pool.

Avant de créer un pool de clone instantané, vous devez utiliser vCenter Server pour prendre un snapshot de la machine virtuelle parente que vous préparez pour le pool. Vous devez éteindre la machine virtuelle parente avant de prendre le snapshot. Horizon 7 utilise le snapshot comme image de base pour créer les clones.

**Remarque** Vous ne pouvez pas créer de pool de clone instantané depuis un modèle de machine virtuelle.

**Tableau 6-1.** Feuille de calcul : options de configuration pour la création d'un pool de postes de travail de clone instantané

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| Affectation d'utilisateur | Sélectionnez **Flottante**. Des postes de travail aléatoires du pool sont attribués aux utilisateurs. | |
| vCenter Server | Sélectionnez **Clones instantanés**, puis le serveur vCenter Server qui gère les machines virtuelles dans le pool. | |
| ID du pool de postes de travail | Nom unique qui identifie le pool dans Horizon Administrator.<br>Si plusieurs configurations du Serveur de connexion sont exécutées dans votre environnement, assurez-vous qu'aucune autre configuration du Serveur de connexion n'utilise le même ID de pool.<br>Une configuration du Serveur de connexion peut être une instance autonome du Serveur de connexion ou un espace d'instances répliquées. | |
| Nom d'affichage | Nom du pool que les utilisateurs voient lorsqu'ils se connectent à partir d'un périphérique client. Si vous ne spécifiez pas de nom d'affichage, l'ID de pool est affiché aux utilisateurs. | |
| Groupe d'accès | Sélectionnez un groupe d'accès dans lequel placer le pool ou laissez ce dernier dans le groupe d'accès racine par défaut.<br>Si vous utilisez un groupe d'accès, vous pouvez déléguer la gestion du pool à un administrateur avec un rôle spécifique. Pour plus d'informations, consultez le chapitre consacré à l'administration déléguée basée sur des rôles du document *Administration de View*.<br>**Remarque** Les groupes d'accès sont différents des dossiers vCenter Server qui stockent les machines virtuelles utilisées en tant que postes de travail. Vous sélectionnez un dossier vCenter Server plus tard dans l'assistant avec d'autres paramètres de vCenter Server. | |
| État | S'il est défini sur **Activé**, le pool est prêt à être utilisé après le provisionnement. S'il est défini sur **Désactivé**, le pool n'est pas disponible pour les utilisateurs. Lors du provisionnement, si vous désactivez le pool, le provisionnement s'arrêtera. | |

**Tableau 6-1.** Feuille de calcul : options de configuration pour la création d'un pool de postes de travail de clone instantané (suite)

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| Restrictions du serveur de connexion | Vous pouvez limiter l'accès au pool à certains Serveurs de connexion en cliquant sur le bouton Parcourir et en sélectionnant un ou plusieurs Serveurs de connexion.<br>Si vous prévoyez de fournir un accès aux postes de travail via VMware Identity Manager et que vous configurez des limitations du Serveur de connexion, il est possible que l'application VMware Identity Manager affiche les postes de travail aux utilisateurs alors que ces postes de travail sont en réalité limités. Les utilisateurs de VMware Identity Manager ne pourront pas lancer ces postes de travail. | |
| Automatically logoff after disconnect (Fermeture de session automatique après la déconnexion) | ■ **Immédiatement**. La session des utilisateurs est fermée lorsqu'ils se déconnectent.<br>■ **Jamais**. La session des utilisateurs n'est jamais fermée.<br>■ **Après**. Durée après laquelle la session des utilisateurs est fermée lorsque ceux-ci se déconnectent. Saisissez la durée en minutes.<br>L'heure de fermeture de session s'applique aux déconnexions futures. Si un utilisateur a déjà fermé une session de poste de travail lorsque vous définissez une heure de fermeture de session, la durée de fermeture pour cet utilisateur démarre au moment où vous définissez l'heure de fermeture de session, pas lorsque l'utilisateur a fermé sa session. Par exemple, si vous définissez cette valeur sur 5 minutes, et qu'une session a été fermée 10 minutes plus tôt, View fermera cette session 5 minutes après que vous avez défini la valeur. | |
| Autoriser l'utilisateur à ouvrir des sessions séparées depuis différents périphériques clients | Lorsque ce paramètre est sélectionné, un utilisateur se connectant au même pool de postes de travail depuis différents périphériques clients accédera à plusieurs sessions de poste de travail. L'utilisateur ne peut rouvrir une session existante qu'à partir du périphérique client depuis lequel la session a été ouverte. Lorsque ce paramètre n'est pas sélectionné, la session existante de l'utilisateur sera rouverte quel que soit le périphérique client utilisé. | |
| Protocole d'affichage par défaut | Sélectionnez le protocole d'affichage par défaut. Les choix sont **Microsoft RDP**, **PCoIP** et **VMware Blast**. | |
| Autoriser les utilisateurs à choisir un protocole | Spécifiez si les utilisateurs peuvent choisir un protocole d'affichage qui n'est pas celui par défaut. | |

**Tableau 6-1.** Feuille de calcul : options de configuration pour la création d'un pool de postes de travail de clone instantané (suite)

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| HTML Access | Sélectionnez **Activé** pour autoriser les utilisateurs à se connecter à des postes de travail distants à partir de leur navigateur Web.<br>Lorsqu'un utilisateur se connecte via la page du portail Web VMware Horizon ou via l'application VMware Identity Manager, et qu'il sélectionne un poste de travail distant, l'agent HTML Access autorise l'utilisateur à se connecter au poste de travail via HTTPS. Le poste de travail est affiché dans le navigateur de l'utilisateur. D'autres protocoles d'affichage, tels que PCoIP ou RDP, ne sont pas utilisés. Le logiciel Horizon Client n'a pas besoin d'être installé sur les périphériques clients.<br>Pour utiliser HTML Access, vous devez installer HTML Access dans votre déploiement de View. Pour obtenir plus d'informations, reportez-vous au document *Utilisation de HTML Access*, disponible sur https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.<br>Pour utiliser HTML Access avec VMware Identity Manager, vous devez coupler le Serveur de connexion View à un serveur d'authentification SAML, comme expliqué dans le document *Administration de View*. VMware Identity Manager doit être installé et configuré pour une utilisation avec le Serveur de connexion View. | |
| Adobe Flash quality (Qualité Adobe Flash) | Détermine la qualité du contenu Adobe Flash affiché sur des pages Web.<br>■ **Ne pas contrôler**. La qualité est déterminée par les paramètres de page Web.<br>■ **Faible**. Ce paramètre se traduit par les meilleures économies de bande passante. Si aucun niveau de qualité n'est spécifié, le système prend la valeur par défaut Low (Faible).<br>■ **Moyenne**. Ce paramètre se traduit par des économies de bande passante modérées.<br>■ **Élevée**. Ce paramètre se traduit par des économies de bande passante moindres.<br>Pour plus d'informations, reportez-vous à la section « Qualité et limitation d'Adobe Flash », page 164. | |
| Adobe Flash throttling (Limitation d'Adobe Flash) | Détermine la fréquence d'image des films Adobe Flash. Si vous activez ce paramètre, vous pouvez réduire ou augmenter le nombre d'images affichées par seconde en sélectionnant un niveau d'agressivité.<br>■ **Désactivé**. Aucune limitation n'est effectuée. L'intervalle du temporisateur n'est pas modifié.<br>■ **Classique**. L'intervalle du temporisateur est de 100 millisecondes. Ce paramètre correspond au plus petit nombre d'images ignorées.<br>■ **Modérée**. L'intervalle du temporisateur est de 500 millisecondes.<br>■ **Agressive**. L'intervalle du temporisateur est de 2 500 millisecondes. Ce paramètre correspond au plus grand nombre d'images ignorées.<br>Pour plus d'informations, reportez-vous à la section « Qualité et limitation d'Adobe Flash », page 164. | |

**Tableau 6-1.** Feuille de calcul : options de configuration pour la création d'un pool de postes de travail de clone instantané (suite)

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| Arrêter l'approvisionnement en cas d'erreur | Vous pouvez faire en sorte qu'View arrête ou continue le provisionnement des machines virtuelles dans un pool de postes de travail suite à une erreur survenue au cours du provisionnement d'une machine virtuelle. Si vous laissez ce paramètre sélectionné, vous pouvez empêcher qu'une erreur de provisionnement se répète sur plusieurs machines virtuelles. | |
| Mode d'attribution de nom | Le modèle que vous spécifiez est utilisé en tant que préfixe dans tous les noms de machines, suivi d'un numéro unique identifiant chaque machine.<br>Pour plus d'informations, reportez-vous à « Utilisation d'un mode d'attribution de nom pour des pools de postes de travail automatisés », page 155. | |
| Nombre max. de machines | Spécifiez le nombre total de machines dans le pool. | |
| Nombre de machines de rechange (sous tension) | Spécifiez le nombre de machines à garder disponibles pour les utilisateurs. Pour plus d'informations, reportez-vous à « Dénomination manuelle de machines ou fourniture d'un mode d'attribution de nom », page 152. | |
| Provisionner des machines à la demande<br>Nombre min. de machines<br>Provisionner toutes les machines à l'avance | Indiquez s'il convient de provisionner toutes les machines lors de la création du pool ou en fonction des besoins.<br>■ **Provisionner toutes les machines à l'avance**. À la création du pool, le système provisionne le nombre de machines que vous spécifiez dans **Nombre max. de machines**.<br>■ **Provisionner des machines à la demande**. Lorsque le pool est créé, le système crée le nombre de machines en fonction de la valeur la plus élevée **Nombre min. de machines** ou **Nombre de machines de rechange (sous tension)**. Des machines supplémentaires sont créées pour conserver ce nombre minimal de machines disponibles à mesure que les utilisateurs se connectent aux postes de travail. | |
| Sélectionner des magasins de données séparés pour les disques de réplication et du système d'exploitation | Vous pouvez stocker le disque de machine virtuelle réplica (maître) sur un magasin de données haute performance et les clones instantanés sur des magasins de données séparés.<br>Pour plus d'informations, reportez-vous à « Stockage de réplicas et de clones sur des magasins de données séparés pour des clones instantanés et des clones liés View Composer », page 289. | |
| Machine virtuelle parente | Sélectionnez la machine virtuelle parente du pool. | |
| Snapshot (image par défaut) | Sélectionnez le snapshot de la machine virtuelle parente à utiliser comme image de base pour le pool.<br>Ne supprimez pas le snapshot et la machine virtuelle parente de vCenter Server tant que le pool existe. | |
| Emplacement du dossier de machine virtuelle | Sélectionnez le dossier dans vCenter Server dans lequel réside le pool de postes de travail. | |
| Cluster | Sélectionnez le cluster vCenter Server sur lequel les machines virtuelles de poste de travail s'exécutent. Vous ne pouvez pas spécifier un hôte ESXi. | |
| Resource pool (Pool de ressources) | Sélectionnez le pool de ressources de vCenter Server dans lequel le pool de postes de travail réside. | |

**Tableau 6-1.** Feuille de calcul : options de configuration pour la création d'un pool de postes de travail de clone instantané (suite)

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| Magasins de données | Sélectionnez un ou plusieurs magasins de données sur lesquels stocker le pool de postes de travail.<br>Sur la page Sélectionner des magasins de données de clone instantané de l'assistant Ajouter un pool de postes de travail, un tableau fournit des recommandations pour estimer les besoins en stockage du pool. Ces recommandations peuvent vous aider à déterminer les magasins de données assez volumineux pour stocker les clones. Le paramètre Surcharge du stockage est toujours défini sur Illimitée et il n'est pas configurable. | |
| Domaine | Sélectionnez un domaine Active Directory. La liste déroulante indique les domaines qui sont ajoutés lorsque vous configurez des administrateurs de domaine de clone instantané. Reportez-vous à la section « Ajouter un administrateur de domaine de clone instantané », page 97. | |
| Conteneur Active Directory | Fournissez le nom unique relatif du conteneur Active Directory.<br>Par exemple : **`CN=Ordinateurs`**<br>Lorsque vous exécutez l'assistant Ajouter un pool de postes de travail, vous pouvez parcourir l'arborescence d'Active Directory à la recherche du conteneur. | |
| Power-off script (Script de désactivation) | Spécifiez un script à exécuter sur les machines avant qu'elles soient désactivées.<br>Fournissez le chemin d'accès au script sur la machine virtuelle parente et aux paramètres de script. | |
| Script de post-synchronisation | Spécifiez un script à exécuter sur les machines après leur création.<br>Fournissez le chemin d'accès au script sur la machine virtuelle parente et aux paramètres de script. | |

# Créer un pool de postes de travail de clone instantané

L'assistant Ajouter un pool de postes de travail d'Horizon Administrator vous guide lors des étapes de création d'un pool de postes de travail de clone instantané.

### Prérequis

- Vérifiez que vous disposez d'un nombre suffisant de ports sur le commutateur virtuel ESXi utilisé pour les machines virtuelles servant de postes de travail distants. La valeur par défaut peut ne pas être suffisante si vous créez des pools de postes de travail volumineux. Le nombre de ports de commutateur virtuel sur l'hôte ESXi doit être égal ou supérieur au nombre de machines virtuelles multiplié par le nombre de cartes réseau virtuelles par machine virtuelle.
- Vérifiez que vous avez préparé une machine virtuelle parente. Horizon Agent doit être installé sur la machine virtuelle parente. Reportez-vous à la section Chapitre 3, « Création et préparation d'une machine virtuelle parente pour le clonage », page 25.
- Prenez un snapshot de la machine virtuelle parente dans vCenter Server. Vous devez éteindre la machine virtuelle parente avant de prendre le snapshot. Horizon 7 utilise le snapshot comme image de base pour créer les clones.
- Collectez les informations de configuration pour le pool. Reportez-vous à la section « Feuille de calcul pour créer un pool de postes de travail de clone instantané », page 98.

- Vérifiez que vous avez ajouté un administrateur de domaine de clone instantané dans View Administrator.

### Procédure

1. Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.
2. Cliquez sur **Ajouter**.
3. Sélectionnez **Pool de postes de travail automatisé**.
4. Sur la page vCenter Server, choisissez **Clones instantanés**.
5. Suivez les invites de l'assistant pour créer le pool.

   Utilisez les informations de configuration que vous avez collectées dans la feuille de calcul. Vous pouvez revenir directement à n'importe quelle page de l'assistant en cliquant sur le nom de page dans le volet de navigation.

Dans Horizon Administrator, vous pouvez afficher les machines à mesure de leur ajout au pool en sélectionnant **Catalogue > Pools de postes de travail**.

Après avoir créé le pool, ne supprimez pas la machine virtuelle parente et ne la retirez pas de l'inventaire de vCenter Server tant que le pool existe, car diverses opérations de pool ont besoin que cette machine virtuelle soit présente. Si vous supprimez la machine virtuelle de l'inventaire de vCenter Server par erreur, vous devez la rajouter et réaliser une image de transfert à l'aide de la même image que celle que le pool possède actuellement.

### Suivant

Autorisez les utilisateurs à accéder au pool. Reportez-vous à la section « Ajouter des droits d'accès à un pool de postes de travail ou d'applications », page 187.

# Personnalisation d'invité ClonePrep

ClonePrep personnalise des clones instantanés lorsqu'ils sont créés et il fonctionne comme QuickPrep.

ClonePrep joint tous les clones instantanés au domaine Active Directory. Les clones ont les mêmes identificateurs de sécurité (SID) d'ordinateur que leur machine virtuelle parente. ClonePrep conserve également les identificateurs globaux uniques (GUID) d'applications, même si certaines applications peuvent générer un nouveau GUID lors de la personnalisation.

Lorsque vous ajoutez un pool de postes de travail de clone instantané, vous pouvez spécifier un script pour qu'il s'exécute immédiatement après la création du clone et un autre script pour qu'il s'exécute avant la désactivation du clone.

## Exécution des scripts par ClonePrep

ClonePrep utilise l'appel API `CreateProcess` de Windows pour exécuter des scripts. Votre script peut appeler n'importe quel processus pouvant être créé avec l'API `CreateProcess`. Par exemple, les processus `cmd`, `vbscript`, `exe` et de fichier de commandes fonctionnent avec l'API.

En particulier, ClonePrep transmet le chemin d'accès spécifié pour le script en tant que deuxième paramètre à l'API `CreateProcess` et définit le premier paramètre sur `NULL`. Par exemple, si le chemin du script est `c:\myscript.cmd`, l'appel à `CreateProcess` est `CreateProcess(NULL,c:\myscript.cmd,...)`.

## Fournir des chemins à des scripts ClonePrep

Vous pouvez spécifier les scripts à exécuter lorsque vous créez ou modifiez le pool de postes de travail. Les scripts doivent résider sur la machine virtuelle parente. Vous ne pouvez pas utiliser de chemin d'accès UNC vers un partage de réseau.

Si vous utilisez un langage de script qui a besoin d'un interprète pour exécuter le script, le chemin du script doit démarrer par l'exécutable de l'interprète. Par exemple, au lieu de spécifier `C:\script\myvb.vbs`, vous devez spécifier `C:\windows\system32\cscript.exe c:\script\myvb.vbs`.

**IMPORTANT** Empêchez les utilisateurs normaux d'accéder aux scripts de personnalisation ClonePrep. Placez les scripts dans un dossier sécurisé.

## Délai d'expiration du script ClonePrep

Par défaut, ClonePrep met fin aux scripts si leur exécution dure plus de 20 secondes. Vous pouvez augmenter la limite du délai d'expiration. Pour plus d'informations, reportez-vous à « Augmenter la limite du délai d'expiration des scripts de personnalisation ClonePrep et QuickPrep », page 59.

Vous pouvez également utiliser votre script pour lancer un autre script ou processus exécutant la longue tâche.

## Compte de script ClonePrep

ClonePrep exécute les scripts à l'aide du compte sous lequel le service VMware Horizon Instant Clone Agent est configuré pour s'exécuter. Par défaut, ce compte est `système local`.

Ne modifiez pas ce compte d'ouverture de session. Si vous le faites, les clones ne parviendront pas à démarrer.

## Privilèges de processus ClonePrep

Pour des raisons de sécurité, certains privilèges du système d'exploitation Windows sont supprimés du processus VMware Horizon Instant Clone Agent qui exécute des scripts de personnalisation ClonePrep. Par conséquent, les scripts ne peuvent pas exécuter des actions qui requièrent ces privilèges.

Les privilèges suivants sont supprimés du processus qui exécute les scripts ClonePrep :

```
SeCreateTokenPrivilege
SeTakeOwnershipPrivilege
SeSecurityPrivilege
SeSystemEnvironmentPrivilege
SeLoadDriverPrivilege
SeSystemtimePrivilege
SeUndockPrivilege
SeManageVolumePrivilege
SeLockMemoryPrivilege
SeIncreaseBasePriorityPrivilege
SeCreatePermanentPrivilege
SeDebugPrivilege
SeAuditPrivilege
```

## Journaux de script ClonePrep

Le journal de script ClonePrep enregistre le début et la fin de l'exécution et journalise des messages de sortie ou d'erreur. Le journal se trouve dans le répertoire `temp` de Windows :

```
C:\Windows\Temp\vmware-viewcomposer-ga-new.log
```

# Utilitaires de maintenance de clone instantané

Sur le Serveur de connexion se trouvent deux utilitaires que vous pouvez utiliser pour la maintenance de machines virtuelles de clone instantané dans vCenter Server et les clusters dans lesquels se trouvent les machines virtuelles.

Les utilitaires sont `IcMaint.cmd` et `IcUnprotect.cmd` et se trouvent dans `C:\Program Files\VMware\VMware View\Server\tools\bin`.

## IcMaint.cmd

Cette commande supprime les machines virtuelles parentes et met éventuellement un hôte en mode de maintenance. Après la maintenance, vous pouvez exécuter cette commande pour sortir un hôte du mode de maintenance.

Syntaxe :

`IcMaint.cmd –vc` *`nom_d_hote_ou_adresse_IP`* `–uid` *`ID_utilisateur`* `–password` *`mot_de_passe`* `–hostName` *`nom_d_hote_ESXi`* `–maintenance ON|OFF`

Paramètres :

- `–vc` *nom d'hôte ou adresse IP de vCenter Server*
- `–uid` *ID d'utilisateur de vCenter Server*
- `–password` *mot de passe d'utilisateur de vCenter Server*
- `–hostname` *nom d'hôte ESXi*
- `–maintenance ON|OFF`

  Ce paramètre spécifie s'il faut passer ou non en mode de maintenance après la suppression des machines virtuelles parentes. Si l'hôte est déjà en mode de maintenance, définir ce paramètre sur `OFF` sort l'hôte du mode de maintenance.

Tous les paramètres sont obligatoires.

## IcUnprotect.cmd

Cet utilitaire annule la protection des dossiers et des machines virtuelles que ClonePrep crée. ClonePrep est le mécanisme qui personnalise les clones instantanés lors du processus de création.

Syntaxe :

`IcUnprotect.cmd –vc` *`nom_d_hote_ou_adresse_IP`* `–uid` *`ID_utilisateur`* `–password` *`mot_de_passe`* `[–clusterId` *`ID_cluster`*`] [–includeFolders]`

Paramètres :

- `–vc` *nom d'hôte ou adresse IP de vCenter Server*
- `–uid` *ID d'utilisateur de vCenter Server*
- `–password` *mot de passe d'utilisateur de vCenter Server*
- `–clusterId` *ID de cluster*
- `–includeFolders`

  Spécifier ce paramètre annule la protection des dossiers et des machines virtuelles.

Tous les paramètres sont obligatoires, sauf `clusterId` et `includeFolders`. Si `clusterId` n'est pas spécifié, la protection est supprimée de toutes les machines virtuelles ClonePrep dans tous les centres de données.

# Création de pools de postes de travail manuels

7

Dans un pool de postes de travail manuel, chaque poste de travail distant accessible par un utilisateur final est une machine distincte. Lorsque vous créez un pool de postes de travail manuel, vous sélectionnez des machines existantes. Pour créer un pool qui contient un poste de travail unique, créez un pool de postes de travail manuel et sélectionnez une seule machine.

Ce chapitre aborde les rubriques suivantes :



## Pools de postes de travail manuels

Pour créer un pool de postes de travail manuel, View provisionne des postes de travail à partir de machines existantes. Vous sélectionnez une machine distincte pour chaque poste de travail du pool.

View peut utiliser plusieurs types de machines dans des pools manuels :

- des machines virtuelles gérées par vCenter Server ;
- des machines virtuelles qui s'exécutent sur une plate-forme de virtualisation autre que vCenter Server ;
- des ordinateurs physiques.

Pour plus d'informations sur la création d'un pool de postes de travail manuel qui utilise des machines virtuelles Linux, consultez le guide *Configuration des postes de travail Horizon 7 for Linux*.

## Feuille de calcul pour créer un pool de postes de travail manuel

Lorsque vous créez un pool de postes de travail manuel, l'assistant Ajouter un pool de postes de travail de View Administrator vous invite à configurer certaines options. Utilisez cette feuille de calcul pour préparer vos options de configuration avant de créer le pool.

Vous pouvez imprimer cette feuille de calcul et noter les valeurs que vous souhaitez spécifier quand vous exécutez l'assistant Ajouter un pool de postes de travail.

**Remarque** Dans un pool manuel, vous devez préparer chaque machine à fournir un accès au poste de travail distant. Horizon Agent doit être installé et en cours d'exécution sur chaque machine.

**Tableau 7-1.** Feuille de calcul : options de configuration pour la création d'un pool de postes de travail manuel

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| Affectation d'utilisateur | Choisissez le type d'affectation d'utilisateur :<br>■ Dans un pool à attribution dédiée, une machine est attribuée à chaque utilisateur. Les utilisateurs reçoivent la même machine chaque fois qu'ils ouvrent une session.<br>■ Dans un pool à attribution flottante, les utilisateurs reçoivent des machines différentes chaque fois qu'ils ouvrent une session.<br>Pour plus d'informations, reportez-vous à « Affectation d'utilisateur dans des pools de postes de travail », page 151. | |
| vCenter Server | Système vCenter Server qui gère les machines.<br>Cette option s'affiche uniquement si les machines sont des machines virtuelles gérées par vCenter Server. | |
| Source de machines | Machines virtuelles ou ordinateurs physiques à inclure dans le pool de postes de travail.<br>1 Choisissez le type de machine que vous souhaitez utiliser. Vous pouvez utiliser des machines virtuelles gérées par vCenter Server ou des machines virtuelles et des ordinateurs non gérés.<br>2 Préparez la liste des machines virtuelles vCenter Server ou des machines virtuelles et des ordinateurs physiques non gérés à inclure dans le pool de postes de travail.<br>3 Installez Horizon Agent sur chaque machine à inclure dans le pool de postes de travail.<br>Pour utiliser PCoIP avec des machines qui sont des machines virtuelles ou des ordinateurs physiques non gérés, vous devez utiliser un matériel Teradici.<br>**Remarque** Lorsque vous activez des postes de travail Windows Server dans View Administrator, View Administrator affiche toutes les machines Windows Server disponibles comme sources de machines potentielles, notamment celles sur lesquelles le Serveur de connexion View et d'autres serveurs View Server sont installés.<br>Vous ne pouvez pas sélectionner des machines pour le pool de postes de travail si le logiciel de View Server est installé sur les machines. Horizon Agent ne peut pas coexister sur une même machine virtuelle ou physique avec un autre composant logiciel View, notamment le Serveur de connexion View, le serveur de sécurité, View Composer ou Horizon Client. | |
| ID du pool de postes de travail | Nom de pool que les utilisateurs voient lorsqu'ils ouvrent une session et qui identifie le pool dans View Administrator.<br>Si plusieurs serveurs vCenter Server sont exécutés dans votre environnement, assurez-vous qu'aucun autre serveur vCenter Server n'utilise le même ID de pool. | |

**Tableau 7-1.** Feuille de calcul : options de configuration pour la création d'un pool de postes de travail manuel (suite)

| Option | Description | Indiquez votre valeur ici |
|---|---|---|
| Paramètres du pool de postes de travail | Paramètres qui déterminent l'état de la machine, l'état d'alimentation lorsqu'une machine virtuelle n'est pas utilisée, le protocole d'affichage, la qualité Adobe Flash, etc.<br>Pour plus d'informations, reportez-vous à « Paramètres de pools de postes de travail pour tous les types de pools de postes de travail », page 160.<br>Pour voir la liste des paramètres qui s'appliquent aux pools manuels, reportez-vous à la section « Paramètres de pool de postes de travail pour des pools manuels », page 111 | |
| Portée du partage de page transparente (Transparent Page Sharing) | Sélectionnez le niveau auquel autoriser le partage de page transparente (TPS). Les choix sont **Machine virtuelle** (par défaut), **Pool**, **Espace** ou **Global**. Si vous activez le partage de page transparente pour les machines du pool, de l'espace ou globalement, l'hôte ESXi élimine les copies redondantes des pages mémoire obtenues si les machines utilisent le même système d'exploitation invité ou les mêmes applications.<br>Le partage de page se produit sur l'hôte ESXi. Par exemple, si vous activez le partage de page transparente au niveau du pool alors que le pool couvre plusieurs hôtes ESXi, seules les machines virtuelles sur le même hôte et à l'intérieur du même pool partageront des pages. Au niveau global, toutes les machines gérées par View sur le même hôte ESXi peuvent partager des pages de mémoire, quel que soit le pool sur lequel résident les machines.<br>REMARQUE Par défaut, les pages de mémoire ne sont pas partagées entre plusieurs machines, car le partage de page transparente (TPS) peut créer un risque. Les recherches indiquent que le partage de page transparente peut être exploité de façon abusive pour obtenir un accès non autorisé à des données dans des scénarios de configuration très limités. | |

# Créer un pool de postes de travail manuel

Vous pouvez créer un pool de postes de travail manuel qui provisionne des postes de travail à partir de machines virtuelles ou d'ordinateurs physiques existants. Vous devez sélectionner les machines à inclure dans le pool de postes de travail.

Pour les pools manuels incluant des machines virtuelles gérées par vCenter Server, View s'assure qu'une machine de rechange est sous tension afin que les utilisateurs puissent s'y connecter. La machine de rechange est mise sous tension, quelle que soit la stratégie d'alimentation en vigueur.

### Prérequis

- Préparez les machines pour fournir un accès au poste de travail distant. Dans un pool manuel, vous devez préparer chaque machine individuellement. Horizon Agent doit être installé et en cours d'exécution sur chaque machine.

  Pour préparer des machines virtuelles gérées par vCenter Server, reportez-vous à Chapitre 3, « Création et préparation d'une machine virtuelle parente pour le clonage », page 25.

Pour préparer des machines virtuelles et des ordinateurs physiques non gérés, reportez-vous à Chapitre 2, « Préparation de machines non gérées », page 19.

- Collectez les informations de configuration que vous devez fournir pour créer le pool. Reportez-vous à la section « Feuille de calcul pour créer un pool de postes de travail manuel », page 107.
- Décidez comment configurer les paramètres d'alimentation, le protocole d'affichage, la qualité Adobe Flash et d'autres paramètres. Reportez-vous à la section « Paramètres de pools de postes de travail pour tous les types de pools de postes de travail », page 160.

### Procédure

1. Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.
2. Cliquez sur **Ajouter**.
3. Sélectionnez **Pool de postes de travail manuel**.
4. Suivez les invites de l'assistant pour créer le pool.

   Utilisez les informations de configuration que vous avez collectées dans la feuille de calcul. Vous pouvez revenir directement à n'importe quelle page de l'assistant en cliquant sur le nom de page dans le volet de navigation.

Dans View Administrator, vous pouvez afficher les machines à mesure de leur ajout au pool en sélectionnant **Catalogue > Pools de postes de travail**.

### Suivant

Autorisez les utilisateurs à accéder au pool. Reportez-vous à la section « Ajouter des droits d'accès à un pool de postes de travail ou d'applications », page 187.

## Créer un pool manuel contenant une seule machine

Vous pouvez créer un pool contenant une seule machine quand un utilisateur requiert un poste de travail dédié unique ou lorsque plusieurs utilisateurs doivent accéder à une application coûteuse avec une seule licence hôte à des heures différentes.

Vous pouvez provisionner une machine individuelle dans son propre pool en créant un pool de postes de travail manuel et en sélectionnant une seule machine.

Pour imiter un ordinateur physique pouvant être partagé par plusieurs utilisateurs, spécifiez une affectation flottante pour les utilisateurs autorisés à accéder au pool.

Que vous configuriez le pool d'une seule machine avec une affectation dédiée ou flottante, les opérations d'alimentation sont initiées par la gestion des sessions. La machine virtuelle est activée lorsqu'un utilisateur demande le poste de travail, et désactivée ou interrompue quand l'utilisateur ferme sa session.

Si vous configurez la stratégie **S'assurer que les machines sont toujours sous tension**, la machine virtuelle reste sous tension. Si l'utilisateur éteint la machine virtuelle, elle redémarre immédiatement.

### Prérequis

- Préparez la machine pour fournir un accès au poste de travail distant. Horizon Agent doit être installé et en cours d'exécution sur la machine.

  Pour préparer une machine virtuelle gérée par vCenter Server, reportez-vous à Chapitre 3, « Création et préparation d'une machine virtuelle parente pour le clonage », page 25

  Pour préparer une machine virtuelle ou un ordinateur physique non géré, reportez-vous à Chapitre 2, « Préparation de machines non gérées », page 19

- Collectez les informations de configuration que vous devez fournir pour créer le pool manuel. Reportez-vous à la section « Feuille de calcul pour créer un pool de postes de travail manuel », page 107.
- Décidez comment configurer les paramètres d'alimentation, le protocole d'affichage, la qualité Adobe Flash et d'autres paramètres. Reportez-vous à la section « Paramètres de pools de postes de travail pour tous les types de pools de postes de travail », page 160.

### Procédure

1. Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.
2. Cliquez sur **Ajouter**.
3. Sélectionnez **Pool de postes de travail manuel**.
4. Sélectionnez le type d'affectation d'utilisateur.

| Option | Description |
|---|---|
| **Dédiée** | La machine est attribuée à un utilisateur. Seul cet utilisateur peut ouvrir une session sur le poste de travail. |
| **Flottante** | La machine est partagée par tous les utilisateurs autorisés à accéder au pool. N'importe quel utilisateur autorisé peut ouvrir une session sur le poste de travail tant qu'un autre utilisateur n'y a pas ouvert de session. |

5. Dans la page Source de la machine, sélectionnez la machine à inclure dans le pool de postes de travail.
6. Suivez les invites de l'assistant pour créer le pool.

   Utilisez les informations de configuration que vous avez collectées dans la feuille de calcul. Vous pouvez revenir directement à n'importe quelle page de l'assistant en cliquant sur le nom de page dans le volet de navigation.

Dans View Administrator, vous pouvez voir la machine ajoutée au pool en sélectionnant **Catalogue > Pools de postes de travail**.

### Suivant

Autorisez les utilisateurs à accéder au pool. Reportez-vous à la section « Ajouter des droits d'accès à un pool de postes de travail ou d'applications », page 187.

## Paramètres de pool de postes de travail pour des pools manuels

Vous devez spécifier des paramètres de machine et de pool lorsque vous configurez des pools de postes de travail manuels. Les paramètres ne s'appliquent pas à tous les types de pools manuels.

Tableau 7-2 répertorie les paramètres qui s'appliquent à des pools de postes de travail manuels qui sont configurés avec ces propriétés :

- des affectations d'utilisateur dédiées ;
- des affectations d'utilisateur flottantes ;
- Machines gérées (machines virtuelles vCenter Server)
- Machines non gérées

Ces paramètres s'appliquent également à un pool manuel qui contient une seule machine.

Pour voir des descriptions de chaque paramètre de pools de postes de travail, reportez-vous à la section « Paramètres de pools de postes de travail pour tous les types de pools de postes de travail », page 160

**Tableau 7-2.** Paramètres des pools de postes de travail manuels

| Paramètre | Pool géré manuel, affectation dédiée | Pool géré manuel, affectation flottante | Pool non géré manuel, affectation dédiée | Pool non géré manuel, affectation flottante |
|---|---|---|---|---|
| État | Oui | Oui | Oui | Oui |
| Restrictions du serveur de connexion | Oui | Oui | Oui | Oui |
| Stratégie d'alimentation de machine distante | Oui | Oui | | |
| Automatically logoff after disconnect (Fermeture de session automatique après la déconnexion) | Oui | Oui | Oui | Oui |
| Autoriser les utilisateurs à réinitialiser leurs machines | Oui | Oui | | |
| Autoriser l'utilisateur à ouvrir des sessions séparées depuis différents périphériques clients | | Oui | | Oui |
| Protocole d'affichage par défaut | Oui | Oui | Oui<br>Pour utiliser PCoIP avec une machine n'est pas gérée par vCenter Server, vous devez installer le matériel Teradici sur la machine. | Oui<br>Pour utiliser PCoIP avec une machine n'est pas gérée par vCenter Server, vous devez installer le matériel Teradici sur la machine. |
| Autoriser les utilisateurs à choisir un protocole | Oui | Oui | Oui | Oui |
| Convertisseur 3D | Oui | Oui | | |
| Max number of monitors (Nombre max. d'écrans) | Oui | Oui | | |
| Max resolution of any one monitor (Résolution max. d'un écran) | Oui | Oui | | |
| Adobe Flash quality (Qualité Adobe Flash) | Oui | Oui | Oui | Oui |

**Tableau 7-2.** Paramètres des pools de postes de travail manuels (suite)

| Paramètre | Pool géré manuel, affectation dédiée | Pool géré manuel, affectation flottante | Pool non géré manuel, affectation dédiée | Pool non géré manuel, affectation flottante |
|---|---|---|---|---|
| Adobe Flash throttling (Limitation d'Adobe Flash) | Oui | Oui | Oui | Oui |
| Remplacer les paramètres de Mirage | Oui | Oui | Oui | Oui |
| Configuration du serveur Mirage | Oui | Oui | Oui | Oui |

# Configuration des hôtes de services Bureau à distance 8

Les hôtes des services Bureau à distance (RDS) Microsoft fournissent des sessions de postes de travail et des applications auxquelles les utilisateurs ont accès à partir de leur périphérique client. Si vous prévoyez de créer des pools de postes de travail ou des pools d'applications RDS, vous devez d'abord configurer des hôtes RDS.

Ce chapitre aborde les rubriques suivantes :



## Hôtes des services Bureau à distance

Un hôte RDS est un ordinateur serveur qui héberge des sessions d'applications et de postes de travail pour un accès distant. Un hôte RDS peut être une machine virtuelle ou un serveur physique.

Un hôte RDS dispose du rôle Services Bureau à distance Microsoft, du service Hôte de session Bureau à distance Microsoft et d'une installation d'Horizon Agent. Services Bureau à distance se nommait précédemment Services Terminal Server. Le service Hôte de session Bureau à distance permet à un serveur d'héberger des sessions d'applications et de postes de travail distants. Lorsqu'Horizon Agent est installé sur un hôte RDS, les utilisateurs peuvent se connecter aux sessions d'applications et de postes de travail à l'aide du protocole d'affichage PCoIP ou Blast Extreme. Les deux protocoles fournissent une expérience utilisateur optimisée pour la livraison de contenu distant, notamment des images, du son et des vidéos.

Les performances d'un hôte RDS dépendent de nombreux facteurs. Pour plus d'informations sur le réglage des performances des différentes versions de Windows Server, reportez-vous à http://msdn.microsoft.com/library/windows/hardware/gg463392.aspx.

Horizon 7 prend en charge au maximum une session de poste de travail et une session d'application par utilisateur sur un hôte RDS.

Lorsque les utilisateurs soumettent simultanément des travaux d'impression à partir d'applications ou de postes de travail RDS qui sont hébergés sur le même hôte RDS, le serveur ThinPrint sur l'hôte RDS traite les demandes d'impression en série et non en parallèle. Cela peut provoquer un retard pour certains utilisateurs. Notez que le serveur d'impression n'attend pas la fin d'un travail d'impression avant de traiter le suivant. Les travaux d'impression qui sont envoyés aux différentes imprimantes s'impriment en parallèle.

Si un utilisateur lance en même temps une application et un poste de travail RDS, et s'ils sont tous deux hébergés sur le même hôte RDS, ils partagent le même profil d'utilisateur. Si l'utilisateur lance une application à partir du poste de travail, des conflits peuvent être créés si les deux applications tentent d'accéder aux mêmes parties du profil d'utilisateur ou de les modifier, et l'une des applications risque de ne pas fonctionner correctement.

Le processus de configuration des applications ou des postes de travail RDS pour un accès distant implique les tâches suivantes :

1. Configurez les hôtes RDS.
2. Créez une batterie de serveurs. Reportez-vous à la section Chapitre 9, « Création de batteries de serveurs », page 129.
3. Créez un pool d'applications ou un pool de postes de travail RDS. Reportez-vous à la section Chapitre 10, « Création de pools d'applications », page 143 ou Chapitre 11, « Création de pools de postes de travail RDS », page 147.
4. Autoriser les utilisateurs et les groupes. Reportez-vous à la section Chapitre 13, « Autorisation d'utilisateurs et de groupes », page 187.
5. (Facultatif) Activer la redirection de fuseaux horaires pour les sessions de postes de travail et d'applications RDS. Reportez-vous à la section « Activer la redirection de fuseau horaire pour les sessions de postes de travail RDS et d'applications », page 123.

**Remarque** Si l'authentification par carte à puce est activée, assurez-vous que le service Smart Card est désactivé sur les hôtes RDS. Sinon, l'authentification peut échouer. Ce service est désactivé par défaut.

**Avertissement** Lorsqu'un utilisateur lance une application, par exemple un navigateur Web, il peut avoir accès aux lecteurs locaux de l'hôte RDS qui héberge l'application. Cela peut se produire si l'application met en œuvre des fonctions entraînant l'exécution de l'Explorateur Windows. Pour empêcher ce type d'accès à l'hôte RDS, suivez la procédure décrite dans la page http://support.microsoft.com/kb/179221 pour empêcher une application d'exécuter l'Explorateur Windows.

Comme la procédure décrite dans http://support.microsoft.com/kb/179221 affecte les sessions de postes de travail et d'applications, il est recommandé de ne pas créer de pools de postes de travail RDS et de pools d'applications sur la même batterie de serveurs si vous prévoyez de suivre la procédure de l'article de la base de connaissances Microsoft, afin que les sessions de postes de travail ne soient pas affectées.

## Installation d'applications

Si vous prévoyez de créer des pools d'applications, vous devez installer les applications sur les hôtes RDS. Si vous souhaitez qu'Horizon 7 affiche automatiquement la liste des applications installées, vous devez installer les applications de manière qu'elles soient disponibles à tous les utilisateurs à partir du menu **Démarrer**. Vous pouvez installer une application à tout moment avant de créer le pool d'applications. Si vous prévoyez de spécifier manuellement une application, vous pouvez installer l'application à tout moment, avant ou après la création d'un pool d'applications.

---

**Important** Lorsque vous installez une application, vous devez l'installer sur tous les hôtes RDS dans une batterie de serveurs au même emplacement sur chaque hôte RDS. Si vous ne le faites pas, un avertissement de santé s'affiche dans le tableau de bord de View Administrator. Dans ce cas, si vous créez un pool d'applications, les utilisateurs peuvent rencontrer une erreur lorsqu'ils tentent d'exécuter l'application.

---

Lorsque vous créez un pool d'applications, Horizon 7 affiche automatiquement les applications qui sont accessibles à tous les utilisateurs plutôt qu'à des utilisateurs individuels à partir du menu **Démarrer** sur tous les hôtes RDS d'une batterie de serveurs. Vous pouvez choisir n'importe quelle application dans cette liste. En outre, vous pouvez spécifier manuellement une application qui n'est pas disponible à tous les utilisateurs à partir du menu **Démarrer**. Il n'y a pas de limite quant au nombre d'applications que vous pouvez installer sur un hôte RDS.

# Installer les services Bureau à distance sur Windows Server 2008 R2

Les services Bureau à distance constituent l'un des rôles dont peut disposer Windows Server. Vous devez installer ce rôle pour configurer un hôte RDS qui exécute Windows Server 2008 R2.

### Prérequis

- Vérifiez que l'hôte RDS exécute Windows Server 2008 R2 Service Pack 1 (SP1).
- Vérifiez que l'hôte RDS fait partie du domaine Active Directory pour le déploiement d'Horizon 7.
- Installez le correctif cumulatif Microsoft documenté dans http://support.microsoft.com/kb/2775511.
- Installez la mise à jour Microsoft https://support.microsoft.com/en-us/kb/2973201.

### Procédure

1. Connectez-vous à l'hôte RDS en tant qu'administrateur.
2. Démarrez le gestionnaire de serveurs.
3. Sélectionnez **Rôles** dans l'arborescence de navigation.
4. Cliquez sur **Ajouter des rôles** pour démarrer l'assistant Ajouter un rôle.
5. Sélectionnez le rôle **Services Bureau à distance**.
6. Sur la page Sélectionner les services de rôle, sélectionnez **Hôte de session Bureau à distance**.
7. Dans la page Spécifier une méthode d'authentification, sélectionnez **Exiger l'authentification au niveau du réseau** ou **Ne nécessite pas l'authentification au niveau du réseau**, selon le cas.
8. Dans la page Configurer l'expérience client, sélectionnez la fonctionnalité que vous souhaitez fournir aux utilisateurs.
9. Suivez les invites et terminez l'installation.

### Suivant

Si vous prévoyez d'utiliser HTML Access ou une redirection de scanner, installez la fonctionnalité Expérience de poste de travail. Les étapes pour installer Expérience de poste de travail diffèrent sur Windows Server 2008 R2 et Windows Server 2012 ou 2012 R2.

Limitez les utilisateurs à une seule session de poste de travail. Reportez-vous à la section « Limiter les utilisateurs à une seule session », page 119.

## Installer les services Bureau à distance sur Windows Server 2012 ou 2012 R2

Les services Bureau à distance constituent l'un des rôles dont peut disposer Windows Server 2012 ou 2012 R2 Vous devez installer ce rôle pour configurer un hôte RDS.

### Prérequis

- Vérifiez que l'hôte RDS exécute Windows Server 2012 ou Windows Server 2012 R2.
- Vérifiez que l'hôte RDS fait partie du domaine Active Directory pour le déploiement d'Horizon 7.

### Procédure

1. Connectez-vous à l'hôte RDS en tant qu'administrateur.
2. Démarrez le gestionnaire de serveurs.
3. Sélectionnez **Ajouter des rôles et des fonctionnalités**.
4. Sur la page Sélectionner un type d'installation, sélectionnez **Installation basée sur des rôles ou des fonctionnalités**.
5. Sur la page Sélectionner le serveur de destination, sélectionnez un serveur.
6. Sur la page Sélectionner des rôles de serveur, sélectionnez **Services Bureau à distance**.
7. Sur la page Sélectionner les fonctionnalités, acceptez les valeurs par défaut.
8. Sur la page Sélectionner les services de rôle, sélectionnez **Hôte de session Bureau à distance**.
9. Suivez les invites et terminez l'installation.

### Suivant

Si vous prévoyez d'utiliser HTML Access ou une redirection de scanner, installez la fonctionnalité Expérience de poste de travail. Les étapes pour installer Expérience de poste de travail diffèrent sur Windows Server 2008 R2 et Windows Server 2012 ou 2012 R2.

Limitez les utilisateurs à une seule session de poste de travail. Reportez-vous à la section « Limiter les utilisateurs à une seule session », page 119.

## Installer la fonctionnalité Expérience utilisateur sur Windows Server 2008 R2

Pour les postes de travail et applications RDS, et pour les postes de travail VDI déployés sur des machines virtuelles mono-utilisateur s'exécutant sous Windows Server, la redirection de scanner requiert l'installation de la fonctionnalité Expérience de poste de travail sur les hôtes RDS et les machines virtuelles mono-utilisateur.

### Procédure

1. Connectez-vous en tant qu'administrateur.
2. Démarrez le gestionnaire de serveurs.

3 Cliquez sur **Fonctionnalités**.

4 Cliquez sur **Ajouter des fonctionnalités**.

5 Sur la page Sélectionner les fonctionnalités, cochez la case **Expérience de poste de travail**.

6 Examinez les informations relatives aux autres fonctionnalités requises par la fonctionnalité Expérience de poste de travail, puis cliquez sur **Ajouter les fonctionnalités requises**.

7 Suivez les invites et terminez l'installation.

## Installer la fonctionnalité Expérience utilisateur sur Windows Server 2012 ou 2012 R2

Pour les postes de travail et applications RDS, et pour les postes de travail VDI déployés sur des machines virtuelles mono-utilisateur s'exécutant sous Windows Server, la redirection de scanner requiert l'installation de la fonctionnalité Expérience de poste de travail sur les hôtes RDS et les machines virtuelles mono-utilisateur.

Windows Server 2012 et Windows Server 2012 R2 sont pris en charge sur les machines utilisées comme hôtes RDS. Windows Server 2012 R2 est pris en charge sur des machines mono-utilisateur :

### Procédure

1 Connectez-vous en tant qu'administrateur.

2 Démarrez le gestionnaire de serveurs.

3 Sélectionnez **Ajouter des rôles et des fonctionnalités**.

4 Sur la page Sélectionner un type d'installation, sélectionnez **Installation basée sur des rôles ou des fonctionnalités**.

5 Sur la page Sélectionner le serveur de destination, sélectionnez un serveur.

6 Sur la page Sélectionner des rôles de serveur, acceptez la sélection par défaut, puis cliquez sur **Suivant**.

7 Sur la page Sélectionner les fonctionnalités, sous **Interfaces utilisateur et infrastructure**, sélectionnez **Expérience de poste de travail**.

8 Suivez les invites et terminez l'installation.

## Limiter les utilisateurs à une seule session

Horizon 7 prend en charge au maximum une session de poste de travail et une session d'application par utilisateur sur un hôte RDS. Vous devez configurer l'hôte RDS pour limiter les utilisateurs à une seule session. Pour Windows Server 2008 R2, Windows Server 2012 et Windows Server 2012 R2, vous pouvez limiter les utilisateurs à une seule session en activant le paramètre de stratégie de groupe `Restrict Remote Desktop Services users to a single Remote Desktop Services session`. Ce paramètre est situé dans le dossier `Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections`. Pour Windows Server 2008 R2, vous pouvez également utiliser la procédure suivante pour limiter les utilisateurs à une seule session.

### Prérequis

- Installez le rôle des services Bureau à distance (RDS), comme expliqué dans « Installer les services Bureau à distance sur Windows Server 2008 R2 », page 117.

### Procédure

1 Cliquez sur **Démarrer > Outils d'administration > Services Bureau à distance > Configuration d'hôte de session Bureau à distance**.

2 Dans le volet Modifier les paramètres, sous Général, double-cliquez sur **Restreindre chaque utilisateur à une seule session**.

3 Dans la boîte de dialogue Propriétés, dans l'onglet Général, sélectionnez **Restreindre chaque utilisateur à une seule session** et cliquez sur **OK**.

### Suivant

Installez Horizon Agent sur l'hôte RDS. Reportez-vous à la section « Installer Horizon Agent sur un hôte des services Bureau à distance (Remote Desktop Services, RDS) », page 120.

## Installer Horizon Agent sur un hôte des services Bureau à distance (Remote Desktop Services, RDS)

Horizon Agent communique avec le Serveur de connexion et prend en charge les protocoles d'affichage PCoIP et Blast Extreme. Vous devez installer Horizon Agent sur un hôte RDS.

### Prérequis

- Installez le rôle des services Bureau à distance (RDS), comme expliqué dans « Installer les services Bureau à distance sur Windows Server 2008 R2 », page 117 ou « Installer les services Bureau à distance sur Windows Server 2012 ou 2012 R2 », page 118.
- Limitez les utilisateurs à une seule session de poste de travail. Reportez-vous à la section « Limiter les utilisateurs à une seule session », page 119.
- Familiarisez-vous avec les options d'installation personnalisée d'Horizon Agent. Reportez-vous à la section « Options d'installation personnalisée d'Horizon Agent pour un hôte RDS », page 121.
- Si le module Microsoft Visual C++ Redistributable est installé sur la machine, vérifiez que la version du module est 2005 SP1 ou version ultérieure. Si la version du module est 2005 ou versions antérieures, vous pouvez effectuer la mise à niveau ou désinstaller le module.
- Téléchargez le fichier du programme d'installation d'Horizon Agent sur la page des produits VMware, à l'adresse http://www.vmware.com/go/downloadview.

### Procédure

1 Connectez-vous en tant qu'administrateur.

2 Pour démarrer le programme d'installation d'Horizon Agent, double-cliquez sur le fichier du programme d'installation.

   Le nom de fichier du programme d'installation est `VMware-viewagent-x86_64-y.y.y-xxxxxx.exe`, où *y.y.y* est le numéro de version et *xxxxxx* le numéro de build.

3 Sélectionnez la version du protocole Internet (**IPv4** ou **IPv6**).

   Vous devez installer tous les composants View avec la même version IP.

4 Sélectionnez les options d'installation personnalisée désirées.

   Ne sélectionnez pas l'option View Composer Agent si vous installez Horizon Agent sur un hôte RDS qui se trouvera dans une batterie de serveurs manuelle.

5 Dans la zone de texte **Serveur**, tapez le nom d'hôte ou l'adresse IP d'un hôte du Serveur de connexion.

   Lors de l'installation, le programme d'installation inscrit l'hôte RDS dans cette instance du Serveur de connexion. Après l'inscription, l'instance du Serveur de connexion spécifiée et toutes les instances supplémentaires incluses dans le même groupe que le Serveur de connexion peuvent communiquer avec l'hôte RDS.

6 Sélectionnez une méthode d'authentification pour inscrire l'hôte RDS dans l'instance du Serveur de connexion.

| Option | Description |
|---|---|
| **Authenticate as the currently logged in user (S'authentifier comme étant l'utilisateur actuellement connecté)** | Les zones de texte **Nom d'utilisateur** et **Mot de passe** sont désactivées et vous êtes connecté à l'instance du Serveur de connexion avec vos nom d'utilisateur et mot de passe actuels. |
| **Specify administrator credentials (Spécifier des informations d'identification d'administrateur)** | Vous devez fournir le nom d'utilisateur et le mot de passe d'un administrateur du Serveur de connexion dans les zones de texte **Nom d'utilisateur** et **Mot de passe**. |

Le compte d'utilisateur doit être un utilisateur de domaine ayant un accès à View LDAP sur l'instance du Serveur de connexion View. Un utilisateur local ne fonctionne pas.

7 Suivez les invites et terminez l'installation.

### Suivant

Créez une batterie de serveurs. Reportez-vous à la section Chapitre 9, « Création de batteries de serveurs », page 129.

## Options d'installation personnalisée d'Horizon Agent pour un hôte RDS

Lorsque vous installez Horizon Agent sur un hôte RDS, vous pouvez sélectionner des options d'installation personnalisées. En outre, Horizon Agent installe automatiquement certaines fonctionnalités sur tous les systèmes d'exploitation invités sur lesquels elles sont prises en charge. Ces fonctionnalités ne sont pas facultatives.

Pour modifier des options d'installation personnalisée après avoir installé la dernière version d'Horizon Agent, vous devez désinstaller et réinstaller Horizon Agent. Pour les correctifs et les mises à niveau, vous pouvez exécuter le nouveau programme d'installation d'Horizon Agent et sélectionner un nouvel ensemble d'options sans désinstaller la version précédente.

**Tableau 8-1.** Options d'installation personnalisée d'Horizon Agent pour un hôte RDS dans un environnement IPv4

| Option | Description |
|---|---|
| Redirection USB | Donne aux utilisateurs un accès aux périphériques de stockage USB localement connectés.<br>Spécifiquement, la redirection de lecteurs flash USB et de disques durs est prise en charge sur les postes de travail et les applications RDS. La redirection d'autres types de périphériques USB (par exemple, d'autres types de périphériques de stockage USB tels que des lecteurs de stockage de sécurité et des CD-ROM USB) n'est pas prise en charge dans les postes de travail et les applications RDS.<br>Cette option n'est pas sélectionnée par défaut. Vous devez sélectionner l'option pour l'installer. Cette option est disponible sur les hôtes RDS qui exécutent Windows Server 2012 ou 2012 R2 mais pas Windows Server 2008 R2.<br>Pour obtenir des instructions sur l'utilisation de la redirection USB en toute sécurité, reportez-vous au guide *Sécurité de View*. Par exemple, vous pouvez utiliser les paramètres de stratégie de groupe pour désactiver une redirection USB pour des utilisateurs spécifiques. |
| HTML Access | Permet aux utilisateurs de se connecter à des postes de travail et applications RDS en utilisant HTML Access. L'agent HTML Access est installé lorsque cette option d'installation est sélectionnée. Cet agent doit être installé sur des hôtes RDS pour permettre aux utilisateurs d'établir des connexions avec HTML Access. |
| 3D RDSH | Offre la prise en charge des graphiques 3D pour les applications exécutées sur cet hôte RDS. |
| View Composer Agent | Sélectionnez cette option si cette machine est une machine virtuelle parente pour la création d'une batterie de serveurs automatisée. Ne sélectionnez pas cette option si cette machine est un hôte RDS dans une batterie de serveurs manuelle. |

**Tableau 8-1.** Options d'installation personnalisée d'Horizon Agent pour un hôte RDS dans un environnement IPv4 (suite)

| Option | Description |
|---|---|
| Redirection de lecteur client | Permet aux utilisateurs d'Horizon Client de partager des lecteurs locaux avec leurs postes de travail et applications RDS.<br>Une fois cette option d'installation installée, aucune autre configuration n'est requise sur l'hôte RDS.<br>La redirection de lecteur client est également prise en charge sur les postes de travail VDI exécutés sur des machines virtuelles mono-utilisateur et des machines non gérées. |
| Impression virtuelle | Permet aux utilisateurs d'imprimer sur n'importe quelle imprimante disponible sur leurs ordinateurs clients. Les utilisateurs n'ont pas à installer des pilotes supplémentaires sur leurs postes de travail.<br>Dans Horizon 6.0.1 et version ultérieure, l'impression virtuelle est prise en charge sur les applications et les postes de travail distants suivants :<br>■ Postes de travail qui sont déployés sur des machines mono-utilisateur, notamment les machines postes de travail Windows et Windows Server<br>■ Postes de travail qui sont déployées sur des hôtes RDS, où les hôtes RDS sont des machines virtuelles<br>■ applications hébergées ;<br>■ Applications hébergées qui sont lancées à partir d'Horizon Client à l'intérieur de postes de travail distants<br>Dans Horizon 6.0 et version antérieure, l'impression virtuelle est prise en charge sur les postes de travail qui sont déployés sur des machines de poste de travail mono-utilisateur.<br>La fonction d'impression virtuelle n'est prise en charge que lorsque vous l'installez à partir d'Horizon Agent. Elle n'est pas prise en charge si vous l'installez avec VMware Tools. |
| vRealize Operations Desktop Agent | Permet à vRealize Operations Manager de fonctionner avec vRealize Operations Manager for Horizon. |
| Redirection de scanner | Permet de rediriger les périphériques d'analyse connectés au système client pour qu'ils puissent être utilisés sur l'application ou le poste de travail RDS.<br>Vous devez installer la fonctionnalité Expérience de poste de travail dans le système d'exploitation Windows Server sur les hôtes RDS pour rendre cette option disponible dans le programme d'installation d'Horizon Agent.<br>Cette option de configuration n'est pas installée par défaut sur les systèmes d'exploitation invités Windows Server. Vous devez sélectionner l'option pour l'installer.<br>La redirection de scanner est disponible dans Horizon 6.0.2 et versions ultérieures. |

Dans un environnement IPv6, il n'y a pas de fonctionnalités facultatives.

**Tableau 8-2.** Fonctionnalités d'Horizon Agent installées automatiquement sur un hôte RDS

| Option | Description |
|---|---|
| PCoIP Agent | Permet aux utilisateurs de se connecter à des applications et à des postes de travail RDS à l'aide du protocole d'affichage PCoIP.<br>Vous devez installer ce composant si vous prévoyez de créer des pools d'applications, car les utilisateurs peuvent uniquement se connecter aux applications à l'aide de PCoIP. |
| Redirection multimédia Windows Media (MMR) | Fournit la redirection multimédia aux postes de travail RDS. Cette fonctionnalité délivre le flux multimédia directement aux ordinateurs client, permettant au flux multimédia d'être traité sur le matériel client plutôt que sur l'hôte ESXi distant. |
| Unity Touch | Permet aux utilisateurs de tablette et de smartphone d'entrer en interaction avec les applications Windows qui s'exécutent sur le poste de travail distant. Les utilisateurs peuvent parcourir, rechercher et ouvrir des applications et des fichiers Windows, choisir des applications et des fichiers favoris, et basculer entre les applications en cours d'exécution sans utiliser le menu Démarrer ni la barre des tâches. |

**Tableau 8-2.** Fonctionnalités d'Horizon Agent installées automatiquement sur un hôte RDS (suite)

| Option | Description |
|---|---|
| PSG Agent | Installe PCoIP Secure Gateway sur des hôtes RDS pour mettre en œuvre le protocole d'affichage PCoIP pour des sessions de poste de travail et d'application qui s'exécutent sur des hôtes RDS. |
| VMwareRDS | Fournit la mise en œuvre VMware de la fonctionnalité Services Bureau à distance. |

Dans un environnement IPv6, les fonctionnalités installées automatiquement sont PCoIP Agent, PSG Agent et VMwareRDS.

Pour découvrir d'autres fonctionnalités prises en charge sur les hôtes RDS, consultez la section « Matrice de prise en charge des fonctionnalités pour Horizon Agent » dans le document *Planification de l'architecture de View*.

## Activer la redirection de fuseau horaire pour les sessions de postes de travail RDS et d'applications

Si un hôte RDS et un utilisateur se trouvent dans deux fuseaux horaires distincts, lorsque l'utilisateur se connecte à un poste de travail RDS, celui-ci affiche l'heure du fuseau horaire de l'hôte RDS. Vous pouvez activer le paramètre de stratégie de groupe Redirection de fuseau horaire pour faire afficher au poste de travail RDS l'heure du fuseau horaire local. Ce paramètre de stratégie s'applique également à des sessions d'application.

### Prérequis

- Vérifiez que la fonctionnalité Gestion de stratégie de groupe est disponible sur votre serveur Active Directory.

  La procédure d'ouverture de la Console de gestion de stratégie de groupe varie entre les versions Windows 2012, Windows 2008 et Windows 2003 d'Active Directory. Reportez-vous à la section « Créer des GPO pour les stratégies de groupe View », page 348.

- Vérifiez que les fichiers d'administration ADMX RDS d'Horizon 7 sont ajoutés à Active Directory. Reportez-vous à la section « Ajouter les fichiers ADMX des services Bureau à distance à Active Directory », page 330.

- Familiarisez-vous avec les paramètres de stratégie de groupe. Reportez-vous à la section « Paramètres de redirection de ressources et de périphériques RDS », page 334.

### Procédure

1. Sur le serveur Active Directory, ouvrez la Console de gestion de stratégie de groupe.
2. Développez votre domaine et les **Objets de stratégie de groupe**.
3. Cliquez avec le bouton droit sur le GPO que vous avez créé pour les paramètres de stratégie de groupe et sélectionnez **Modifier**.
4. Dans l'Éditeur de gestion de stratégie de groupe, accédez à **Configuration de l'ordinateur > Règles > Modèles d'administration > Composants Windows > Services RDSH Horizon View > Hôte de session de poste de travail distant > Redirection de périphériques et de ressources**.
5. Activez le paramètre **Autoriser la redirection de fuseau horaire**.

## Activer le thème de style de base Windows pour les applications

Si un utilisateur ne s'est jamais connecté à un poste de travail sur un hôte RDS et qu'il lance une application hébergée sur l'hôte RDS, le thème de base Windows n'est pas appliqué à l'application, même si un paramètre de GPO est configuré pour charger le thème de style Aero. Horizon 7 ne prend pas en charge le thème de style Aero, mais prend en charge le thème de base Windows. Pour que le thème de base Windows s'applique à l'application, vous devez configurer un autre paramètre GPO.

### Prérequis

- Vérifiez que la fonctionnalité Gestion de stratégie de groupe est disponible sur votre serveur Active Directory.

  La procédure d'ouverture de la Console de gestion de stratégie de groupe varie entre les versions Windows 2012, Windows 2008 et Windows 2003 d'Active Directory. Reportez-vous à la section « Créer des GPO pour les stratégies de groupe View », page 348.

### Procédure

1. Sur le serveur Active Directory, ouvrez la Console de gestion de stratégie de groupe.
2. Développez votre domaine et les **Objets de stratégie de groupe**.
3. Cliquez avec le bouton droit sur le GPO que vous avez créé pour les paramètres de stratégie de groupe et sélectionnez **Modifier**.
4. Dans l'Éditeur de gestion des stratégies de groupe, accédez à **Configuration utilisateur > Stratégies > Modèles d'administration > Panneau de configuration > Personnalisation**.
5. Activez le paramètre **Forcer un fichier de style visuel spécifique ou forcer le style Windows Classique** et définissez le chemin d'accès du style visuel sur `%windir%\resources\Themes\Aero\aero.msstyles`.

## Configurer une stratégie de groupe pour démarrer Runonce.exe

Par défaut, certaines applications qui reposent sur le fichier Explorer.exe peuvent ne pas fonctionner dans une session d'application. Pour éviter ce problème, vous devez configurer un paramètre de GPO permettant de démarrer runonce.exe.

### Prérequis

- Vérifiez que la fonctionnalité Gestion de stratégie de groupe est disponible sur votre serveur Active Directory.

  La procédure d'ouverture de la Console de gestion de stratégie de groupe varie entre les versions Windows 2012, Windows 2008 et Windows 2003 d'Active Directory. Reportez-vous à la section « Créer des GPO pour les stratégies de groupe View », page 348.

### Procédure

1. Sur le serveur Active Directory, ouvrez la Console de gestion de stratégie de groupe.
2. Développez votre domaine et les **Objets de stratégie de groupe**.
3. Cliquez avec le bouton droit sur le GPO que vous avez créé pour les paramètres de stratégie de groupe et sélectionnez **Modifier**.
4. Dans l'Éditeur de gestion des stratégies de groupes, accédez à **Configuration utilisateur > Règles > Paramètres Windows > Scripts (ouverture/fermeture de session)**.
5. Double-cliquez sur **Connexion**, puis cliquez sur **Ajouter**.
6. Dans la case Nom du script, tapez `runonce.exe`.

7 Dans la case Paramètres du script, tapez **`/AlternateShellStartup`**.

## Options de performances d'Hôte de session Bureau à distance

Vous pouvez optimiser Windows pour les programmes d'avant-plan ou les services d'arrière-plan en définissant des options de performances. Par défaut, Horizon 7 désactive certaines options de performances pour les hôtes RDS pour toutes les versions prises en charge de Windows Server.

Le tableau suivant montre les options de performances qui sont désactivées par Horizon 7.

**Tableau 8-3.** Options de performances désactivées par Horizon 7

| Options de performances désactivées par Horizon 7 |
|---|
| Animer les fenêtres lors de leur réduction et de leur agrandissement |
| Afficher des ombres sous le pointeur de la souris |
| Afficher une ombre sous les fenêtres |
| Utiliser des ombres portées pour le nom des icônes sur le Bureau |
| Afficher le contenu des fenêtres pendant leur déplacement |

Les cinq options de performances qui sont désactivées par Horizon 7 correspondent à quatre paramètres d'Horizon 7 dans le Registre. Le tableau suivant montre les paramètres d'Horizon 7 et leurs valeurs de Registre par défaut. Les valeurs de Registre se trouvent toutes dans la sous-clé du Registre `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration`. Vous pouvez réactiver les options de performances en définissant une ou plusieurs des valeurs de Registre d'Horizon 7 sur **`false`**.

**Tableau 8-4.** Paramètres d'Horizon 7 associés aux options de performances Windows

| Paramètre d'Horizon 7 | Valeur de Registre |
|---|---|
| Désactiver l'ombre du curseur | DisableMouseShadows |
| Désactiver l'affichage du déplacement des fenêtres | DisableFullWindowDrag |
| Désactiver l'ombre ListView | DisableListViewShadow |
| Désactiver l'animation des fenêtres | DisableWindowAnimation |

# Configuration de graphiques 3D pour les hôtes RDS

Avec les graphiques 3D configurés pour les hôtes RDS, les applications dans des pools d'applications et les applications exécutées sur des postes de travail RDS peuvent afficher des graphiques 3D.

Les options graphiques 3D suivantes sont disponibles :

**NVIDIA GRID vGPU (accélération matérielle GPU partagée)**
Un GPU physique sur un hôte ESXi est partagé entre plusieurs machines virtuelles. Requiert ESXi 6.0 ou version ultérieure.

**GPU multi-utilisateur AMD utilisant vDGA**
Un GPU physique sur un hôte ESXi est partagé entre plusieurs machines virtuelles. Requiert ESXi 6.0 ou version ultérieure.

**vDGA (Virtual Dedicated Graphics Acceleration)**
Un GPU physique sur un hôte ESXi est dédié à une seule machine virtuelle. Requiert ESXi 5.5 ou version ultérieure.

> **Remarque** Certaines cartes Intel vDGA requièrent une version spécifique de vSphere 6. Consultez la liste de compatibilité matérielle VMware à l'adresse http://www.vmware.com/resources/compatibility/search.php. De plus, pour Intel vDGA, le GPU intégré Intel est utilisé à la place de GPU discrets, comme c'est le cas avec d'autres fournisseurs.

Avec vDGA, vous allouez un GPU entier à une seule machine pour des performances maximales. L'hôte RDS doit se trouver dans une batterie de serveurs manuelle.

Avec le GPU multi-utilisateur AMD utilisant vDGA, vous pouvez partager un GPU AMD entre plusieurs hôtes RDS en le faisant apparaître sous la forme de plusieurs périphériques de relais PCI. L'hôte RDS doit se trouver dans une batterie de serveurs manuelle.

Avec NVIDIA GRID VGPU, chaque carte graphique peut prendre en charge plusieurs hôtes RDS et les hôtes RDS doivent se trouver dans une batterie de serveurs manuelle. Si un hôte ESXi contient plusieurs GPU physiques, vous pouvez également configurer la façon dont l'hôte ESXi attribue des machines virtuelles aux GPU. Par défaut, l'hôte ESXi attribue des machines virtuelles au GPU physique contenant le moins de machines virtuelles déjà attribuées. Il s'agit du mode de performances. Vous pouvez également choisir le mode de consolidation, où l'hôte ESXi attribue des machines virtuelles au même GPU physique jusqu'à atteindre le nombre maximal de machines virtuelles avant de placer des machines virtuelles sur le prochain GPU physique. Pour configurer le mode de consolidation, modifiez le fichier `/etc/vmware/config` sur l'hôte ESXi et ajoutez l'entrée suivante :

```
vGPU.consolidation = "true"
```

Les graphiques 3D ne sont pris en charge que lorsque vous utilisez le protocole PCoIP ou VMware Blast. Par conséquent, la batterie de serveurs doit utiliser PCoIP ou VMware Blast comme protocole par défaut et les utilisateurs ne doivent pas être autorisés à choisir le protocole.

## Présentation des étapes de configuration des graphiques 3D

Cette présentation décrit les tâches que vous devez réaliser dans vSphere et Horizon 7 pour configurer des graphiques 3D. Pour plus d'informations sur la configuration de NVIDIA GRID vGPU, consultez le document Guide de déploiement de NVIDIA GRID vGPU pour VMware Horizon 6.1. Pour plus d'informations sur la configuration de vDGA, consultez le document Accélération graphique sur les postes de travail virtuels View. Pour plus d'informations sur la configuration du GPU multi-utilisateur AMD utilisant vDGA, reportez-vous à la section « Préparation de l'utilisation des capacités du GPU multi-utilisateur AMD utilisant vDGA », page 181.

1 Configurez une machine virtuelle d'hôte RDS. Pour plus d'informations, reportez-vous à la section Chapitre 8, « Configuration des hôtes de services Bureau à distance », page 115.

2 Ajoutez le périphérique PCI graphique à la machine virtuelle. Voir « Autre configuration de périphérique de machine virtuelle » dans le chapitre « Configuration du matériel de machine virtuelle » dans le document *Administration d'une machine virtuelle vSphere*. Veillez à cliquer sur **Réserver toute la mémoire** lors de l'ajout du périphérique.

3 Sur la machine virtuelle, installez le pilote de périphérique pour la carte graphique.

4 Ajoutez l'hôte RDS à une batterie de serveurs manuelle, créez un pool de postes de travail RDS, connectez-vous au poste de travail avec PCoIP et activez la carte vidéo.

Vous n'avez pas à configurer les graphiques 3D pour les hôtes RDS dans View Administrator. La sélection de l'option **RDSH 3D** lorsque vous installez Horizon Agent est suffisante. Par défaut, cette option n'est pas sélectionnée et les graphiques 3D sont désactivés.

# Création de batteries de serveurs 9

Une batterie de serveurs est un groupe d'hôtes RDS qui fournit un ensemble commun d'applications ou de postes de travail RDS à des utilisateurs.

Ce chapitre aborde les rubriques suivantes :



## Batteries de serveurs

Les batteries de serveurs simplifient la tâche de gestion des hôtes RDS, des postes de travail RDS et des applications dans une entreprise. Vous pouvez créer des batteries de serveurs manuelles ou automatisées pour servir des groupes d'utilisateurs de taille variable ou ayant différents besoins en termes de postes de travail ou d'applications.

Une batterie de serveurs manuelle se compose d'hôtes RDS qui existent déjà. Les hôtes RDS peuvent être des machines physiques ou virtuelles. Vous ajoutez manuellement les hôtes RDS lorsque vous créez la batterie de serveurs.

Une batterie de serveurs automatisée se compose d'hôtes RDS qui sont des machines virtuelles de clone lié dans vCenter Server. View Composer crée les machines virtuelles en fonction des paramètres que vous spécifiez lorsque vous créez la batterie de serveurs. Les machines virtuelles sont clonées à partir d'une seule machine virtuelle parente et sont liées au parent dans un mécanisme qui réduit la quantité de stockage dont les machines virtuelles ont besoin.

Lorsque vous créez un pool d'applications ou un pool de postes de travail RDS, vous devez spécifier une seule et unique batterie de serveurs. Les hôtes RDS d'une batterie de serveurs peuvent héberger des postes de travail RDS, des applications, ou les deux. Une batterie de serveurs peut prendre en charge un seul pool de postes de travail RDS, mais plusieurs pools d'applications. Une batterie de serveurs peut prendre en charge les deux types de pools simultanément.

Les batteries de serveurs offrent les fonctionnalités suivantes :

- Équilibrage de charge

Par défaut, Horizon 7 équilibre la charge des sessions de postes de travail RDS et des sessions d'application entre tous les hôtes RDS de la batterie de serveurs. Vous pouvez contrôler le placement de nouvelles sessions d'application en écrivant et en configurant des scripts d'équilibrage de charge. Pour plus d'informations, consultez « Configuration de l'équilibrage de charge pour des hôtes RDS » dans le document *Administration de View*.

- Redondance

  Si un hôte RDS d'une batterie de serveurs est hors connexion, les autres hôtes RDS de la batterie de serveurs continuent à fournir des applications et des postes de travail aux utilisateurs.

- Évolutivité

  Une batterie de serveurs peut comporter un nombre variable d'hôtes RDS. Vous pouvez créer des batteries de serveurs comportant différents nombres d'hôtes RDS pour servir des groupes d'utilisateurs de tailles différentes.

Les batteries de serveurs ont les propriétés suivantes :

- Un espace Horizon 7 peut disposer d'un maximum de 200 batteries de serveurs.
- Une batterie de serveurs peut disposer d'un maximum de 200 hôtes RDS.
- Les hôtes RDS d'une batterie de serveurs peuvent exécuter n'importe quelle version prise en charge de Windows Server. Reportez-vous à la section « Configuration requise pour les systèmes d'exploitation invités » dans le document *Installation de View*.
- Les batteries de serveurs automatisées prennent en charge l'opération de recomposition View Composer mais pas l'opération d'actualisation ou de rééquilibrage. Vous pouvez recomposer une batterie de serveurs automatisée mais pas un sous-ensemble des hôtes RDS dans la batterie de serveurs.

**Important** Microsoft recommande de configurer des profils itinérants pour les utilisateurs séparément pour chaque batterie de serveurs. Les profils ne doivent pas être partagés entre des batteries de serveurs ou les postes de travail physiques d'utilisateurs, car une altération de profil et une perte de données peuvent se produire si un utilisateur se connecte simultanément à deux machines qui chargent le même profil.

## Préparation d'une machine virtuelle parente pour une batterie de serveurs automatisée

Pour créer une batterie de serveurs automatisée, vous devez d'abord préparer une machine virtuelle parente. View Composer utilise cette machine virtuelle parente pour créer des machines virtuelles de clone lié, qui sont les hôtes RDS dans la batterie de serveurs.

- Préparer une machine virtuelle parente d'hôte RDS page 131

  Le service View Composer requiert une machine virtuelle parente à partir de laquelle vous générez une image de base pour créer des clones liés.

- Activation de Windows sur des hôtes RDS de clone lié page 133

  Pour vous assurer que View Composer active correctement les systèmes d'exploitation Windows Server sur des hôtes RDS de clone lié, vous devez utiliser l'activation en volume Microsoft sur la machine virtuelle parente. La technologie d'activation du volume requiert une clé de licence en volume.

- Désactiver la mise en veille prolongée Windows sur la machine virtuelle parente page 133

  La fonctionnalité de mise en veille prolongée Windows crée un fichier système masqué, `Hiberfil.sys`, et utilise ce fichier pour stocker des informations nécessaires pour la veille hybride. La désactivation de la mise en veille prolongée réduit la taille du disque virtuel d'un clone instantané ou d'un clone lié View Composer.

## Préparer une machine virtuelle parente d'hôte RDS

Le service View Composer requiert une machine virtuelle parente à partir de laquelle vous générez une image de base pour créer des clones liés.

### Prérequis

- Vérifiez qu'une machine virtuelle d'hôte RDS est configurée. Reportez-vous à la section Chapitre 8, « Configuration des hôtes de services Bureau à distance », page 115. Pour configurer l'hôte RDS, veillez à ne pas utiliser une machine virtuelle qui était précédemment enregistrée sur le Serveur de connexion View.

  Une machine virtuelle parente que vous utilisez pour View Composer doit appartenir au même domaine Active Directory que celui que les machines de clone lié joindront ou être membre du Groupe de travail local.

- Vérifiez que la machine virtuelle n'a pas été convertie depuis un clone lié View Composer. Une machine virtuelle convertie depuis un clone lié contient les informations de disque interne et d'état du clone. Une machine virtuelle parente ne peut pas contenir d'informations d'état.

  **Important** Les clones liés et les machines virtuelles qui ont été convertis depuis des clones liés ne sont pas pris en charge en tant que machines virtuelles parentes.

- Lorsque vous installez Horizon Agent sur la machine virtuelle parente, sélectionnez l'option **View Composer Agent**. Reportez-vous à la section « Installer Horizon Agent sur un hôte des services Bureau à distance (Remote Desktop Services, RDS) », page 120.

  Pour mettre à jour Horizon Agent dans un environnement volumineux, vous pouvez utiliser des mécanismes de mise à jour Windows standard comme Altiris, SMS, LanDesk, BMC ou d'autres logiciels de gestion des systèmes. Vous pouvez également utiliser l'opération de recomposition pour mettre à jour Horizon Agent.

  **Remarque** Ne modifiez pas le compte d'ouverture de session pour le service VMware View Composer Guest Agent Server dans une machine virtuelle parente. Par défaut, il s'agit du compte de système local. Si vous modifiez ce compte, les clones liés créés à partir du parent ne démarrent pas.

- Pour déployer des machines Windows, configurez une clé de licence en volume et activez le système d'exploitation de la machine virtuelle parente avec l'activation en volume. Reportez-vous à la section « Activation de Windows sur des clones instantanés et des clones liés View Composer », page 57.

- Familiarisez-vous avec la procédure de désactivation de la recherche de pilotes de périphérique de Windows Update. Consultez l'article de Microsoft Technet « Désactiver la recherche de pilotes de périphérique de Windows Update » à l'adresse http://technet.microsoft.com/en-us/library/cc730606(v=ws.10).aspx.

- Pour implémenter la fonction d'équilibrage de charge de l'hôte RDS, modifiez la machine virtuelle parente de l'hôte RDS comme décrit dans « Configuration de l'équilibrage de charge pour des hôtes RDS » dans le document *Administration de View*.

### Procédure

- Désactivez le bail DHCP sur la machine virtuelle parente pour empêcher la copie d'une adresse IP avec bail vers les clones liés de la batterie de serveurs.

  a Sur la machine virtuelle parente, ouvrez une invite de commande.

  b Saisissez la commande `ipconfig /release`.

- Vérifiez que le disque système contient un seul volume.

  Vous ne pouvez pas déployer de clones liés à partir d'une machine virtuelle parente contenant plusieurs volumes. Le service View Composer ne prend pas en charge les partitions de disque multiples. Plusieurs disques virtuels sont pris en charge.

- Vérifiez que la machine virtuelle ne contient pas de disque indépendant.

  Un disque indépendant est exclu lorsque vous prenez un snapshot de la machine virtuelle. Les clones liés qui sont créés ou recomposés à partir de la machine virtuelle ne contiendront pas le disque indépendant.

- Désactivez l'option de mise en veille prolongée pour réduire la taille des disques du système d'exploitation de clone lié créés à partir de la machine virtuelle parente.

- Avant de prendre un snapshot de la machine virtuelle parente, désactivez la recherche de pilotes de périphérique de Windows Update.

  Cette fonctionnalité Windows peut interférer avec la personnalisation des machines de clone lié. À chaque fois qu'un clone lié est personnalisé, Windows peut rechercher les meilleurs pilotes sur Internet pour ce clone, ce qui entraîne des recherches répétées et des retards de personnalisation.

- Dans vSphere Client, désactivez le paramètre vApp Options (Options vApp) sur la machine virtuelle parente.

- Sur les machines Windows Server 2008 R2 et Windows Server 2012 R2, désactivez la tâche de maintenance planifiée qui récupère de l'espace disque en supprimant des fonctionnalités inutilisées.

  Par exemple : `Schtasks.exe /change /disable /tn "\Microsoft\Windows\AppxDeploymentClient\Pre-staged app cleanup"`

  Si elle est maintenue activée, cette tâche de maintenance peut supprimer le script de personnalisation Sysprep après la création des clones liés, ce qui entraînerait l'échec des opérations de recomposition suivantes avec des erreurs d'expiration de délai de l'opération de personnalisation. Pour plus d'informations, reportez-vous à l'article de base de connaissances Microsoft disponible à l'adresse http://support.microsoft.com/kb/2928948.

- Sur des machines Windows Server 2012, appliquez le correctif Microsoft disponible à l'adresse https://support.microsoft.com/en-us/kb/3020396.

  Ce correctif permet à Sysprep de personnaliser une machine virtuelle Windows Server 2012 avec le rôle RDS activé. Sans le correctif, la personnalisation Sysprep échouera sur les machines de clone lié Windows Server 2012 qui sont déployées dans une batterie de serveurs automatisée.

### Suivant

Utilisez vSphere Client ou vSphere Web Client pour prendre un snapshot de la machine virtuelle parente dans son état hors tension. Ce snapshot sert de configuration de ligne de base pour le premier ensemble de machines de clone lié ancrées à la machine virtuelle parente.

---

**Important** Avant de prendre un snapshot, arrêtez complètement la machine virtuelle parente à l'aide de la commande **Arrêter** dans le système d'exploitation client.

---

## Activation de Windows sur des hôtes RDS de clone lié

Pour vous assurer que View Composer active correctement les systèmes d'exploitation Windows Server sur des hôtes RDS de clone lié, vous devez utiliser l'activation en volume Microsoft sur la machine virtuelle parente. La technologie d'activation du volume requiert une clé de licence en volume.

Pour activer Windows avec l'activation en volume, vous devez utiliser le service de gestion des clés (KMS, Key Management Service) qui nécessite une clé de licence KMS. Contactez votre revendeur Microsoft pour acquérir une clé de licence en volume et configurer l'activation du volume.

**Remarque** View Composer ne prend pas en charge la licence MAK (clé d'activation multiple).

Avant de créer des machines de clone lié avec View Composer, vous devez utiliser l'activation du volume pour activer le système d'exploitation sur la machine virtuelle parente.

Lors de la création d'une machine de clone lié, et à chaque recomposition du clone lié, l'agent View Composer utilise le serveur KMS de la machine virtuelle parente pour activer le système d'exploitation sur le clone lié.

Pour la licence KMS, View Composer utilise le serveur KMS configuré pour activer la machine virtuelle parente. Le serveur KMS traite un clone lié activé en tant qu'ordinateur avec une nouvelle licence émise.

## Désactiver la mise en veille prolongée Windows sur la machine virtuelle parente

La fonctionnalité de mise en veille prolongée Windows crée un fichier système masqué, `Hiberfil.sys`, et utilise ce fichier pour stocker des informations nécessaires pour la veille hybride. La désactivation de la mise en veille prolongée réduit la taille du disque virtuel d'un clone instantané ou d'un clone lié View Composer.

**Avertissement** Lorsque vous désactivez la mise en veille prolongée, la veille hybride ne fonctionne pas. Les utilisateurs peuvent perdre des données en cas de perte de puissance.

### Procédure

1. Dans vSphere Client, sélectionnez la machine virtuelle parente et sélectionnez **Ouvrir la console**.
2. Connectez-vous en tant qu'administrateur.
3. Désactivez l'option de mise en veille prolongée.
   a. Cliquez sur **Démarrer** et saisissez **`cmd`** dans la zone **Rechercher**.
   b. Dans la liste de résultats de la recherche, cliquez avec le bouton droit sur **Invite de commandes** et cliquez sur **Exécuter en tant qu'administrateur**.
   c. À l'invite Contrôle de compte d'utilisateur, cliquez sur **Continuer**.
   d. À l'invite de commande, saisissez **`powercfg.exe /hibernate off`** et appuyez sur Entrée.
   e. Saisissez **`exit`** et appuyez sur Entrée.

# Feuille de calcul pour la création d'une batterie de serveurs manuelle

Lorsque vous créez une batterie de serveurs manuelle, l'assistant Ajouter une batterie de serveurs vous invite à configurer certains paramètres.

Vous pouvez imprimer cette feuille de calcul et prendre note des valeurs que vous souhaitez spécifier quand vous exécutez l'assistant Ajouter une batterie de serveurs.

**Tableau 9-1.** Feuille de calcul : paramètres de configuration pour la création d'une batterie de serveurs manuelle

| Paramètre | Description | Indiquez votre valeur ici |
|---|---|---|
| ID | Nom unique qui identifie la batterie de serveurs dans View Administrator. | |
| Description | Description de cette batterie de serveurs. | |
| Groupe d'accès | Groupe d'accès dans lequel placer tous les pools de cette batterie de serveurs.<br>Pour plus d'informations sur l'accès aux groupes, consultez le chapitre sur l'administration déléguée basée sur des rôles dans le document *Administration de View*. | |
| Protocole d'affichage par défaut | Sélectionnez **VMware Blast**, **PCoIP** ou **RDP**. RDP s'applique aux pools de postes de travail uniquement. Le protocole d'affichage des pools d'applications est toujours **VMware Blast** ou **PCoIP**. Si vous sélectionnez **RDP** et que vous prévoyez d'utiliser cette batterie de serveurs pour héberger des pools d'applications, vous devez définir **Autoriser les utilisateurs à choisir un protocole** sur **Oui**. L'option par défaut est **PCoIP**. | |
| Autoriser les utilisateurs à choisir un protocole | Sélectionnez **Oui** ou **Non**. Ce paramètre ne s'applique qu'aux pools de postes de travail RDS. Si vous sélectionnez **Oui**, les utilisateurs peuvent choisir le protocole d'affichage quand ils se connectent à un poste de travail RDS depuis Horizon Client. La valeur par défaut est **Oui**. | |
| Délai d'expiration de session vide (applications seulement) | Détermine la durée pendant laquelle une session d'application vide est laissée ouverte. Une session d'application est vide quand toutes les applications qui s'exécutent pendant la session sont fermées. Quand la session est ouverte, les utilisateurs peuvent ouvrir les applications plus rapidement. Vous pouvez enregistrer des ressources système si vous vous déconnectez ou fermez les sessions d'applications vides. Sélectionnez **Jamais** ou indiquez le nombre de minutes correspondant à la valeur du délai d'expiration. La valeur par défaut est **Après 1 minutes**. | |
| En cas d'expiration de délai | Détermine si une session d'application vide est déconnectée ou fermée après que la limite du **Délai d'expiration de session vide** est atteinte. Sélectionnez **Déconnecter** ou **Fermer la session**. La fermeture d'une session libère des ressources, mais l'ouverture d'une application prend plus de temps. La valeur par défaut est **Déconnecter**. | |
| Fermer les sessions déconnectées | Détermine quand une session déconnectée est fermée. Ce paramètre s'applique aux sessions de postes de travail et d'applications. Sélectionnez **Jamais**, **Immédiat** ou **Après ... minutes**. Soyez prudent lorsque vous sélectionnez **Immédiat** ou **Après ... minutes**. Quand une session déconnectée est fermée, elle est perdue. La valeur par défaut est **Jamais**. | |
| Autoriser l'installation de HTML Access sur les postes de travail et les applications de cette batterie de serveurs | Détermine si HTML Access sur les postes de travail et les applications RDS est autorisé. Cochez la case **Activé** pour autoriser HTML Access sur les postes de travail et les applications RDS. Lorsque vous modifiez ce paramètre après la création d'une batterie de serveurs, la nouvelle valeur s'applique aux postes de travail et aux applications existants comme aux nouveaux. | |

**Remarque** Contrairement à une batterie de serveurs automatisée, une batterie de serveurs manuelle n'a pas le paramètre **Nombre max. de sessions par serveur RDS**, car une batterie de serveurs manuelle peut contenir des hôtes RDS qui ne sont pas identiques. Pour les hôtes RDS dans une batterie de serveurs manuelle, vous pouvez modifier des hôtes RDS individuels et modifier le paramètre équivalent **Nombre de connexions**.

# Feuille de calcul pour la création d'une batterie de serveurs automatisée

Lorsque vous créez une batterie de serveurs automatisée, l'assistant Ajouter une batterie de serveurs vous invite à configurer certains paramètres.

Vous pouvez imprimer cette feuille de calcul et prendre note des valeurs que vous souhaitez spécifier quand vous exécutez l'assistant Ajouter une batterie de serveurs.

**Tableau 9-2.** Feuille de calcul : paramètres de configuration pour la création d'une batterie de serveurs automatisée

| Paramètre | Description | Indiquez votre valeur ici |
|---|---|---|
| ID | Nom unique qui identifie la batterie de serveurs dans View Administrator. | |
| Description | Description de cette batterie de serveurs. | |
| Groupe d'accès | Groupe d'accès dans lequel placer tous les pools de cette batterie de serveurs.<br>Pour plus d'informations sur l'accès aux groupes, consultez le chapitre sur l'administration déléguée basée sur des rôles dans le document *Administration de View*. | |
| Protocole d'affichage par défaut | Sélectionnez **VMware Blast**, **PCoIP** ou **RDP**. RDP s'applique aux pools de postes de travail uniquement. Le protocole d'affichage des pools d'applications est toujours **VMware Blast** ou **PCoIP**. Si vous sélectionnez **RDP** et que vous prévoyez d'utiliser cette batterie de serveurs pour héberger des pools d'applications, vous devez définir **Autoriser les utilisateurs à choisir un protocole** sur **Oui**. L'option par défaut est **PCoIP**. | |
| Autoriser les utilisateurs à choisir un protocole | Sélectionnez **Oui** ou **Non**. Ce paramètre ne s'applique qu'aux pools de postes de travail RDS. Si vous sélectionnez **Oui**, les utilisateurs peuvent choisir le protocole d'affichage quand ils se connectent à un poste de travail RDS depuis Horizon Client. La valeur par défaut est **Oui**. | |
| Délai d'expiration de session vide (applications seulement) | Détermine la durée pendant laquelle une session d'application vide est laissée ouverte. Une session d'application est vide quand toutes les applications qui s'exécutent pendant la session sont fermées. Quand la session est ouverte, les utilisateurs peuvent ouvrir les applications plus rapidement. Vous pouvez enregistrer des ressources système si vous vous déconnectez ou fermez les sessions d'applications vides. Sélectionnez **Jamais** ou indiquez le nombre de minutes correspondant à la valeur du délai d'expiration. La valeur par défaut est **Après 1 minutes**. | |
| En cas d'expiration de délai | Détermine si une session d'application vide est déconnectée ou fermée après que la limite du **Délai d'expiration de session vide** est atteinte. Sélectionnez **Déconnecter** ou **Fermer la session**. La fermeture d'une session libère des ressources, mais l'ouverture d'une application prend plus de temps. La valeur par défaut est **Déconnecter**. | |
| Fermer les sessions déconnectées | Détermine quand une session déconnectée est fermée. Ce paramètre s'applique aux sessions de postes de travail et d'applications. Sélectionnez **Jamais**, **Immédiat** ou **Après ... minutes**. Soyez prudent lorsque vous sélectionnez **Immédiat** ou **Après ... minutes**. Quand une session déconnectée est fermée, elle est perdue. La valeur par défaut est **Jamais**. | |

**Tableau 9-2.** Feuille de calcul : paramètres de configuration pour la création d'une batterie de serveurs automatisée (suite)

| Paramètre | Description | Indiquez votre valeur ici |
|---|---|---|
| Autoriser l'installation de HTML Access sur les postes de travail et les applications de cette batterie de serveurs | Détermine si HTML Access sur les postes de travail et les applications RDS est autorisé. Cochez la case **Activé** pour autoriser HTML Access sur les postes de travail et les applications RDS. Lorsque vous modifiez ce paramètre après la création d'une batterie de serveurs, la nouvelle valeur s'applique aux postes de travail et aux applications existants comme aux nouveaux. | |
| Nombre max. de sessions par serveur RDS | Détermine le nombre maximum de sessions qu'un hôte RDS peut prendre en charge. Sélectionnez **Illimité** ou **Pas plus que...**. La valeur par défaut est **Illimité**. | |
| Activer l'approvisionnement | Cochez cette case pour activer le provisionnement lorsque vous avez terminé cet assistant. Cette case est cochée par défaut. | |
| Arrêter l'approvisionnement en cas d'erreur | Cochez cette case pour arrêter le provisionnement lorsqu'une erreur de provisionnement se produit. Cette case est cochée par défaut. | |
| Mode d'attribution de nom | Spécifiez un préfixe ou un format de nom. View ajoutera ou insérera un numéro généré automatiquement commençant par 1 pour former le nom de la machine. Si vous voulez que le numéro soit à la fin, spécifiez simplement un préfixe. Sinon, spécifiez **{n}** n'importe où dans une chaîne de caractères et **{n}** sera remplacé par le numéro. Vous pouvez également spécifier **{n:fixed=<nombre de chiffres>}**, où **fixed=<nombre de chiffres>** indique le nombre de chiffres à utiliser pour le numéro. Par exemple, spécifiez **vm-{n:fixed=3}-sales** et les noms des machines seront vm-001-sales, vm-002-sales, etc.<br>**Remarque** Chaque nom de machine, numéro généré automatiquement inclus, a une limite de 15 caractères. | |
| Nombre max. de machines | Nombre de machines à provisionner. | |
| Nombre minimal de machines prêtes (provisionnées) pendant les opérations de maintenance de View Composer | Ce paramètre vous permet de conserver le nombre spécifié de machines disponibles pour accepter des demandes de connexion alors que View Composer recompose les machines dans la batterie de serveurs. | |
| Utiliser vSphere Virtual SAN | Spécifiez si vous souhaitez utiliser VMware Virtual SAN, le cas échéant. Virtual SAN est une couche de stockage définie par logiciel qui virtualise les disques de stockage physique locaux disponibles sur un cluster d'hôtes ESXi. Pour plus d'informations, reportez-vous à la section « Utilisation de Virtual SAN pour un stockage haute performance et une gestion basée sur les stratégies », page 273 | |
| Sélectionner des magasins de données séparés pour les disques de réplication et du système d'exploitation | (Disponible uniquement si vous n'utilisez pas Virtual SAN) Vous pouvez placer des disques de réplica et du système d'exploitation sur différentes banques de données pour les performances ou d'autres raisons. | |
| Machine virtuelle parente | Sélectionnez une machine virtuelle parente dans la liste. Sachez que la liste comporte des machines virtuelles sur lesquelles View Composer Agent n'est pas installé. Vous ne devez pas sélectionner ces machines, car View Composer Agent est requis. Il vous est recommandé d'utiliser une convention de dénomination qui indique si View Composer Agent est installé sur une machine virtuelle. | |

**Tableau 9-2.** Feuille de calcul : paramètres de configuration pour la création d'une batterie de serveurs automatisée (suite)

| Paramètre | Description | Indiquez votre valeur ici |
|---|---|---|
| Snapshot | Sélectionnez le snapshot de la machine virtuelle parente à utiliser comme image de base pour la batterie de serveurs.<br>Ne supprimez pas le snapshot et la machine virtuelle parente de vCenter Server, sauf si aucun clone lié dans la batterie de serveurs n'utilise l'image par défaut, et si aucun autre clone lié ne sera créé à partir de cette image par défaut. Le système requiert que la machine virtuelle parente et le snapshot provisionnent les nouveaux clones liés dans la batterie de serveurs, conformément aux stratégies de la batterie de serveurs. La machine virtuelle parente et le snapshot sont également requis pour les opérations de maintenance de View Composer. | |
| Emplacement du dossier de machine virtuelle | Sélectionnez le dossier dans vCenter Server dans lequel réside la batterie de serveurs. | |
| Host or cluster (Hôte ou cluster) | Sélectionnez l'hôte ou le cluster ESXi sur lequel les machines virtuelles de poste de travail s'exécutent.<br>Avec des banques de données Virtual SAN (fonctionnalité de vSphere 5.5 Update 1), vous pouvez sélectionner un cluster contenant jusqu'à 20 hôtes ESXi. Avec des banques de données Virtual Volumes (fonctionnalité de vSphere 6.0), vous pouvez sélectionner un cluster contenant jusqu'à 32 hôtes ESXi.<br>Dans vSphere 5.1 ou supérieur, vous pouvez sélectionner un cluster contenant jusqu'à 32 hôtes ESXi si les réplicas sont stockés sur des magasins de données VMFS5 ou supérieur ou sur des magasins de données NFS. Si vous stockez les réplicas sur une version VMFS antérieure à VMFS5, un cluster peut contenir 8 hôtes au maximum.<br>Dans vSphere 5.0, vous pouvez sélectionner un cluster avec plus de 8 hôtes ESXi si les réplicas sont stockés sur des magasins de données NFS. Si vous stockez les réplicas sur des magasins de données VMFS, un cluster peut contenir au maximum 8 hôtes. | |
| Resource pool (Pool de ressources) | Sélectionnez le pool de ressources de vCenter Server dans lequel la batterie de serveurs réside. | |
| Magasins de données | Sélectionnez un ou plusieurs magasins de données sur lesquels stocker la batterie de serveurs.<br>Sur la page Sélectionner des banques de données de clone lié de l'assistant Ajouter une batterie de serveurs, un tableau fournit des recommandations pour estimer les besoins en stockage de la batterie de serveurs. Ces recommandations peuvent vous aider à déterminer les magasins de données assez volumineux pour stocker les disques de clone lié. Pour plus d'informations, reportez-vous à « Dimensionnement du stockage pour des pools de postes de travail de clone instantané et de clone lié View Composer », page 280.<br>Vous pouvez utiliser des magasins de données partagés ou locaux pour un hôte ESXi individuel ou pour des clusters ESXi. Si vous utilisez des magasins de données locaux dans un cluster ESXi, vous devez prendre en compte les contraintes de l'infrastructure vSphere qui sont imposées sur votre déploiement de poste de travail. Reportez-vous à la section « Stockage de clones liés View Composer sur des magasins de données locaux », page 288.<br>**Remarque** Si vous utilisez Virtual SAN, sélectionnez une seule banque de données. | |

**Tableau 9-2.** Feuille de calcul : paramètres de configuration pour la création d'une batterie de serveurs automatisée (suite)

| Paramètre | Description | Indiquez votre valeur ici |
|---|---|---|
| Surcharge du stockage | Déterminez le niveau de surcharge du stockage auquel les clones liés sont créés sur chaque banque de données.<br>À mesure que le niveau augmente, plus de clones liés sont placés sur le magasin de données et moins d'espace est réservé pour la croissance des clones individuels. Un niveau de surcharge du stockage élevé vous permet de créer des clones liés ayant une taille logique totale supérieure à la limite de stockage physique du magasin de données. Pour plus d'informations, reportez-vous à « Surcharge de stockage des machines virtuelles de clone lié View Composer », page 285.<br>**Remarque** Ce paramètre n'a aucun effet si vous utilisez Virtual SAN. | |
| Utiliser des snapshots NFS natifs (VAAI) | (Disponible uniquement si vous n'utilisez pas Virtual SAN) Si votre déploiement inclut des périphériques NAS prenant en charge la technologie VAAI (vStorage APIs for Array Integration), vous pouvez utiliser la technologie de snapshot native pour cloner des machines virtuelles.<br>Vous pouvez utiliser cette fonction uniquement si vous sélectionnez des magasins de données résidant sur des périphériques NAS prenant en charge les opérations de clonage natif via VAAI.<br>Vous ne pouvez pas utiliser cette fonction si vous stockez des réplicas et des disques du système d'exploitation sur des magasins de données séparés. Vous ne pouvez pas utiliser cette fonctionnalité sur les machines virtuelles intégrant des disques à optimisation d'espace.<br>Cette fonction est prise en charge sur vSphere 5.0 et supérieur.<br>Pour plus d'informations, reportez-vous à « Utilisation du stockage VAAI des clones liés View Composer », page 294. | |
| Récupérer l'espace disque de machine virtuelle | (Disponible uniquement si vous n'utilisez pas Virtual SAN ou Virtual Volumes) Déterminez si vous souhaitez autoriser des hôtes ESXi à récupérer l'espace disque non utilisé sur les clones liés qui sont créés au format de disque à optimisation d'espace. La fonction de récupération d'espace réduit l'espace de stockage total requis pour les postes de travail de clone lié.<br>Cette fonction est prise en charge sur vSphere 5.1 et supérieur. Les machines virtuelles de clone lié doivent avoir la version matérielle virtuelle 9 ou supérieure.<br>Pour plus d'informations, reportez-vous à « Récupérer l'espace disque sur des clones liés View Composer », page 292. | |
| Initier la récupération lorsque l'espace inutilisé de la machine virtuelle dépasse : | (Disponible uniquement si vous n'utilisez pas Virtual SAN ou Virtual Volumes) Tapez le volume minimal d'espace disque inutilisé, en giga-octets, qui doit s'accumuler sur un disque du système d'exploitation de clone lié pour déclencher la récupération d'espace. Lorsque l'espace disque inutilisé dépasse ce seuil, View initie l'opération qui demande à l'hôte ESXi de récupérer l'espace sur le disque du système d'exploitation.<br>Cette valeur est mesurée par machine virtuelle. L'espace disque inutilisé doit dépasser le seuil spécifié sur une machine virtuelle individuelle pour que View démarre le processus de récupération d'espace sur cette machine.<br>Par exemple : **2** Go.<br>La valeur par défaut est 1 Go. | |

**Tableau 9-2.** Feuille de calcul : paramètres de configuration pour la création d'une batterie de serveurs automatisée (suite)

| Paramètre | Description | Indiquez votre valeur ici |
|---|---|---|
| Durée d'interruption | Configurez les jours et les heures auxquels la récupération de l'espace disque de machine virtuelle n'a pas lieu.<br>Pour vous assurer que des ressources ESXi sont dédiées à des tâches de premier plan lorsque cela est nécessaire, vous pouvez empêcher les hôtes ESXi d'exécuter ces opérations pendant des périodes de temps spécifiées certains jours.<br>Pour plus d'informations, reportez-vous à « Définir les durées d'interruption de Storage Accelerator et de récupération d'espace des clones liés View Composer », page 295. | |
| Portée du partage de page transparente (Transparent Page Sharing) | Sélectionnez le niveau auquel autoriser le partage de page transparente (TPS). Les choix sont **Machine virtuelle** (par défaut), **Batterie de serveurs**, **Espace** ou **Global**. Si vous activez le partage de page transparente pour les machines de la batterie de serveurs, de l'espace ou globalement, l'hôte ESXi élimine les copies redondantes des pages mémoire obtenues si les machines utilisent le même système d'exploitation invité ou les mêmes applications.<br>Le partage de page se produit sur l'hôte ESXi. Par exemple, si vous activez le partage de page transparente au niveau de la batterie de serveurs alors que la batterie de serveurs couvre plusieurs hôtes ESXi, seules les machines virtuelles sur le même hôte et à l'intérieur de la même batterie de serveurs partageront des pages. Au niveau global, toutes les machines gérées par View sur le même hôte ESXi peuvent partager des pages de mémoire, quelle que soit la batterie de serveurs sur laquelle résident les machines.<br>**Remarque** Par défaut, les pages de mémoire ne sont pas partagées entre plusieurs machines, car le partage de page transparente (TPS) peut créer un risque. Les recherches indiquent que le partage de page transparente peut être exploité de façon abusive pour obtenir un accès non autorisé à des données dans des scénarios de configuration très limités. | |
| Domaine | Sélectionnez le domaine Active Directory et le nom d'utilisateur.<br>View Composer requiert certains privilèges utilisateur pour la batterie de serveurs. Domaine et compte d'utilisateur utilisés par Sysprep pour personnaliser les machines de clone lié.<br>Vous spécifiez cet utilisateur lorsque vous configurez des paramètres de View Composer pour vCenter Server. Vous pouvez spécifier plusieurs domaines et utilisateurs lorsque vous configurez les paramètres de View Composer. Lorsque vous utilisez l'assistant Ajouter une batterie de serveurs pour créer une batterie de serveurs, vous devez sélectionner un domaine et un utilisateur dans la liste.<br>Pour plus d'informations sur la configuration de View Composer, reportez-vous au document *Administration de View*. | |
| Conteneur Active Directory | Fournissez le nom unique relatif du conteneur Active Directory.<br>Par exemple : `CN=Ordinateurs`<br>Lorsque vous exécutez l'assistant Ajouter une batterie de serveurs, vous pouvez parcourir votre arborescence Active Directory pour rechercher le conteneur. | |

**Tableau 9-2.** Feuille de calcul : paramètres de configuration pour la création d'une batterie de serveurs automatisée (suite)

| Paramètre | Description | Indiquez votre valeur ici |
|---|---|---|
| Autoriser la réutilisation de comptes d'ordinateur pré-existants | Sélectionnez ce paramètre pour utiliser des comptes d'ordinateur existants dans Active Directory pour des clones liés qui sont provisionnés par View Composer. Ce paramètre vous permet de contrôler les comptes d'ordinateur qui sont créés dans Active Directory.<br>Lorsqu'un clone lié est provisionné, si le nom d'un compte d'ordinateur Active Directory existant correspond au nom de la machine de clone lié, View Composer utilise le compte d'ordinateur existant. Sinon, un nouveau compte d'ordinateur est créé.<br>Les comptes d'ordinateur existants doivent être situés dans le conteneur Active Directory que vous spécifiez avec le paramètre **Conteneur Active Directory**.<br>Lorsque ce paramètre est désactivé, un nouveau compte d'ordinateur AD est créé lorsque View Composer provisionne un clone lié. Ce paramètre est désactivé par défaut.<br>Pour plus d'informations, reportez-vous à « Utiliser des comptes d'ordinateur Active Directory existants pour des clones liés », page 92. | |
| Utiliser une spécification de personnalisation (Sysprep) | Fournissez une spécification de personnalisation Sysprep pour personnaliser les machines virtuelles. | |

# Créer une batterie de serveurs manuelle

Vous créez une batterie de serveurs manuelle dans le cadre du processus visant à accorder aux utilisateurs l'accès aux applications ou aux postes de travail RDS.

### Prérequis

- Configurez les hôtes RDS faisant partie de la batterie de serveurs. Reportez-vous à la section Chapitre 8, « Configuration des hôtes de services Bureau à distance », page 115.
- Vérifiez que l'état de tous les hôtes RDS est Disponible. Dans View Administrator, sélectionnez **Configuration de View > Machines inscrites** et vérifiez l'état de chaque hôte RDS dans l'onglet Hôtes RDS.
- Rassemblez les informations de configuration à fournir pour créer la batterie de serveurs. Reportez-vous à la section « Feuille de calcul pour la création d'une batterie de serveurs manuelle », page 133.

### Procédure

1. Dans View Administrator, cliquez sur **Ressources > Batteries de serveurs**.
2. Cliquez sur **Ajouter** pour entrer les informations de configuration que vous avez rassemblées dans la feuille de calcul.
3. Sélectionnez **Batterie de serveurs manuelle**.
4. Suivez les invites de l'assistant pour créer la batterie de serveurs.

   Utilisez les informations de configuration que vous avez collectées dans la feuille de calcul. Vous pouvez revenir directement à n'importe quelle page de l'assistant en cliquant sur le nom de page dans le volet de navigation.
5. Sélectionnez les hôtes RDS à ajouter à la batterie de serveurs, puis cliquez sur **Suivant**.
6. Cliquez sur **Terminer**.

Dans View Administrator, vous pouvez désormais afficher la batterie de serveurs en cliquant sur **Ressources > Batteries de serveurs**.

### Suivant

Créez un pool d'applications ou un pool de postes de travail RDS. Reportez-vous à la section Chapitre 10, « Création de pools d'applications », page 143 ou Chapitre 11, « Création de pools de postes de travail RDS », page 147.

## Créer une batterie de serveurs automatisée

Vous créez une batterie de serveurs automatisée dans le cadre du processus visant à accorder aux utilisateurs l'accès aux applications ou aux postes de travail RDS.

### Prérequis

- Vérifiez que le service View Composer est installé. Reportez-vous au document *Installation de View*.
- Vérifiez que les paramètres de View Composer pour vCenter Server sont configurés dans View Administrator. Reportez-vous au document *Administration de View*.
- Vérifiez que vous disposez d'un nombre suffisant de ports sur le commutateur virtuel ESXi utilisé pour les machines virtuelles servant de postes de travail distants. La valeur par défaut peut ne pas être suffisante si vous créez des pools de postes de travail volumineux. Le nombre de ports de commutateur virtuel sur l'hôte ESXi doit être égal ou supérieur au nombre de machines virtuelles multiplié par le nombre de cartes réseau virtuelles par machine virtuelle.
- Vérifiez que vous avez préparé une machine virtuelle parente. Horizon Agent et View Composer Agent doivent être installés sur la machine virtuelle parente. Reportez-vous à la section « Préparation d'une machine virtuelle parente pour une batterie de serveurs automatisée », page 130.
- Prenez un snapshot de la machine virtuelle parente dans vCenter Server. Vous devez éteindre la machine virtuelle parente avant de prendre le snapshot. View Composer utilise le snapshot comme image de base depuis laquelle les clones sont créés.

  **Remarque** Vous ne pouvez pas créer de pool de clone lié depuis un modèle de machine virtuelle.

- Rassemblez les informations de configuration à fournir pour créer la batterie de serveurs. Reportez-vous à la section « Feuille de calcul pour la création d'une batterie de serveurs automatisée », page 135.

### Procédure

1. Dans View Administrator, cliquez sur **Ressources > Batteries de serveurs**.
2. Cliquez sur **Ajouter** pour entrer les informations de configuration que vous avez rassemblées dans la feuille de calcul.
3. Sélectionnez **Batterie de serveurs automatisée**.
4. Suivez les invites de l'assistant pour créer la batterie de serveurs.

   Utilisez les informations de configuration que vous avez collectées dans la feuille de calcul. Vous pouvez revenir directement à n'importe quelle page de l'assistant en cliquant sur le nom de page dans le volet de navigation.

Dans View Administrator, vous pouvez désormais afficher la batterie de serveurs en cliquant sur **Ressources > Batteries de serveurs**.

### Suivant

Créez un pool d'applications ou un pool de postes de travail RDS. Reportez-vous à la section Chapitre 10, « Création de pools d'applications », page 143 ou Chapitre 11, « Création de pools de postes de travail RDS », page 147.

# Création de pools d'applications 10

L'une des tâches que vous effectuez pour accorder aux utilisateurs l'accès distant à une application consiste à créer un pool d'applications. Les utilisateurs autorisés à un pool d'applications peuvent accéder à l'application à distance depuis différents types de périphériques clients.

Ce chapitre aborde les rubriques suivantes :



## Pools d'applications

Avec les pools d'applications, vous pouvez livrer une seule application à un grand nombre d'utilisateurs. L'application s'exécute sur une batterie de serveurs d'hôtes RDS.

Lorsque vous créez un pool d'applications, vous déployez une application dans le centre de données auquel les utilisateurs ont accès n'importe où sur le réseau. Pour une introduction aux pools d'applications, reportez-vous à « Batteries de serveurs, hôtes RDS et pools de postes de travail et d'applications », page 11.

Un pool d'applications comporte une seule application et est associé à une seule batterie de serveurs. Pour éviter les erreurs, vous devez installer l'application sur l'ensemble des hôtes RDS de la batterie de serveurs.

Lorsque vous créez un pool d'applications, View affiche automatiquement les applications qui sont accessibles à tous les utilisateurs plutôt qu'à des utilisateurs individuels dans le menu **Démarrer** sur tous les hôtes RDS de la batterie de serveurs. Vous pouvez sélectionner une ou plusieurs applications dans la liste. Si vous sélectionnez plusieurs applications dans la liste, un pool d'applications distinct est créé pour chaque application. Vous pouvez également spécifier manuellement une application ne figurant pas dans la liste. Si une application que vous souhaitez spécifier manuellement n'est pas déjà installée, View affiche un message d'avertissement.

Lorsque vous créez un pool d'applications, vous ne pouvez pas spécifier le groupe d'accès dans lequel placer le pool. Pour les pools d'applications et les pools de postes de travail RDS, vous spécifiez le groupe d'accès lors de la création d'une batterie de serveurs.

Une application prend en charge les protocoles d'affichage PCoIP et VMware Blast. Pour activer HTML Access, reportez-vous à la section « Préparer des postes de travail, des pools et des batteries de serveurs pour HTML Access » dans le chapitre « Configuration et installation » du document *Utilisation de HTML Access*, disponible à l'adresse https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

## Feuille de calcul pour la création manuelle d'un pool d'applications

Lorsque vous créez un pool d'applications et spécifiez manuellement une application, l'assistant Ajouter des pools d'applications vous invite à entrer des informations sur l'application. Il n'est pas nécessaire que l'application soit déjà installée sur un hôte RDS.

Vous pouvez imprimer cette feuille de calcul et noter les propriétés de l'application lorsque vous spécifiez l'application manuellement.

**Tableau 10-1.** Feuille de calcul : Propriétés d'application pour la création manuelle d'un pool d'applications

| Propriété | Description | Indiquez votre valeur ici |
|---|---|---|
| ID | Nom unique qui identifie le pool dans View Administrator. Ce champ est obligatoire. | |
| Nom d'affichage | Nom du pool qui s'affiche pour les utilisateurs lorsqu'ils ouvrent une session sur Horizon Client. Si vous ne spécifiez pas de nom d'affichage, celui-ci sera identique à l'**ID**. | |
| Version | Version de l'application. | |
| Éditeur | Éditeur de l'application. | |
| Chemin d'accès | Chemin complet de l'application. Par exemple, `C:\Program Files\app1.exe`. Ce champ est obligatoire. | |
| Dossier de démarrage | Chemin d'accès complet du répertoire de démarrage de l'application. | |
| Paramètres | Paramètres à transmettre à l'application lors de son démarrage. Par exemple, vous pouvez spécifier `-username user1 -loglevel 3`. | |
| Description | Description de ce pool d'applications. | |

## Créer un pool d'applications

Vous créez un pool d'applications dans le cadre du processus d'attribution aux utilisateurs d'un accès à une application qui s'exécute sur des hôtes RDS.

### Prérequis

- Configurez les hôtes RDS. Reportez-vous à la section Chapitre 8, « Configuration des hôtes de services Bureau à distance », page 115.
- Créez une batterie de serveurs qui contient les hôtes RDS. Reportez-vous à la section Chapitre 9, « Création de batteries de serveurs », page 129.
- Si vous prévoyez d'ajouter un pool d'applications manuellement, recueillez des informations sur l'application. Reportez-vous à la section « Feuille de calcul pour la création manuelle d'un pool d'applications », page 144.

### Procédure

1 Dans View Administrator, cliquez sur **Catalogue > Pools d'applications**.

2 Cliquez sur **Ajouter**.

3 Suivez les invites de l'assistant pour créer le pool.

   Si vous choisissez d'ajouter un pool d'applications manuellement, utilisez les informations de configuration que vous avez rassemblées sur la feuille de calcul. Si vous sélectionnez des applications dans la liste affichée par View Administrator, vous pouvez sélectionner plusieurs applications. Un pool distinct est créé pour chaque application.

Dans View Administrator, vous pouvez désormais afficher le pool d'applications en cliquant sur **Catalogue > Pools d'applications**.

### Suivant

Autorisez les utilisateurs à accéder au pool. Reportez-vous à la section Chapitre 13, « Autorisation d'utilisateurs et de groupes », page 187.

Vérifiez que vos utilisateurs finaux ont accès au logiciel Horizon Client 3.0 ou version ultérieure qui est nécessaire pour la prise en charge des applications RDS.

Si vous devez vous assurer que le Serveur de connexion View lance l'application uniquement sur des hôtes RDS disposant de ressources suffisantes pour exécuter l'application, configurez une règle anti-affinité pour le pool d'applications. Pour plus d'informations, consultez « Configurer une règle anti-affinité pour un pool d'applications » dans le document *Administration de View*.

# Création de pools de postes de travail RDS 11

L'une des tâches que vous devez effectuer pour accorder aux utilisateurs un accès distant aux postes de travail basés sur une session consiste à créer un pool de postes de travail des services Bureau à distance (RDS). Un pool de postes de travail RDS dispose de propriétés susceptibles de répondre à certains besoins spécifiques d'un déploiement de postes de travail distants.

Ce chapitre aborde les rubriques suivantes :



## Présentation des pools de postes de travail RDS

Le pool de postes de travail RDS est l'un des trois types de pools de postes de travail que vous pouvez créer. Ce type de pool était appelé pool des Services Terminal Server Microsoft dans les versions précédentes de View.

Un pool de postes de travail RDS et un poste de travail RDS ont les caractéristiques suivantes :

- Un pool de postes de travail RDS est associé à une batterie de serveurs qui est un groupe d'hôtes RDS. Chaque hôte RDS est un serveur Windows pouvant héberger plusieurs postes de travail RDS.
- Un poste de travail RDS est basé sur une session sur un hôte RDS. En revanche, un poste de travail d'un pool de postes de travail automatisé est basé sur une machine virtuelle, et un poste de travail d'un pool de postes de travail manuel est basé sur une machine virtuelle ou physique.
- Un poste de travail RDS prend en charge les protocoles d'affichage RDP, PCoIP et VMware Blast. Pour activer HTML Access, reportez-vous à la section « Préparer des postes de travail, des pools et des batteries de serveurs pour HTML Access » dans le chapitre « Configuration et installation » du document *Utilisation de HTML Access*, disponible à l'adresse https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.
- Un pool de postes de travail RDS est uniquement pris en charge par des systèmes d'exploitation Windows Server prenant en charge le rôle RDS et pris en charge par View. Reportez-vous à la section « Configuration requise pour les systèmes d'exploitation invités » dans le document *Installation de View*.
- View fournit aux batteries de serveurs l'équilibrage de charge des hôtes RDS en dirigeant les demandes de connexion vers l'hôte RDS qui contient le plus petit nombre de sessions actives.

- Du fait qu'un pool de postes de travail RDS fournit des postes de travail basés sur une session, il ne prend pas en charge les opérations propres à un pool de postes de travail de clone lié, telles que l'actualisation, la recomposition et le rééquilibrage.
- Si un hôte RDS est une machine virtuelle gérée par vCenter Server, vous pouvez utiliser des snapshots comme images de base. Vous pouvez utiliser vCenter Server pour gérer les snapshots. L'utilisation de snapshots sur des machines virtuelles RDS est transparente pour View.
- Les postes de travail RDS ne prennent pas en charge View Persona Management.
- La fonction copier-coller est désactivée par défaut pour HTML Access. Pour activer la fonction, reportez-vous à « Paramètres de stratégie de groupe de HTML Access » dans le chapitre « Configuration de HTML Access pour les utilisateurs finaux » dans le document *Utilisation de HTML Access*, disponible sur le site https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

## Créer un pool de postes de travail RDS

Vous pouvez créer un pool de postes de travail RDS dans le cadre du processus donnant aux utilisateurs accès aux postes de travail RDS.

### Prérequis

- Configurez les hôtes RDS. Reportez-vous à la section Chapitre 8, « Configuration des hôtes de services Bureau à distance », page 115.
- Créez une batterie de serveurs qui contient les hôtes RDS. Reportez-vous à la section Chapitre 9, « Création de batteries de serveurs », page 129.
- Décidez comment configurer les paramètres du pool. Reportez-vous à la section « Paramètres des pools de postes de travail RDS », page 149.

### Procédure

1. Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.
2. Cliquez sur **Ajouter**.
3. Sélectionnez **Pool de postes de travail RDS**.
4. Fournissez un ID de pool, un nom d'affichage et une description.

   L'ID du pool est le nom unique qui identifie le pool dans View Administrator. Le nom d'affichage est le nom du pool de postes de travail RDS que les utilisateurs voient lorsqu'ils se connectent à Horizon Client. Si vous ne spécifiez pas de nom d'affichage, celui-ci sera identique à l'ID du pool.
5. Sélectionnez les paramètres du pool.
6. Sélectionnez ou créez une batterie de serveurs pour ce pool.

Dans View Administrator, vous pouvez maintenant afficher le pool de postes de travail RDS en sélectionnant **Catalogue > Pools de postes de travail**.

### Suivant

Autorisez les utilisateurs à accéder au pool. Reportez-vous à la section « Ajouter des droits d'accès à un pool de postes de travail ou d'applications », page 187.

Assurez-vous que vos utilisateurs finaux ont accès à Horizon Client 3.0 ou logiciel ultérieur, qui est requis pour prendre en charge les pools de postes de travail RDS.

## Paramètres des pools de postes de travail RDS

Vous pouvez spécifier certains paramètres de pool lorsque vous créez un pool de postes de travail RDS. Tous les paramètres de pool ne s'appliquent pas à tous les types de pools de postes de travail.

Pour obtenir une description de tous les paramètres de pool, consultez « Paramètres de pools de postes de travail pour tous les types de pools de postes de travail », page 160. Les paramètres de pool suivants s'appliquent à un pool de postes de travail RDS.

**Tableau 11-1.** Paramètres d'un pool de postes de travail RDS

| Paramètre | Valeur par défaut |
|---|---|
| État | Activé |
| Restrictions du serveur de connexion | Aucune |
| Adobe Flash quality (Qualité Adobe Flash) | Ne pas contrôler |
| Adobe Flash throttling (Limitation d'Adobe Flash) | Désactivé |

## Configurer la limitation d'Adobe Flash avec Internet Explorer pour des pools de postes de travail RDS

Pour s'assurer que la limitation d'Adobe Flash fonctionne avec Internet Explorer sur des postes de travail RDS, les utilisateurs doivent activer des extensions de navigateur tiers.

### Procédure

1 Démarrez Horizon Client et connectez-vous sur le poste de travail d'un utilisateur.

2 Dans Internet Explorer, cliquez sur **Outils > Options Internet**.

3 Cliquez sur l'onglet **Avancé**, sélectionnez **Activer les extensions tierce partie du navigateur**, puis cliquez sur **OK**.

4 Redémarrez Internet Explorer.

# Approvisionnement de pools de postes de travail 12

Lorsque vous créez un pool de postes de travail, vous sélectionnez des options de configuration qui déterminent la façon dont le pool est géré et comment les utilisateurs interagissent avec les postes de travail.

Ces tâches de provisionnement s'appliquent aux pools de postes de travail qui sont déployés sur des machines mono-utilisateur. Elles ne s'appliquent pas à des pools de postes de travail RDS. Cependant, les paramètres de qualité et de limitation d'Adobe Flash s'appliquent à tous les types de pools de postes de travail, y compris RDS.

Ce chapitre aborde les rubriques suivantes :



## Affectation d'utilisateur dans des pools de postes de travail

Pour les pools de postes de travail manuels et les pools de postes de travail automatisés de machines virtuelles complètes ou de clones liés View Composer, vous pouvez choisir l'affectation d'utilisateur flottante ou dédiée pour les postes de travail. Pour les pools de postes de travail de clone instantané, vous ne pouvez choisir que l'affectation d'utilisateur flottante.

Avec une affectation dédiée, chaque poste de travail est affecté à un utilisateur spécifique. Un utilisateur se connectant pour la première fois obtient un poste de travail qui n'est pas affecté à un autre utilisateur. Par la suite, cet utilisateur obtiendra toujours ce poste de travail après la connexion, et ce poste de travail ne sera disponible pour aucun autre utilisateur.

Avec une affectation flottante, les utilisateurs obtiennent un poste de travail aléatoire chaque fois qu'ils se connectent. Lorsqu'un utilisateur se déconnecte, le poste de travail est renvoyé au pool.

Avec des clones instantanés, le poste de travail est toujours supprimé et recréé à partir de l'image actuelle lorsqu'un utilisateur se déconnecte. Avec des clones liés View Composer, vous pouvez configurer des machines d'affectation flottante pour qu'elles soient supprimées lorsque les utilisateurs se déconnectent. La suppression automatique vous permet de ne conserver que les machines virtuelles dont vous avez besoin en même temps.

Avec l'affectation flottante, vous pouvez réduire les coûts de licence logicielle.

## Dénomination manuelle de machines ou fourniture d'un mode d'attribution de nom

Avec un pool de postes de travail automatisé de machines virtuelles complètes ou de clones liés View Composer, vous pouvez spécifier une liste de noms pour les machines de poste de travail ou fournir un mode d'attribution de nom. Avec un pool de postes de travail de clone instantané, vous pouvez uniquement spécifier un mode d'attribution de nom lors du provisionnement du pool.

Si vous nommez des machines en spécifiant une liste, vous pouvez utiliser le modèle de dénomination de votre entreprise, et vous pouvez associer chaque nom de machine à un utilisateur.

Si vous fournissez un mode d'attribution de nom, View peut créer et attribuer dynamiquement des machines à mesure que les utilisateurs en ont besoin.

Tableau 12-1 compare les deux méthodes de nommage, en montrant comment chaque méthode affecte la façon dont vous créez et administrez un pool de postes de travail.

**Tableau 12-1.** Dénomination manuelle de machines ou prestation d'un mode d'attribution de nom

| Fonction | Utilisation d'un mode d'attribution de nom | Dénomination manuelle de machines |
|---|---|---|
| Noms de machines | Les noms de machine sont générés en ajoutant un numéro au mode d'attribution de nom.<br>Pour plus d'informations, reportez-vous à « Utilisation d'un mode d'attribution de nom pour des pools de postes de travail automatisés », page 155. | Vous spécifiez une liste de noms de machines.<br>Dans un pool à attribution dédiée, vous pouvez coupler des utilisateurs avec des machines en répertoriant des noms d'utilisateurs avec les noms de machines.<br>Pour plus d'informations, reportez-vous à « Spécifier une liste de noms de machines », page 154. |
| Taille de pool | Vous spécifiez un nombre maximal de machines. | Votre liste de noms de machines détermine le nombre de machines. |
| Pour ajouter des machines au pool | Vous pouvez augmenter la taille de pool maximale. | Vous pouvez ajouter des noms de machines à la liste.<br>Pour plus d'informations, reportez-vous à « Ajouter des machines à un pool automatisé provisionné par une liste de noms », page 158. |
| Approvisionnement à la demande | Disponible.<br>View crée et provisionne dynamiquement le nombre minimal de machines et le nombre de machines de rechange spécifiés à mesure que les utilisateurs se connectent pour la première fois ou que vous attribuez les machines aux utilisateurs.<br>View peut également créer et provisionner toutes les machines lorsque vous créez le pool. | Non disponible.<br>View crée et provisionne toutes les machines que vous spécifiez dans votre liste lorsque le pool est créé. |

**Tableau 12-1.** Dénomination manuelle de machines ou prestation d'un mode d'attribution de nom (suite)

| Fonction | Utilisation d'un mode d'attribution de nom | Dénomination manuelle de machines |
|---|---|---|
| Personnalisation initiale | Disponible.<br>Lorsqu'une machine est provisionnée, View peut exécuter une spécification de personnalisation que vous sélectionnez. | Disponible.<br>Lorsqu'une machine est provisionnée, View peut exécuter une spécification de personnalisation que vous sélectionnez. |
| Personnalisation manuelle de machines dédiées | Non disponible pour les clones instantanés.<br>Pour personnaliser des machines et renvoyer l'accès au poste de travail à vos utilisateurs, vous devez supprimer et réattribuer la propriété de chaque machine. En fonction de l'attribution ou non de machines lors de la première ouverture de session, vous devrez peut-être effectuer ces étapes deux fois. Vous ne pouvez pas démarrer des machines en mode de maintenance. Après la création du pool, vous pouvez mettre manuellement les machines en mode de maintenance. | Vous pouvez personnaliser et tester des machines sans avoir à réattribuer la propriété.<br>Lorsque vous créez le pool, vous pouvez démarrer toutes les machines en mode de maintenance pour empêcher les utilisateurs d'y accéder. Vous pouvez personnaliser les machines et quitter le mode de maintenance pour renvoyer l'accès à vos utilisateurs.<br>Pour plus d'informations, reportez-vous à « Personnalisation manuelle des machines », page 159. |
| Taille de pool dynamique ou fixe | Dynamique.<br>Si vous supprimez une attribution d'utilisateur d'une machine dans un pool à attribution dédiée, la machine est renvoyée au pool de machines disponibles.<br>Si vous choisissez de supprimer des machines à la fermeture de session dans un pool à attribution flottante, la taille du pool peut croître ou diminuer en fonction du nombre de sessions utilisateurs actives.<br>**Remarque** Les pools de clone instantané ne peuvent être que des pools d'affectation flottante. Les machines sont toujours supprimées lors de la fermeture de session. | Fixe.<br>Le pool contient le nombre de machines que vous indiquez dans la liste de noms de machines.<br>Vous ne pouvez pas sélectionner le paramètre **Supprimer la machine à la fermeture de session** si vous nommez les machines manuellement. |

**Tableau 12-1.** Dénomination manuelle de machines ou prestation d'un mode d'attribution de nom (suite)

| Fonction | Utilisation d'un mode d'attribution de nom | Dénomination manuelle de machines |
|---|---|---|
| Machines de rechange | Vous pouvez spécifier un nombre de machines de rechange que View maintient sous tension pour les nouveaux utilisateurs.<br>View crée de nouvelles machines pour conserver le nombre spécifié. View cesse de créer des machines de rechange lorsqu'il atteint la taille de pool maximale.<br>View maintient les machines de rechange sous tension, même quand la stratégie d'alimentation du pool est **Mettre hors tension** ou **Interrompre**, ou quand vous ne définissez aucune stratégie d'alimentation.<br>**Remarque** Les pools de clone instantané n'ont pas de stratégie d'alimentation. | Vous pouvez spécifier un nombre de machines de rechange que View maintient sous tension pour les nouveaux utilisateurs.<br>View ne crée pas de nouvelles machines de rechange pour conserver le nombre spécifié.<br>View maintient les machines de rechange sous tension, même quand la stratégie d'alimentation du pool est **Mettre hors tension** ou **Interrompre**, ou quand vous ne définissez aucune stratégie d'alimentation. |
| Affectation d'utilisateur | Vous pouvez utiliser un mode d'attribution de nom pour des pools d'affectation dédiée et flottante.<br>**Remarque** Les pools de clone instantané ne peuvent être que des pools d'affectation flottante. | Vous pouvez spécifier des noms de machines pour des pools à attribution dédiée et flottante.<br>**Remarque** Dans un pool à attribution flottante, vous ne pouvez pas associer des noms d'utilisateurs à des noms de machines. Les machines ne sont pas dédiées aux utilisateurs associés. Dans un pool à attribution flottante, toutes les machines qui ne sont pas utilisées actuellement restent accessibles à tout utilisateur ouvrant une session. |

## Spécifier une liste de noms de machines

Vous pouvez provisionner un pool de postes de travail automatisé en spécifiant manuellement une liste de noms de machines. Cette méthode vous permet d'utiliser les conventions de dénomination de votre entreprise pour identifier les machines dans un pool.

Lorsque vous spécifiez explicitement des noms de machines, les utilisateurs peuvent voir des noms familiers basés sur l'organisation de leur entreprise quand ils ouvrent une session sur leurs postes de travail distants.

Suivez ces directives pour spécifier manuellement des noms de machines :

- Tapez chaque nom de machine sur une ligne distincte.
- Un nom de machine peut comporter jusqu'à 15 caractères alphanumériques.
- Vous pouvez ajouter un nom d'utilisateur à chaque entrée de machine. Utilisez une virgule pour séparer le nom d'utilisateur de celui de la machine.

Dans cet exemple, deux machines sont spécifiées. La deuxième machine est associée à un utilisateur :

```
Desktop-001
Desktop-002,abccorp.com\jdoe
```

**Remarque** Dans un pool à attribution flottante, vous ne pouvez pas associer des noms d'utilisateurs à des noms de machines. Les machines ne sont pas dédiées aux utilisateurs associés. Dans un pool à attribution flottante, toutes les machines qui ne sont pas utilisées actuellement restent accessibles à tout utilisateur ouvrant une session.

### Prérequis

Assurez-vous que chaque nom de machine est unique. Vous ne pouvez pas utiliser les noms de machines virtuelles existantes dans vCenter Server.

### Procédure

1 Créez un fichier texte contenant la liste des noms de machines.

   Si vous prévoyez de créer un pool de postes de travail comportant seulement quelques machines, vous pouvez saisir les noms de machines directement dans l'assistant Ajouter un pool de postes de travail. Vous n'avez pas à créer un fichier texte séparé.

2 Dans View Administrator, démarrez l'assistant Ajouter un pool de postes de travail pour commencer la création d'un pool de postes de travail automatisé.

3 Sur la page Paramètres d'approvisionnement, sélectionnez **Spécifier des noms manuellement** et cliquez sur **Entrer des noms**.

4 Copiez votre liste de noms de machines dans la page Entrer des noms de machine et cliquez sur **Suivant**.

   L'assistant Entrer des noms de machines affiche la liste des postes de travail et indique les erreurs de validation avec un **!** rouge.

5 Corrigez les noms de machines non valides.

   a Placez votre curseur sur un nom non valide pour afficher le message d'erreur lié en bas de la page.

   b Cliquez sur **Précédent**.

   c Modifiez les noms incorrects et cliquez sur **Suivant**.

6 Cliquez sur **Terminer**.

7 (Facultatif) Sélectionnez **Démarrer des machines en mode de maintenance**.

   Cette option vous permet de personnaliser les machines avant que les utilisateurs puissent ouvrir une session et les utiliser.

8 Suivez les invites de l'assistant pour terminer la création du pool de postes de travail.

View crée une machine pour chaque nom dans la liste. Quand une entrée inclut un nom de machine et un nom d'utilisateur, View attribue la machine à cet utilisateur.

Après la création du pool de postes de travail, vous pouvez ajouter des machines en important un autre fichier de liste qui contient des noms de machine et des utilisateurs supplémentaires. Consultez « Ajouter des machines à un pool automatisé provisionné par une liste de noms » dans le document *Administration de View*.

## Utilisation d'un mode d'attribution de nom pour des pools de postes de travail automatisés

Vous pouvez provisionner les machines dans un pool en fournissant un mode d'attribution de nom et le nombre total de machines souhaité dans le pool. Par défaut, View utilise votre modèle comme préfixe dans tous les noms de machines et ajoute un numéro unique pour identifier chaque machine.

### Longueur du mode d'attribution de nom dans un nom de machine

Les noms de machines sont limités à 15 caractères, incluant votre mode d'attribution de nom et le numéro généré automatiquement.

**Tableau 12-2.** Longueur maximale du mode d'attribution de nom dans un nom de machine

| Si vous définissez ce nombre de machines dans le pool | Longueur de préfixe maximale |
|---|---|
| 1-99 | 13 caractères |
| 100-999 | 12 caractères |
| 1,000 ou plus | 11 caractères |

Les noms contenant des jetons de longueur fixe ont des limites de longueur différentes. Reportez-vous à la section « Longueur du mode d'attribution de nom quand vous utilisez un jeton de longueur fixe », page 156.

### Utilisation d'un jeton dans un nom de machine

Vous pouvez placer le numéro généré automatiquement n'importe où dans le nom en utilisant un jeton. Lorsque vous saisissez le nom de pool, saisissez **n** entre accolades pour désigner le jeton.

Par exemple : **amber-{n}-desktop**

Lorsqu'une machine est créée, View remplace **{n}** par un numéro unique.

Vous pouvez générer un jeton de longueur fixe en saisissant **{n:fixed=*number of digits*}**.

View remplace le jeton par des numéros contenant le nombre de chiffres spécifié.

Par exemple, si vous saisissez **amber-{n:fixed=3}**, View remplace **{n:fixed=3}** par un nombre à trois chiffres et crée ces noms de machine : **amber-001**, **amber-002**, **amber-003**, etc.

### Longueur du mode d'attribution de nom quand vous utilisez un jeton de longueur fixe

Les noms qui contiennent des jetons de longueur fixe ont une limite de 15 caractères, y compris votre mode d'attribution de nom et le nombre de chiffres dans le jeton.

**Tableau 12-3.** Longueur maximale du mode d'attribution de nom quand vous utilisez un jeton de longueur fixe

| Jeton de longueur fixe | Longueur maximale du mode d'attribution de nom |
|---|---|
| **{n:fixed=1}** | 14 caractères |
| **{n:fixed=2}** | 13 caractères |
| **{n:fixed=3}** | 12 caractères |

## Exemple de dénomination de machine

Cet exemple montre comment créer deux pools de postes de travail automatisés qui utilisent les mêmes noms de machine mais différentes séries de numéros. Les stratégies utilisées dans cet exemple atteignent un objectif d'utilisateur spécifique et illustrent la flexibilité des méthodes de dénomination de machine.

L'objectif est de créer 2 pools avec la même convention de dénomination, telle que VDIABC-*XX*, où *XX* représente un numéro. Chaque pool a un jeu différent de numéros séquentiels. Par exemple, le premier pool peut contenir les machines VDIABC-01 à VDIABC-10. Le deuxième pool contient les machines VDIABC-11 à VDIABC-20.

Vous pouvez utiliser l'une ou l'autre de ces méthodes de dénomination de machines pour atteindre cet objectif.

- Pour créer des ensembles fixes de machines de façon ponctuelle, spécifiez manuellement des noms de machine.

- Pour créer des machines dynamiquement lorsque les utilisateurs se connectent pour la première fois, fournissez un mode d'attribution de nom et utilisez un jeton pour désigner les numéros séquentiels.

## Spécification manuelle des noms

1 Préparez un fichier texte pour le premier pool qui contient la liste des noms de machine, de VDIABC-01 à VDIABC-10.

2 Dans View Administrator, créez le pool et spécifiez les noms de machine manuellement.

3 Cliquez sur **Entrer des noms** et copiez votre liste dans la zone de liste **Entrer des noms de machine**.

4 Répétez ces étapes pour le deuxième pool, en utilisant les noms VDIABC-11 à VDIABC-20.

Pour obtenir des instructions détaillées, reportez-vous à

« Spécifier une liste de noms de machines », page 154.

Vous pouvez ajouter des machines à chaque pool après sa création. Par exemple, vous pouvez ajouter les machines VDIABC-21 à VDIABC-30 au premier pool, et VDIABC-31 à VDIABC-40 au second. Reportez-vous à la section « Ajouter des machines à un pool automatisé provisionné par une liste de noms », page 158.

## Fournir un mode d'attribution de nom avec un jeton

1 Dans View Administrator, créez le premier pool et utilisez un mode d'attribution de nom pour provisionner les noms de machine.

2 Dans la zone de texte d'attribution de nom, saisissez **`VDIABC-0{n}`**.

3 Limitez la taille maximale du pool à 9.

4 Répétez ces étapes pour le deuxième pool, mais dans la zone de texte d'attribution de nom, saisissez **`VDIABC-1{n}`**.

Le premier pool contient les machines VDIABC-01 à VDIABC-09. Le second pool contient les machines VDIABC-11 à VDIABC-19.

Vous pouvez également configurer les pools pour que chacun contienne jusqu'à 99 machines en utilisant un jeton à longueur fixe de 2 chiffres :

- Pour le premier pool, saisissez **`VDIABC-0{n:fixed=2}`**.
- Pour le deuxième pool, saisissez **`VDIABC-1{n:fixed=2}`**.

Limitez la taille maximale de chaque pool à 99. Cette configuration produit des machines qui contiennent un mode d'attribution de nom séquentiel à 3 chiffres.

First pool:

```
VDIABC-001
VDIABC-002
VDIABC-003
```

Second pool:

```
VDIABC-101
VDIABC-102
VDIABC-103
```

Pour plus d'informations sur les modes d'attribution de nom et les jetons, reportez-vous à « Utilisation d'un mode d'attribution de nom pour des pools de postes de travail automatisés », page 155.

## Ajouter des machines à un pool automatisé provisionné par une liste de noms

Pour ajouter des machines à un pool de postes de travail automatisé provisionné en spécifiant manuellement les noms des machines, vous fournissez une autre liste de nouveaux noms de machines. Cette fonction vous permet de développer un pool de postes de travail et de continuer à utiliser les conventions de dénomination de votre entreprise.

Dans Horizon 7.0, cette fonctionnalité n'est pas prise en charge pour les clones instantanés.

Suivez les instructions suivantes pour ajouter manuellement les noms des machines :

- Tapez chaque nom de machine sur une ligne distincte.
- Un nom de machine peut comporter jusqu'à 15 caractères alphanumériques.
- Vous pouvez ajouter un nom d'utilisateur à chaque entrée de machine. Utilisez une virgule pour séparer le nom d'utilisateur de celui de la machine.

Dans cet exemple, deux machines sont ajoutées. La deuxième machine est associée à un utilisateur :

```
Desktop-001
Desktop-002,abccorp.com/jdoe
```

---

**Remarque** Dans un pool à attribution flottante, vous ne pouvez pas associer des noms d'utilisateurs à des noms de machines. Les machines ne sont pas dédiées aux utilisateurs associés. Dans un pool à attribution flottante, toutes les machines qui ne sont pas utilisées actuellement restent accessibles à tout utilisateur ouvrant une session.

---

### Prérequis

Vérifiez que vous avez créé le pool de postes de travail en spécifiant manuellement les noms des machines. Vous ne pouvez pas ajouter des machines en fournissant de nouveaux noms de machines si vous avez créé le pool en désignant un mode d'attribution de nom.

### Procédure

1. Créez un fichier texte contenant la liste des noms de machines supplémentaires.

   Si vous prévoyez d'ajouter seulement quelques machines, vous pouvez taper les noms de machines directement dans l'assistant Ajouter un pool de postes de travail. Vous n'avez pas à créer un fichier texte séparé.
2. Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.
3. Sélectionnez le pool de postes de travail à étendre.
4. Cliquez sur **Modifier**.
5. Cliquez sur l'onglet **Paramètres d'approvisionnement**.
6. Cliquez sur **Ajouter des machines**.
7. Copiez votre liste de noms de machines dans la page Entrer des noms de machine et cliquez sur **Suivant**.

   L'assistant Entrer des noms de machine affiche la liste des machines et indique les erreurs de validation avec un **X** rouge.
8. Corrigez les noms de machines non valides.
   a. Placez votre curseur sur un nom non valide pour afficher le message d'erreur lié en bas de la page.
   b. Cliquez sur **Précédent**.
   c. Modifiez les noms incorrects et cliquez sur **Suivant**.

9 Cliquez sur **Terminer**.

10 Cliquez sur **OK**.

Dans vCenter Server, vous pouvez surveiller la création des nouvelles machines virtuelles.

Dans View Administrator, vous pouvez afficher les machines à mesure de leur ajout au pool de postes de travail en sélectionnant **Catalogue > Pools de postes de travail**.

# Personnalisation manuelle des machines

Après avoir créé un pool automatisé, vous pouvez personnaliser certaines machines sans réattribuer la propriété. En démarrant les machines en mode de maintenance, vous pouvez les modifier et les tester avant de les mettre à la disposition des utilisateurs.

**Remarque** Cette fonctionnalité n'est pas disponible pour un pool de postes de travail de clone instantané.

## Personnalisation de machines en mode de maintenance

Le mode de maintenance empêche les utilisateurs d'accéder à leurs postes de travail. Si vous démarrez des machines en mode de maintenance, View place chacune d'elles en mode de maintenance lors de sa création.

Dans un pool à attribution dédiée, vous pouvez utiliser le mode de maintenance pour vous connecter à une machine sans devoir réattribuer la propriété à votre propre compte d'administrateur. Lorsque vous avez terminé la personnalisation, vous n'avez pas à rendre la propriété à l'utilisateur auquel la machine est attribuée.

Dans un pool à attribution flottante, vous pouvez tester les machines en mode de maintenance avant de laisser les utilisateurs s'y connecter.

Pour effectuer la même personnalisation sur toutes les machines dans un pool automatisé, personnalisez la machine virtuelle que vous préparez en tant que modèle ou parent. View déploie votre personnalisation sur toutes les machines. Lorsque vous créez le pool, vous pouvez également utiliser une spécification de personnalisation Sysprep pour configurer toutes les machines avec des paramètres d'attribution de licence, d'association de domaine, de protocole DHCP et d'autres propriétés.

**Remarque** Vous pouvez démarrer des machines en mode de maintenance si vous spécifiez manuellement les noms de machines pour le pool, mais pas si vous nommez des machines en fournissant un mode d'attribution de nom.

## Personnaliser des machines individuelles

Vous pouvez personnaliser des machines individuelles après avoir créé un pool en démarrant les machines en mode de maintenance.

### Procédure

1 Dans View Administrator, commencez par créer un pool de postes de travail automatisé en démarrant l'assistant Ajouter un pool de postes de travail.

2 Sur la page Paramètres d'approvisionnement, sélectionnez **Spécifier des noms manuellement**.

3 Sélectionnez **Démarrer des machines en mode de maintenance**.

4 Exécutez l'assistant Ajouter un pool de postes de travail pour terminer la création du pool de postes de travail.

5 Dans vCenter Server, connectez-vous à chaque machine virtuelle, personnalisez-la et testez-la.

   Vous pouvez personnaliser les machines manuellement ou à l'aide d'un logiciel de gestion de systèmes Windows standard tel qu'Altiris, SMS, LanDesk ou BMC.

6 Dans View Administrator, sélectionnez le pool de postes de travail.

7 Utilisez l'outil de filtre pour sélectionner les machines spécifiques à libérer pour vos utilisateurs.

8 Cliquez sur **Plus de commandes > Quitter le mode de maintenance**.

### Suivant

Informez vos utilisateurs qu'ils peuvent ouvrir une session sur leurs postes de travail.

## Paramètres de pools de postes de travail pour tous les types de pools de postes de travail

Vous devez spécifier des paramètres de machine et de pool de postes de travail lorsque vous configurez des pools automatisés contenant des machines virtuelles complètes, des pools de postes de travail de clone lié, des pools de postes de travail manuels, des pools de postes de travail de clone instantané et des pools de postes de travail RDS. Les paramètres ne s'appliquent pas à tous les types de pools de postes de travail.

**Tableau 12-4.** Descriptions des paramètres de pool de postes de travail

| Paramètre | Options |
|---|---|
| État | ■ **Activé**. Une fois créé, le pool de postes de travail est activé et prêt pour une utilisation immédiate.<br>■ **Désactivé**. Une fois créé, le pool de postes de travail est désactivé et ne peut pas être utilisé. L'approvisionnement est arrêté pour le pool. Il s'agit d'un paramètre approprié si vous voulez réaliser des activités de post-déploiement comme des tests ou d'autres formes de maintenance de ligne de base.<br>Lorsque cet état est effectif, les postes de travail distants sont indisponibles. |
| Restrictions du serveur de connexion | ■ **Aucune**. Le pool de postes de travail est accessible à partir de n'importe quelle instance du Serveur de connexion.<br>■ **Avec balises**. Sélectionnez une ou plusieurs balises Serveur de connexion pour rendre le pool de postes de travail accessible uniquement aux instances du Serveur de connexion qui comportent ces balises. Vous pouvez utiliser les cases à cocher pour sélectionner plusieurs balises.<br>Si vous prévoyez de fournir un accès à vos postes de travail via VMware Identity Manager et si vous configurez des limitations du Serveur de connexion, il est possible que l'application VMware Identity Manager affiche les postes de travail aux utilisateurs alors que ces postes de travail sont en réalité limités. Les utilisateurs de VMware Identity Manager ne pourront pas lancer ces postes de travail. |
| Stratégie d'alimentation de machine distante | Détermine comment une machine virtuelle se comporte quand un utilisateur ferme sa session sur le poste de travail associé.<br>Pour la description des options de stratégie d'alimentation, reportez-vous à « Règles d'alimentation pour des pools de postes de travail », page 165<br>Pour plus d'informations sur la façon dont les stratégies d'alimentation affectent les pools automatisés, reportez-vous à « Définition de règles d'alimentation pour des pools de postes de travail », page 165<br>Non applicable aux pools de postes de travail de clone instantané. Les clones instantanés sont toujours activés. |
| Automatically logoff after disconnect (Fermeture de session automatique après la déconnexion) | ■ **Immédiatement**. La session des utilisateurs est fermée dès que ceux-ci se déconnectent.<br>■ **Jamais**. La session des utilisateurs n'est jamais fermée.<br>■ **Après**. Durée après laquelle la session des utilisateurs est fermée lorsque ceux-ci se déconnectent. Saisissez la durée en minutes.<br>L'heure de fermeture de session s'applique aux déconnexions futures. Si un utilisateur a déjà fermé une session de poste de travail lorsque vous définissez une heure de fermeture de session, la durée de fermeture pour cet utilisateur démarre au moment où vous définissez l'heure de fermeture de session, pas lorsque l'utilisateur a fermé sa session. Par exemple, si vous définissez cette valeur sur 5 minutes, et qu'une session a été fermée 10 minutes plus tôt, View fermera cette session 5 minutes après que vous avez défini la valeur. |

**Tableau 12-4.** Descriptions des paramètres de pool de postes de travail (suite)

| Paramètre | Options |
|---|---|
| Autoriser les utilisateurs à réinitialiser leurs machines | Autorisez les utilisateurs à réinitialiser leurs propres postes de travail.<br>Non applicable aux pools de postes de travail de clone instantané. |
| Autoriser l'utilisateur à ouvrir des sessions séparées depuis différents périphériques clients | Lorsque ce paramètre est sélectionné, un utilisateur se connectant au même pool de postes de travail depuis différents périphériques clients accédera à plusieurs sessions de poste de travail. L'utilisateur ne peut rouvrir une session existante qu'à partir du périphérique client depuis lequel la session a été ouverte. Lorsque ce paramètre n'est pas sélectionné, la session existante de l'utilisateur sera rouverte quel que soit le périphérique client utilisé. |
| Supprimer la machine après la fermeture de session | Indiquez si vous souhaitez supprimer les machines virtuelles complètes à attribution flottante.<br>■ **Non**. Les machines virtuelles restent dans le pool de postes de travail quand les utilisateurs ferment leur session.<br>■ **Oui**. Les machines virtuelles sont désactivées et supprimées dès que les utilisateurs ferment leur session.<br>Pour les postes de travail de clone instantané, la machine est toujours supprimée et recréée après la fermeture de session. |
| Supprimer ou actualiser la machine à la fermeture de session | Indiquez si vous souhaiter supprimer, actualiser ou ne pas modifier les machines virtuelles de clone lié à attribution flottante.<br>■ **Jamais**. Les machines virtuelles restent dans le pool et ne sont pas actualisées quand les utilisateurs ferment leur session.<br>■ **Supprimer immédiatement**. Les machines virtuelles sont désactivées et supprimées dès que les utilisateurs ferment leur session. Lorsque les utilisateurs ferment une session, les machines virtuelles passent immédiatement à l'état `Suppression`.<br>■ **Actualiser immédiatement**. Les machines virtuelles sont actualisées dès que les utilisateurs ferment leur session. Lorsque les utilisateurs ferment leur session, les machines virtuelles passent immédiatement en mode de maintenance pour empêcher d'autres utilisateurs d'ouvrir une session au démarrage de l'opération d'actualisation.<br>Pour les postes de travail de clone instantané, la machine est toujours supprimée et recréée après la fermeture de session. |
| Actualiser le disque du système d'exploitation après la fermeture de session | Indiquez si vous souhaitez actualiser les disques du système d'exploitation des machines virtuelles de clone lié à attribution dédiée et, le cas échéant, à quel moment effectuer l'actualisation.<br>■ **Jamais**. Le disque du système d'exploitation n'est jamais actualisé.<br>■ **Toujours**. Le disque du système d'exploitation est actualisé chaque fois que l'utilisateur ferme sa session.<br>■ **Tous les**. Le disque du système d'exploitation est actualisé à intervalles réguliers sur un nombre spécifié de jours. Saisissez le nombre de jours.<br>Le nombre de jours est compté depuis la dernière actualisation, ou depuis l'approvisionnement initial si aucune actualisation ne s'est encore produite. Par exemple, si la valeur spécifiée est **3** jours, et si trois jours se sont écoulés depuis la dernière actualisation, la machine est actualisée après la fermeture de session de l'utilisateur.<br>■ **À**. Le disque du système d'exploitation est actualisé lorsque sa taille actuelle atteint le pourcentage spécifié de sa taille maximale autorisée. La taille maximale du disque du système d'exploitation d'un clone lié est la taille du disque du système d'exploitation du réplica. Saisissez le pourcentage auquel les opérations d'actualisation se produisent.<br>Avec l'option **À**, la taille du disque du système d'exploitation du clone lié dans le magasin de données est comparée à sa taille maximale autorisée. Ce pourcentage d'utilisation du disque ne reflète pas l'utilisation du disque que vous pouvez voir dans le système d'exploitation invité de la machine.<br>Lorsque vous actualisez les disques du système d'exploitation dans un pool de clone lié avec affectation dédiée, les disques persistants de View Composer ne sont pas affectés.<br>Pour les postes de travail de clone instantané, la machine est toujours supprimée et recréée après la fermeture de session. |

**Tableau 12-4.** Descriptions des paramètres de pool de postes de travail (suite)

| Paramètre | Options | |
|---|---|---|
| Protocole d'affichage par défaut | Sélectionnez le protocole d'affichage que vous souhaitez que le Serveur de connexion utilise pour communiquer avec les clients. | |
| | **VMware Blast** | Le protocole VMware Blast Extreme est basé sur le protocole H.264 et prend en charge la plage la plus large de périphériques clients, notamment les smartphones, les tablettes, les PC à très bas coût et les Mac, sur n'importe quel réseau. Ce protocole consomme le moins de ressources CPU, il offre donc une plus longue durée de vie des batteries sur les périphériques mobiles. |
| | **PCoIP** | Option par défaut quand prise en charge. PCoIP est pris en charge en tant que protocole d'affichage pour les machines virtuelles et les machines physiques équipées de matériel Teradici. PCoIP offre une utilisation optimisée du PC pour délivrer des images, du contenu audio et vidéo à un grand nombre d'utilisateurs sur le réseau LAN ou sur le réseau WAN. |
| | **Microsoft RDP** | La Connexion Bureau à distance Microsoft utilise RDP pour transmettre des données. RDP est un protocole multicanal qui permet à un utilisateur de se connecter à distance à un ordinateur. |
| Autoriser les utilisateurs à choisir un protocole | Autoriser les utilisateurs à remplacer le protocole d'affichage par défaut pour leurs postes de travail en utilisant Horizon Client. | |
| Convertisseur 3D | Vous pouvez choisir d'activer le rendu graphique 3D si votre pool comporte des postes de travail Windows 7 ou supérieur. Vous pouvez configurer **Convertisseur 3D** afin qu'il utilise le rendu logiciel ou le rendu matériel en fonction des cartes de processeur graphique physiques installées sur les hôtes ESXi 5.1 ou supérieur.<br>Pour activer cette fonctionnalité, vous devez sélectionner PCoIP ou VMware Blast comme protocole et désactiver le paramètre **Autoriser les utilisateurs à choisir un protocole** (sélectionnez **Non**).<br>Avec les options de **Convertisseur 3D** basé sur le matériel, les utilisateurs peuvent bénéficier des applications graphiques pour la conception, la modélisation et le multimédia. Avec l'option de **Convertisseur 3D** logiciel, les utilisateurs peuvent bénéficier d'améliorations graphiques dans des applications moins gourmandes, telles qu'AERO, Microsoft Office et Google Earth. Pour plus d'informations sur la configuration système, reportez-vous à « Configuration du rendu 3D pour les postes de travail », page 171.<br>Si votre déploiement de View n'est pas exécuté sur vSphere 5.0 ou version ultérieure, ce paramètre n'est pas disponible et est inactif dans View Administrator.<br>Lorsque vous sélectionnez cette fonction, si vous sélectionnez l'option **Automatique**, **Logiciel** ou **Matériel**, vous pouvez configurer la quantité de VRAM attribuée aux machines du pool. Le nombre maximal de moniteurs est de 2 et la résolution maximale est 1 920 x 1 200.<br>Si vous sélectionnez **Gérer à l'aide de vSphere Client** ou **NVIDIA GRID vGPU**, vous devez configurer la quantité de mémoire 3D et le nombre de moniteurs dans vCenter Server. Vous pouvez sélectionner au maximum quatre écrans pour vos machines qui sont utilisées comme des postes de travail distants, en fonction de la résolution d'écran.<br>**Remarque** Lorsque vous configurez ou modifiez ce paramètre, vous devez mettre les machines virtuelles existantes hors tension, vérifier que les machines sont reconfigurées dans vCenter Server, puis mettre les machines sous tension pour que le nouveau paramètre s'applique. Le redémarrage d'une machine virtuelle n'entraîne pas l'application du paramètre.<br>Pour obtenir plus d'informations, reportez-vous à « Configuration du rendu 3D pour les postes de travail », page 171, « Options de convertisseur 3D », page 175. et « Meilleures pratiques pour la configuration du rendu 3D », page 177.<br>Non disponible pour les pools de postes de travail de clone instantané. | |

**Tableau 12-4.** Descriptions des paramètres de pool de postes de travail (suite)

| Paramètre | Options |
|---|---|
| Max number of monitors (Nombre max. d'écrans) | Si vous sélectionnez PCoIP ou VMware Blast comme protocole d'affichage, vous pouvez sélectionner le **Nombre max. d'écrans** sur lesquels les utilisateurs peuvent afficher le poste de travail.<br>Vous pouvez sélectionner jusqu'à quatre écrans.<br>Lorsque le paramètre **Convertisseur 3D** n'est pas sélectionné, le paramètre **Nombre max. d'écrans** affecte la quantité de VRAM attribuée aux machines du pool. Lorsque vous augmentez le nombre d'écrans, davantage de mémoire est consommée sur les hôtes ESXi associés.<br>Lorsque le paramètre **Convertisseur 3D** n'est pas sélectionné, trois écrans au maximum sont pris en charge avec la résolution de 3 840 x 2 160 sur un système d'exploitation invité Windows 7 avec Aero désactivé. Pour les autres systèmes d'exploitation, ou pour Windows 7 avec Aero activé, un écran est pris en charge avec la résolution de 3 840 x 2 160.<br>Lorsque le paramètre **Convertisseur 3D** est sélectionné, un écran est pris en charge avec la résolution 3 840 x 2 160. Une résolution inférieure est plus adaptée lorsqu'il y a plusieurs écrans. Sélectionnez moins d'écrans si vous choisissez une résolution supérieure.<br>**Remarque** Vous devez désactiver et activer des machines virtuelles existantes pour que ce paramètre prenne effet. Le redémarrage d'une machine virtuelle n'entraîne pas la prise d'effet du paramètre.<br>Non disponible pour les pools de postes de travail de clone instantané. Dans Horizon 7.0, le nombre maximal d'écrans pour les clones instantanés est de 2. |
| Max resolution of any one monitor (Résolution max. d'un écran) | Si vous sélectionnez PCoIP ou VMware Blast comme protocole d'affichage, vous devez spécifier l'option **Résolution maximale d'un écran**.<br>L'option **Résolution max. d'un écran** est définie sur 1 920 x 1 200 pixels par défaut, mais vous pouvez configurer cette valeur.<br>Lorsque le paramètre **Convertisseur 3D** n'est pas sélectionné, le paramètre **Résolution max. d'un écran** affecte la quantité de VRAM attribuée aux machines du pool. Lorsque vous augmentez la résolution, davantage de mémoire est consommée sur les hôtes ESXi associés.<br>Lorsque le paramètre **Convertisseur 3D** n'est pas sélectionné, trois écrans au maximum sont pris en charge avec la résolution de 3 840 x 2 160 sur un système d'exploitation invité Windows 7 avec Aero désactivé. Pour les autres systèmes d'exploitation, ou pour Windows 7 avec Aero activé, un écran est pris en charge avec la résolution de 3 840 x 2 160.<br>Lorsque le paramètre **Convertisseur 3D** est sélectionné, un écran est pris en charge avec la résolution 3 840 x 2 160. Une résolution inférieure est plus adaptée lorsqu'il y a plusieurs écrans. Sélectionnez moins d'écrans si vous choisissez une résolution supérieure.<br>**Remarque** Vous devez désactiver et activer des machines virtuelles existantes pour que ce paramètre prenne effet. Le redémarrage d'une machine virtuelle n'entraîne pas la prise d'effet du paramètre.<br>Non disponible pour les pools de postes de travail de clone instantané. Dans Horizon 7.0, la résolution maximale d'un écran est de 2 560 x 1 600. |
| HTML Access | Sélectionnez **Activé** pour autoriser les utilisateurs à se connecter à des postes de travail distants à partir de leur navigateur Web.<br>Lorsqu'un utilisateur se connecte via la page du portail Web VMware Horizon ou via l'application VMware Identity Manager, et qu'il sélectionne un poste de travail distant, l'agent HTML Access autorise l'utilisateur à se connecter au poste de travail via HTTPS. Le poste de travail est affiché dans le navigateur de l'utilisateur. D'autres protocoles d'affichage, tels que PCoIP ou RDP, ne sont pas utilisés. Le logiciel Horizon Client n'a pas besoin d'être installé sur les périphériques clients.<br>Pour utiliser HTML Access, vous devez installer HTML Access dans votre déploiement de View. Pour obtenir plus d'informations, reportez-vous au document *Utilisation de HTML Access*, disponible sur https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.<br>Pour utiliser HTML Access avec VMware Identity Manager, vous devez coupler le Serveur de connexion à un serveur d'authentification SAML, comme expliqué dans le document *Administration de View*. VMware Identity Manager doit être installé et configuré pour une utilisation avec le Serveur de connexion. |

**Tableau 12-4.** Descriptions des paramètres de pool de postes de travail (suite)

| Paramètre | Options |
|---|---|
| Adobe Flash quality (Qualité Adobe Flash) | Détermine la qualité du contenu Adobe Flash affiché sur des pages Web.<br>■ **Ne pas contrôler**. La qualité est déterminée par les paramètres de page Web.<br>■ **Faible**. Ce paramètre se traduit par les meilleures économies de bande passante. Si aucun niveau de qualité n'est spécifié, le système prend la valeur par défaut Low (Faible).<br>■ **Moyenne**. Ce paramètre se traduit par des économies de bande passante modérées.<br>■ **Élevée**. Ce paramètre se traduit par des économies de bande passante moindres.<br>Pour plus d'informations, reportez-vous à la section « Qualité et limitation d'Adobe Flash », page 164. |
| Adobe Flash throttling (Limitation d'Adobe Flash) | Détermine la fréquence d'image des films Adobe Flash. Si vous activez ce paramètre, vous pouvez réduire ou augmenter le nombre d'images affichées par seconde en sélectionnant un niveau d'agressivité.<br>■ **Désactivé**. Aucune limitation n'est effectuée. L'intervalle du temporisateur n'est pas modifié.<br>■ **Classique**. L'intervalle du temporisateur est de 100 millisecondes. Ce paramètre correspond au plus petit nombre d'images ignorées.<br>■ **Modérée**. L'intervalle du temporisateur est de 500 millisecondes.<br>■ **Agressive**. L'intervalle du temporisateur est de 2 500 millisecondes. Ce paramètre correspond au plus grand nombre d'images ignorées.<br>Pour plus d'informations, reportez-vous à la section « Qualité et limitation d'Adobe Flash », page 164. |
| Remplacer les paramètres de Mirage | Pour spécifier le même serveur Mirage pour tous les pools de postes de travail, utilisez le paramètre de configuration global View, plutôt que ce paramètre spécifique du pool.<br>Non disponible pour les pools de postes de travail de clone instantané. |
| Configuration du serveur Mirage | Vous permet de spécifier l'URL d'un serveur Mirage au format **`mirage://server-name:port`** ou **`mirages://server-name:port`**. Ici, *server-name* correspond au nom du domaine complet. Si vous ne spécifiez pas de numéro de port, le port par défaut 8000 est employé.<br>La spécification du serveur Mirage dans View Administrator est une alternative à la spécification du serveur Mirage lors de l'installation du client Mirage. Pour déterminer quelles versions de Mirage prennent en charge la spécification de serveur dans View Administrator, consultez la documentation de Mirage, à l'adresse https://www.vmware.com/support/pubs/mirage_pubs.html.<br>Non disponible pour les pools de postes de travail de clone instantané. |

# Qualité et limitation d'Adobe Flash

Vous pouvez spécifier un niveau admissible maximum de qualité pour le contenu Adobe Flash qui remplace des paramètres de page Web. Si la qualité Adobe Flash pour une page Web est supérieure au niveau maximum autorisé, la qualité est réduite au maximum spécifié. Une qualité inférieure se traduit par plus d'économies de bande passante.

Pour utiliser des paramètres de réduction de bande passante Adobe Flash, Adobe Flash ne doit pas être exécuté en mode Plein écran.

Tableau 12-5 montre les paramètres de qualité du rendu Adobe Flash disponibles.

**Tableau 12-5.** Paramètres de qualité d'Adobe Flash

| Paramètre de qualité | Description |
|---|---|
| **Ne pas contrôler** | La qualité est déterminée par les paramètres de page Web. |
| **Basse** | Ce paramètre se traduit par les meilleures économies de bande passante. |
| **Moyenne** | Ce paramètre se traduit par des économies de bande passante modérées. |
| **Haute** | Ce paramètre se traduit par des économies de bande passante moindres. |

Si aucun niveau maximum de qualité n'est spécifié, le système prend la valeur par défaut **Faible**.

Adobe Flash utilise des services de temporisateur pour mettre à jour ce qui apparaît à l'écran à une heure donnée. La valeur d'intervalle du temporisateur Adobe Flash classique est comprise entre 4 et 50 millisecondes. En limitant, ou en prolongeant, l'intervalle, vous pouvez réduire la fréquence d'image et ainsi réduire la bande passante.

Tableau 12-6 montre les paramètres de limitation d'Adobe Flash disponibles.

**Tableau 12-6.** Paramètres de limitation d'Adobe Flash

| Paramètre de limitation | Description |
|---|---|
| **Désactivé** | Aucune limitation n'est effectuée. L'intervalle du temporisateur n'est pas modifié. |
| **Classique** | L'intervalle du temporisateur est de 100 millisecondes. Ce paramètre correspond au plus petit nombre d'images ignorées. |
| **Modérée** | L'intervalle du temporisateur est de 500 millisecondes. |
| **Agressive** | L'intervalle du temporisateur est de 2 500 millisecondes. Ce paramètre correspond au plus grand nombre d'images ignorées. |

La vitesse audio reste constante quel que soit le paramètre de limitation sélectionné.

# Définition de règles d'alimentation pour des pools de postes de travail

Vous pouvez configurer une stratégie d'alimentation pour les machines virtuelles d'un pool de postes de travail si les machines virtuelles sont gérées par vCenter Server, sauf les clones instantanés. Les clones instantanés sont toujours activés.

Les règles d'alimentation contrôlent comment une machine virtuelle se comporte lorsque son poste de travail associé n'est pas utilisé. Un poste de travail est considéré comme n'étant pas utilisé avant qu'un utilisateur ouvre une session et après qu'un utilisateur se déconnecte ou ferme sa session. Les règles d'alimentation contrôlent également comment une machine virtuelle se comporte après l'exécution de tâches administratives, telles qu'une actualisation, une recomposition et un rééquilibrage.

Vous configurez des règles d'alimentation lorsque vous créez ou modifiez des pools de postes de travail dans View Administrator.

**Remarque** Vous ne pouvez pas configurer des stratégies d'alimentation pour des pools de postes de travail comportant des machines non gérées.

## Règles d'alimentation pour des pools de postes de travail

Les stratégies d'alimentation contrôlent le comportement d'une machine virtuelle lorsque son poste de travail distant associé n'est pas utilisé.

Vous définissez des stratégies d'alimentation lorsque vous créez ou modifiez un pool de postes de travail. Tableau 12-7 décrit les stratégies d'alimentation disponibles.

**Tableau 12-7.** Règles d'alimentation

| Règle d'alimentation | Description |
|---|---|
| **Ne prendre aucune action d'alimentation** | View n'applique aucune stratégie d'alimentation après la fermeture d'une session par un utilisateur. Ce paramètre a deux conséquences.<br>■ View ne modifie pas l'état d'alimentation de la machine virtuelle après la fermeture d'une session par un utilisateur.<br>Par exemple, si un utilisateur éteint la machine virtuelle, celle-ci reste désactivée. Si un utilisateur ferme sa session sans éteindre, la machine virtuelle reste activée. Lorsqu'un utilisateur se reconnecte au poste de travail, la machine virtuelle redémarre si elle a été désactivée.<br>■ View n'applique aucun état d'alimentation après l'exécution d'une tâche administrative.<br>Par exemple, un utilisateur peut fermer sa session sans éteindre. La machine virtuelle reste activée. Quand une recomposition planifiée a lieu, la machine virtuelle est désactivée. Après la recomposition, View ne fait rien pour modifier l'état d'alimentation de la machine virtuelle. Elle reste désactivée. |
| **S'assurer que les machines sont toujours sous tension** | La machine virtuelle reste activée, même lorsqu'elle n'est pas utilisée. Si un utilisateur éteint la machine virtuelle, elle redémarre immédiatement. La machine virtuelle redémarre également après l'exécution d'une tâche administrative, telle qu'une actualisation, une recomposition ou un rééquilibrage.<br>Sélectionnez **S'assurer que les machines sont toujours sous tension** si vous exécutez des processus de traitement par lot ou des outils de gestion système qui doivent contacter les machines virtuelles à des heures planifiées. |
| **Interrompre** | La machine virtuelle est interrompue quand un utilisateur ferme sa session, mais pas quand il se déconnecte.<br>Vous pouvez également configurer les machines d'un pool dédié afin qu'elles soient interrompues lorsqu'un utilisateur se déconnecte sans fermer sa session. Pour configurer cette règle, vous devez définir un attribut dans View LDAP. Reportez-vous à la section « Configurer des machines dédiées à interrompre après la déconnexion des utilisateurs », page 168.<br>Lorsque plusieurs machines virtuelles reprennent après avoir été interrompues, l'activation de certaines d'entre elles peut être retardée. Les retards dépendent du matériel de l'hôte ESXi et du nombre de machines virtuelles configurées sur un hôte ESXi. Les utilisateurs qui se connectent à leur poste de travail à partir d'Horizon Client peuvent voir temporairement un message indiquant que le poste de travail n'est pas disponible. Pour accéder à leurs postes de travail, les utilisateurs peuvent se reconnecter. |
| **Mettre hors tension** | La machine virtuelle s'éteint quand un utilisateur ferme sa session, mais pas quand il se déconnecte. |

**Remarque** Lorsque vous ajoutez une machine à un pool manuel, View met la machine sous tension pour s'assurer qu'elle est complètement configurée, même lorsque vous sélectionnez la stratégie d'alimentation **Désactiver** ou **Ne prendre aucune action d'alimentation**. Quand Horizon Agent est configuré, il est marqué comme étant Ready (Prêt) et les paramètres normaux de gestion d'alimentation pour le pool s'appliquent.

Pour les pools manuels incluant des machines gérées par vCenter Server, View s'assure qu'une machine de rechange est sous tension afin que les utilisateurs puissent s'y connecter. La machine de rechange est mise sous tension, quelle que soit la stratégie d'alimentation en vigueur.

Tableau 12-8 indique à quel moment View applique la stratégie d'alimentation configurée.

**Tableau 12-8.** Moment auquel View applique la stratégie d'alimentation

| Type de pool de postes de travail | La règle d'alimentation est appliquée... |
|---|---|
| Pool manuel contenant une seule machine (machine virtuelle gérée par vCenter Server) | Les opérations d'alimentation sont initiées par la gestion des sessions. La machine virtuelle est activée lorsqu'un utilisateur demande le poste de travail, et désactivée ou interrompue quand l'utilisateur ferme sa session.<br>**Remarque** La stratégie **S'assurer que les machines sont toujours sous tension** s'applique toujours, que le pool d'une seule machine utilise une attribution flottante ou dédiée, et que la machine soit ou non attribuée. |
| Pool automatisé avec affectation dédiée | Aux machines non attribuées uniquement.<br>Sur les machines attribuées, les opérations d'alimentation sont initiées par la gestion des sessions. Les machines virtuelles sont mises sous tension lorsqu'un utilisateur demande une machine attribuée, et elles sont mises hors tension ou interrompues lorsque l'utilisateur ferme sa session.<br>**Remarque** La stratégie **S'assurer que les machines sont toujours sous tension** s'applique aux machines attribuées et non attribuées. |
| Pool automatisé avec affectation flottante | Lorsqu'une machine n'est pas utilisée et qu'un utilisateur ferme sa session.<br>Lorsque vous configurez la stratégie d'alimentation **Désactiver** ou **Interrompre** pour un pool de postes de travail à attribution flottante, définissez **Fermeture de session automatique après la déconnexion** sur **Immédiatement** pour éviter les sessions ignorées ou orphelines. |
| Pool manuel avec affectation dédiée | Aux machines non attribuées uniquement.<br>Sur les machines attribuées, les opérations d'alimentation sont initiées par la gestion des sessions. Les machines virtuelles sont mises sous tension lorsqu'un utilisateur demande une machine attribuée, et elles sont mises hors tension ou interrompues lorsque l'utilisateur ferme sa session.<br>**Remarque** La stratégie **S'assurer que les machines sont toujours sous tension** s'applique aux machines attribuées et non attribuées. |
| Pool manuel avec affectation flottante | Lorsqu'une machine n'est pas utilisée et qu'un utilisateur ferme sa session.<br>Lorsque vous configurez la stratégie d'alimentation **Désactiver** ou **Interrompre** pour un pool de postes de travail à attribution flottante, définissez **Fermeture de session automatique après la déconnexion** sur **Immédiatement** pour éviter les sessions ignorées ou orphelines. |

La façon dont View applique la stratégie d'alimentation configurée à des pools automatisés dépend de la disponibilité d'une machine. Pour plus d'informations, reportez-vous à « Effet de stratégies d'alimentation sur les pools de postes de travail automatisés », page 168.

## Configurer des machines dédiées à interrompre après la déconnexion des utilisateurs

La stratégie d'alimentation **Interrompre** entraîne l'interruption de machines virtuelles lorsqu'un utilisateur ferme une session, mais pas lorsqu'il se déconnecte. Vous pouvez également configurer les machines d'un pool dédié pour les interrompre lorsque l'utilisateur se déconnecte d'un poste de travail sans fermer la session. L'utilisation de la stratégie d'interruption lors de la déconnexion des utilisateurs permet d'économiser des ressources.

Pour activer l'interruption lors de la déconnexion pour des machines dédiées, vous devez définir un attribut dans View LDAP.

### Procédure

1 Démarrez l'utilitaire ADSI Edit sur votre hôte du Serveur de connexion View.

2 Dans l'arborescence de la console, sélectionnez **Se connecter à**.

3 Dans le champ **Sélectionnez ou entrez un domaine ou un serveur**, tapez le nom du serveur sous la forme `localhost:389`

4 Sous **Point de connexion**, cliquez sur **Sélectionnez ou entrez un nom unique ou un contexte d'attribution de nom**, tapez le nom unique sous la forme `DC=vdi,DC=vmware,DC=int`, puis cliquez sur **OK**.

   La fenêtre principale de l'Éditeur ADSI ADAM s'affiche.

5 Développez l'arborescence d'ADAM ADSI et développez **OU=Properties**.

6 Sélectionnez **OU=Global** et sélectionnez **CN=Common** dans le volet de droite

7 Sélectionnez **Action > Propriétés** et, sous l'attribut **pae-NameValuePair**, ajoutez l'entrée `suspendOnDisconnect=1`.

8 Redémarrez le service Serveur de connexion VMware Horizon View ou Serveur de connexion View.

## Effet de stratégies d'alimentation sur les pools de postes de travail automatisés

La façon dont View applique la stratégie d'alimentation configurée à des pools automatisés dépend de la disponibilité d'une machine.

Une machine dans un pool automatisé est considérée comme étant disponible lorsqu'elle satisfait les critères suivants :

- Il est actif.
- Il ne contient pas de session utilisateur.
- Il n'est pas affecté à un utilisateur.

Le service Horizon Agent en cours d'exécution sur la machine confirme la disponibilité de la machine au Serveur de connexion View.

Lorsque vous configurez un pool automatisé, vous pouvez spécifier le nombre minimal et maximal de machines virtuelles devant être provisionnées, et le nombre de machines de rechange devant être maintenues sous tension et disponibles à tout moment.

## Exemples de règle d'alimentation pour des pools automatisés avec des affectations flottantes

Lorsque vous configurez un pool automatisé à attributions flottantes, vous pouvez spécifier qu'un nombre particulier de machines doit être disponible à une heure donnée. Les machines de rechange disponibles sont toujours sous tension, quelle que soit la définition de la stratégie de pool.

### Exemple 1 de règle d'alimentation

Tableau 12-9 décrit le pool automatisé d'affectation flottante dans cet exemple. Le pool utilise un mode d'attribution de nom de machine pour provisionner et nommer les machines.

**Tableau 12-9.** Exemple 1 des paramètres de pool de postes de travail d'un pool automatisé avec une affectation flottante

| Paramètre du pool de postes de travail | Valeur |
|---|---|
| Nombre de machines (minimum) | 10 |
| Nombre de machines (maximum) | 20 |
| Nombre de machines de rechange sous tension | 2 |
| Stratégie d'alimentation de machine distante | Désactiver |

Lorsque ce pool de postes de travail est provisionné, 10 machines sont créées, deux machines sont mises sous tension et deviennent immédiatement disponibles, et huit machines sont mises hors tension.

Pour chaque nouvel utilisateur qui se connecte au pool, une machine est mise sous tension pour conserver le nombre de machines de rechange disponibles. Lorsque le nombre d'utilisateurs connectés est supérieur à huit, des machines supplémentaires (20 au maximum) sont créées pour conserver le nombre de machines de rechange. Lorsque le nombre maximal est atteint, les machines des deux premiers utilisateurs qui se déconnectent restent sous tension pour conserver le nombre de machines de rechange. La machine de chaque utilisateur suivant est mise hors tension conformément à la stratégie d'alimentation.

### Exemple 2 de règle d'alimentation

Tableau 12-10 décrit le pool automatisé d'affectation flottante dans cet exemple. Le pool utilise un mode d'attribution de nom de machine pour provisionner et nommer les machines.

**Tableau 12-10.** Exemple 2 des paramètres de pool de postes de travail d'un pool automatisé avec des affectations flottantes

| Paramètre du pool de postes de travail | Valeur |
|---|---|
| Nombre de machines (minimum) | 5 |
| Nombre de machines (maximum) | 5 |
| Nombre de machines de rechange sous tension | 2 |
| Stratégie d'alimentation de machine distante | Désactiver |

Lorsque ce pool de postes de travail est provisionné, cinq machines sont créées, deux machines sont mises sous tension et deviennent immédiatement disponibles, et trois machines sont mises hors tension.

Si une quatrième machine de ce pool est mise hors tension, l'une des machines existantes est mise sous tension. Aucune machine supplémentaire n'est mise sous tension, car le nombre maximal de machines est déjà atteint.

## Exemple de règle d'alimentation pour des pools automatisés avec des affectations dédiées

Contrairement à une machine sous tension d'un pool automatisé à attributions flottantes, une machine sous tension d'un pool automatisé à attributions dédiées n'est pas nécessairement disponible. Elle n'est disponible que si elle n'est pas attribuée à un utilisateur.

Tableau 12-11 décrit le pool automatisé d'affectation dédiée dans cet exemple.

**Tableau 12-11.** Exemple des paramètres de pool de postes de travail d'un pool automatisé avec des affectations dédiées

| Paramètre du pool de postes de travail | Valeur |
|---|---|
| Nombre de machines (minimum) | 3 |
| Nombre de machines (maximum) | 5 |
| Nombre de machines de rechange sous tension | 2 |
| Stratégie d'alimentation de machine distante | S'assurer que les machines sont toujours sous tension |

Lorsque ce pool de postes de travail est provisionné, trois machines sont créées et mises sous tension. Si les machine sont mises hors tension dans vCenter Server, elles sont immédiatement remises sous tension, conformément à la stratégie d'alimentation.

Lorsqu'un utilisateur se connecte à une machine du pool, celle-ci lui est attribuée de façon permanente. Dès qu'il s'en déconnecte, la machine n'est plus disponible pour les autres utilisateurs. En revanche, la stratégie **S'assurer que les machines sont toujours sous tension** s'applique toujours. Si la machine attribuée est mise hors tension dans vCenter Server, elle est immédiatement remise sous tension.

Lorsqu'un autre utilisateur se connecte, une deuxième machine est attribuée. Comme le nombre de machines de rechange devient inférieur à la limite lorsque le deuxième utilisateur se connecte, une autre machine est créée et mise sous tension. Une machine supplémentaire est créée et mise sous tension chaque fois qu'un nouvel utilisateur est attribué, jusqu'à ce que la limite du nombre maximal de machines soit atteinte.

## Éviter les conflits de règle d'alimentation de View

Lorsque vous utilisez View Administrator pour configurer une règle d'alimentation, vous devez comparer la règle d'alimentation aux paramètres dans le panneau de configuration Options d'alimentation du système d'exploitation client pour éviter les conflits de règle d'alimentation.

Une machine virtuelle peut devenir temporairement inaccessible si sa stratégie d'alimentation configurée n'est pas compatible avec celle qui est configurée pour le système d'exploitation invité. Si le même pool contient d'autres machines, elles peuvent également être affectées.

La configuration suivante est un exemple de conflit de règle d'alimentation :

- Dans View Administrator, la stratégie d'alimentation **Interrompre** est configurée pour la machine virtuelle. Cette règle force la machine virtuelle à s'interrompre lorsqu'elle n'est pas utilisée.
- Dans le panneau de configuration Options d'alimentation du système d'exploitation client, l'option **Mettre l'ordinateur en veille** est définie sur trois minutes.

Dans cette configuration, le Serveur de connexion View et le système d'exploitation client peuvent interrompre la machine virtuelle. L'option d'alimentation du système d'exploitation client peut rendre la machine virtuelle indisponible lorsque le Serveur de connexion View s'attend à la voir activée.

## Configuration du rendu 3D pour les postes de travail

Lorsque vous créez ou modifiez un pool de postes de travail de machines virtuelles, vous pouvez configurer le rendu graphique 3D pour vos postes de travail. Les postes de travail peuvent tirer parti de vSGA (Virtual Shared Graphics Acceleration),vDGA (Virtual Dedicated Graphics Acceleration) ou NVIDIA GRID vGPU (accélération matérielle GPU partagée). vDGA et NVIDIA GRID vGPU sont des fonctionnalités vSphere qui utilisent les cartes graphiques physiques installées sur les hôtes ESXi et gèrent les ressources GPU (processeur graphique) entre plusieurs machines virtuelles.

**Remarque** Cette fonctionnalité n'est pas disponible pour les clones instantanés dans Horizon 7.0.

Les utilisateurs peuvent bénéficier d'applications 3D pour la conception, la modélisation et le multimédia, qui exigent généralement une GPU physique pour être exécutées correctement. Pour les utilisateurs qui n'ont pas besoin d'une ressource GPU physique, une option logicielle fournit les améliorations graphiques pouvant prendre en charge des applications moins exigeantes telles que Windows AERO, Microsoft Office et Google Earth. Voici de brèves descriptions des options graphiques 3D :

**NVIDIA GRID vGPU (accélération matérielle GPU partagée)**

Disponible dans vSphere 6.0 et versions ultérieures, cette fonctionnalité permet de partager une seule ressource GPU physique sur un hôte ESXi entre plusieurs machines virtuelles. Cette fonctionnalité offre des profils 3D souples accélérés par le matériel allant des exécutants de tâches 3D légères aux utilisateurs graphiques expérimentés de stations de travail haut de gamme.

**GPU multi-utilisateur AMD utilisant vDGA**

Disponible avec vSphere 6.0 et versions ultérieures, cette fonctionnalité permet à plusieurs machines virtuelles de partager un GPU AMD en faisant apparaître le GPU sous la forme de plusieurs périphériques de relais PCI. Cette fonctionnalité offre des profils 3D souples accélérés par le matériel allant des exécutants de tâches 3D légères aux utilisateurs graphiques expérimentés de stations de travail haut de gamme.

**vDGA (Virtual Dedicated Graphics Acceleration)**

Disponible dans vSphere 5.5 et versions ultérieures, cette fonctionnalité dédie une seule GPU physique sur un hôte ESXi à une machine virtuelle unique. Utilisez cette fonctionnalité si vous avez besoin de graphiques de workstation haut de gamme accélérés par le matériel.

**Remarque** Certaines cartes Intel vDGA requièrent une version spécifique de vSphere 6. Consultez la liste de compatibilité matérielle VMware à l'adresse http://www.vmware.com/resources/compatibility/search.php. De plus, pour Intel vDGA, le GPU intégré Intel est utilisé à la place de GPU discrets, comme c'est le cas avec d'autres fournisseurs.

**vSGA (Virtual Shared Graphics Acceleration)**

Disponible dans vSphere 5.1 et versions ultérieures, cette fonctionnalité permet à plusieurs machines virtuelles de partager des GPU physiques sur les hôtes ESXi. Cette fonctionnalité convient aux applications de milieu de gamme de conception 3D, de modélisation et de contenu multimédia.

**Soft 3D**

Les graphiques à accélération logicielle, disponibles dans vSphere 5.0 et versions ultérieures, vous permettent d'exécuter des applications DirectX 9 et OpenGL 2.1 sans nécessiter de GPU physique. Utilisez cette fonctionnalité pour les applications 3D moins exigeantes, comme les thèmes Windows Aero, Microsoft Office 2010 et Google Earth.

Comme NVIDIA GRID vGPU, GPU multi-utilisateur AMD utilisant vDGA et toutes les solutions vDGA utilisent le relais PCI sur l'hôte ESXi, Live VMotion n'est pas pris en charge. vSGA et Soft 3D prennent en charge Live VMotion.

Dans certains cas, si une application comme un jeu vidéo ou un benchmark 3D contraint le poste de travail à s'afficher en mode Plein écran, il se peut que la session du poste de travail se déconnecte. Les solutions possibles consistent notamment à configurer l'application pour qu'elle s'exécute en mode fenêtré ou à faire correspond re la résolution du poste de travail de la session View à la résolution par défaut requise par l'application.

## Configuration requise pour tous les types de rendu 3D

Pour activer le rendu graphique 3D, votre déploiement de pools doit répondre aux exigences suivantes :

- Les machines virtuelles doivent fonctionner sous Windows 7 ou version ultérieure.
- Le pool doit utiliser PCoIP ou VMware Blast Extreme comme protocole d'affichage par défaut.
- Les utilisateurs ne doivent pas être autorisés à choisir leur propre protocole.

**Important** Lorsque vous configurez ou modifiez le paramètre **Convertisseur 3D**, vous devez mettre hors tension les machines virtuels existantes, vérifier que les machines sont reconfigurées dans vCenter Server, puis mettre les machines sous tension pour appliquer le nouveau paramètre. Le redémarrage d'une machine virtuelle n'entraîne pas l'application du paramètre.

## Conditions requises supplémentaires pour NVIDIA GRID vGPU

Avec NVIDIA GRID vGPU, une GPU physique unique sur un hôte ESXi peut être partagée entre plusieurs machines virtuelles. Pour prendre en charge ce type d'accélération matérielle GPU partagée, un pool doit satisfaire les conditions requises suivantes :

- Les machines virtuelles doivent s'exécuter sur ESXi 6.0 ou des hôtes de version ultérieure, disposer d'un matériel virtuel de version 11 ou ultérieure, et être gérées par vCenter Server 6.0 ou un logiciel de version ultérieure.

  Vous devez configurer la machine virtuelle parente ou le modèle de machine virtuelle pour utiliser un périphérique PCI partagé avant de pouvoir créer le pool de postes de travail dans View. Pour obtenir des instructions détaillées, consultez le Guide de déploiement de NVIDIA GRID vGPU pour VMware Horizon 6.1.
- Vous devez installer les pilotes graphiques du fournisseur de ressource GPU dans le système d'exploitation invité de la machine virtuelle.

  **Remarque** Pour voir une liste du matériel de processeur graphique pris en charge, consultez la liste de compatibilité matérielle VMware à l'adresse http://www.vmware.com/resources/compatibility/search.php.
- Vous devez définir l'option **Convertisseur 3D** dans View Administrator sur **NVIDIA GRID vGPU**.

## Conditions requises supplémentaires pour AGPU multi-utilisateur AMD utilisant vDGA

Avec GPU multi-utilisateur AMD utilisant vDGA, plusieurs machines virtuelles peuvent partager un GPU AMD en faisant apparaître le GPU sous la forme de plusieurs périphériques de relais PCI. Pour prendre en charge ce type d'accélération matérielle GPU partagée, un pool doit satisfaire les conditions requises suivantes :

- Les machines virtuelles doivent s'exécuter sur ESXi 6.0 ou des hôtes de version ultérieure, disposer d'un matériel virtuel de version 11 ou ultérieure, et être gérées par vCenter Server 6.0 ou un logiciel de version ultérieure.

- Vous devez activer le relais GPU sur les hôtes ESXi, configurer AMD SR-IOV (virtualisation d'E/S d'une racine unique) et configurer les machines virtuelles individuelles pour utiliser des périphériques PCI dédiés. Reportez-vous à la section « Préparation de l'utilisation des capacités du GPU multi-utilisateur AMD utilisant vDGA », page 181.

  **Remarque** Seuls les pools de postes de travail manuels sont pris en charge pour cette version.

- Vous devez installer les pilotes graphiques du fournisseur de ressource GPU dans le système d'exploitation invité de la machine virtuelle.

  **Remarque** Pour voir une liste du matériel de processeur graphique pris en charge, consultez la liste de compatibilité matérielle VMware à l'adresse http://www.vmware.com/resources/compatibility/search.php.

- Vous devez définir l'option **Convertisseur 3D** dans View Administrator sur **Gérer à l'aide de vSphere Client**.

## Conditions requises supplémentaires pour l'utilisation de vDGA

Cette fonctionnalité dédie une ressource GPU (carte graphique) physique unique sur un hôte ESXi à une seule machine virtuelle. Pour prendre en charge vDGA, un pool doit satisfaire ces conditions requises supplémentaires :

- Les machines virtuelles doivent s'exécuter sur ESXi 5.5 ou des hôtes de version ultérieure, disposer d'un matériel virtuel de version 9 ou ultérieure, et être gérées par vCenter Server 5.5 ou un logiciel de version ultérieure.

  Vous devez activer le relais GPU sur les hôtes ESXi et configurer les machines virtuelles individuelles pour utiliser des périphériques PCI dédiés après la création du pool de postes de travail dans View. Vous ne pouvez pas configurer la machine virtuelle parente ou un modèle pour vDGA, puis créer un pool de postes de travail, car la même GPU physique serait dédiée à chaque machine virtuelle du pool. Reportez-vous à « Installation de vDGA » dans le Livre blanc VMware sur l'accélération graphique.

  Pour les machines virtuelles de clone lié, les paramètres vDGA sont conservés après les opérations d'actualisation, de recomposition et de rééquilibrage.

- Vous devez installer les pilotes graphiques du fournisseur de ressource GPU dans le système d'exploitation invité de la machine virtuelle.

  **Remarque** Pour voir une liste du matériel de processeur graphique pris en charge, consultez la liste de compatibilité matérielle VMware à l'adresse http://www.vmware.com/resources/compatibility/search.php.

- Vous devez définir l'option **Convertisseur 3D** sur **Gérer à l'aide de vSphere Client**.

## Conditions requises supplémentaires pour l'utilisation de vSGA

vSGA permet à plusieurs machines virtuelles de partager les GPU physiques sur des hôtes ESXi. Pour prendre en charge vSGA, un pool doit satisfaire les conditions requises supplémentaires suivantes :

- Les machines virtuelles doivent s'exécuter sur des hôtes ESXi 5.1 ou version ultérieure, et doivent être gérées par vCenter Server 5.1 ou un logiciel de version ultérieure.
- Les cartes de processeur graphique et les VIB (vSphere Installation Bundle) associés doivent être installés sur les hôtes ESXi. Pour voir une liste du matériel de processeur graphique pris en charge, consultez la liste de compatibilité matérielle VMware à l'adresse http://www.vmware.com/resources/compatibility/search.php.

- Les machines Windows 7 doivent disposer de la version matérielle virtuelle 8 ou ultérieure. Les machines Windows 8 doivent disposer de la version matérielle virtuelle 9 ou ultérieure. Les machines Windows 10 doivent disposer de la version matérielle virtuelle 10 ou ultérieure.
- Vous pouvez définir l'option **Convertisseur 3D** sur l'un des paramètres suivants : **Gérer à l'aide de vSphere Client**, **Automatique** ou **Matériel**. Voir aussi « Options de configuration RAM vidéo pour le convertisseur 3D », page 174.

  **Automatique** utilise l'accélération matérielle si une ressource GPU matérielle compatible est disponible sur l'hôte ESXi. Si une ressource GPU matérielle n'est pas disponible, la machine virtuelle utilise le convertisseur 3D logiciel pour les tâches 3D.

## Conditions requises supplémentaires pour l'utilisation de Soft 3D

Pour prendre en charge le rendu 3D logiciel, un pool doit répondre aux exigences supplémentaires suivantes :

- Les machines virtuelles doivent s'exécuter sur ESXi 5.0 ou version ultérieure, et doivent être gérées par vCenter Server 5.0 ou un logiciel de version ultérieure.
- Les machines doivent disposer de la version 8 du matériel virtuel ou d'une version ultérieure.
- Vous devez définir l'option **Convertisseur 3D** sur **Logiciel**. Voir aussi « Options de configuration RAM vidéo pour le convertisseur 3D », page 174.

## Options de configuration RAM vidéo pour le convertisseur 3D

Lorsque vous activez le paramètre **Convertisseur 3D**, si vous sélectionnez l'option **Automatique**, **Logiciel** ou **Matériel**, vous pouvez configurer la quantité de VRAM attribuée aux machines virtuelles dans le pool en déplaçant le curseur dans la boîte de dialogue Configurer VRAM pour les clients 3D. La taille VRAM minimale est de 64 Mo. La quantité de VRAM par défaut dépend de la version du matériel virtuel :

- Pour les machines virtuelles disposant de la version matérielle virtuelle 8 (vSphere 5.0), la taille VRAM par défaut est de 64 Mo et vous pouvez configurer une taille maximale de 128 Mo.
- Pour les machines virtuelles disposant de la version matérielle virtuelle 9 (vSphere 5.1) et 10 ( vSphere 5.5 Update 1), la taille VRAM par défaut est de 96 Mo et vous pouvez configurer une taille maximale de 512 Mo.
- Pour les machines virtuelles disposant de la version matérielle virtuelle 11 (vSphere 6.0), la taille VRAM par défaut est de 96 Mo et vous pouvez configurer une taille maximale de 128 Mo. Dans vSphere 6.0 et les machines virtuelles ultérieures, ce paramètre se réfère uniquement à la quantité de mémoire graphique de la carte graphique et a donc un paramètre maximal inférieur aux versions de matériel virtuel antérieures qui incluaient la mémoire graphique et la mémoire d'invité pour le stockage des objets 3D.

Les paramètres VRAM que vous configurez dans View Administrator sont prioritaires sur les paramètres VRAM qui peuvent être configurés pour les machines virtuelles dans vSphere Client ou vSphere Web Client, sauf si vous sélectionnez l'option **Gérer à l'aide de vSphere Client**.

Pour plus d'informations sur les options de convertisseur 3D **Automatique**, **Logiciel** ou **Matériel**, reportez-vous à « Options de convertisseur 3D », page 175.

## Options de convertisseur 3D

Le paramètre **Convertisseur 3D** pour les pools de postes de travail fournit des options vous permettant de configurer le rendu graphique de différentes façons.

Le tableau suivant décrit les différences entre les divers types d'options de rendu 3D disponibles dans View Administrator, mais ne fournit pas d'informations complètes pour la configuration de machines virtuelles et d'hôtes ESXi pour vSGA (Virtual Shared Graphics Acceleration), vDGA (Virtual Dedicated Graphics Acceleration), les GPU multi-utilisateurs AMD utilisant vDGA et NVIDIA GRID vGPU (accélération matérielle GPU partagée). Ces tâches peuvent être effectuées avec vSphere Web Client avant de tenter de créer des pools de postes de travail dans Administrator. Pour obtenir des instructions sur ces tâches pour vSGA et vDGA, reportez-vous au Libre blanc VMware sur l'accélération graphique. Pour obtenir des instructions sur NVIDIA GRID vGPU, consultez le Guide de déploiement de NVIDIA GRID vGPU pour VMware Horizon 6.1. Pour obtenir des instructions sur le GPU multi-utilisateur AMD utilisant vDGA, reportez-vous à la section « Préparation de l'utilisation des capacités du GPU multi-utilisateur AMD utilisant vDGA », page 181.

**Tableau 12-12.** Options du convertisseur 3D pour les pools exécutés sur vSphere 5.1 ou supérieur

| Option | Description |
|---|---|
| Gérer à l'aide de vSphere Client | L'option **Convertisseur 3D** définie dans vSphere Web Client (ou vSphere Client dans vSphere 5.1 ou version ultérieure) pour une machine virtuelle détermine le type de rendu graphique 3D obtenu. View ne contrôle pas le rendu 3D.<br>Dans vSphere Web Client, vous pouvez configurer les options **Automatique**, **Logiciel** ou **Matériel**. Ces options ont le même effet que lorsque vous les définissez dans View Administrator.<br>Utilisez ce paramètre lors de la configuration de vDGA et du GPU multi-utilisateur AMD utilisant vDGA. Ce paramètre est également une option pour vSGA.<br>Lorsque vous sélectionnez l'option **Gérer à l'aide de vSphere Client**, les paramètres **Configurer VRAM pour des clients 3D**, **Nombre max. d'écrans** et **Résolution max. d'un écran** sont inactifs dans View Administrator. Vous pouvez configurer la quantité de mémoire de vSphere Web Client. |
| Automatique | Le rendu 3D est activé. L'hôte ESXi contrôle le type de rendu 3D qui a lieu.<br>Par exemple, l'hôte ESXi réserve des ressources matérielles de processeur graphique sur la base « premier arrivé, premier servi » à mesure que les machines virtuelles sont activées. Si toutes les ressources matérielles de processeur graphique sont déjà réservées lorsqu'une machine virtuelle est activée, ESXi utilise le convertisseur logiciel pour cette machine.<br>Ce paramètre est une option lors de la configuration de vSGA.<br>L'hôte ESXi alloue de la VRAM à une machine virtuelle en fonction de la valeur définie dans la boîte de dialogue Configurer VRAM pour des clients 3D. |
| Logiciel | Le rendu 3D est activé. L'hôte ESXi utilise le rendu graphique 3D logiciel. Si une carte de processeur graphique est installée sur l'hôte ESXi, ce pool ne l'utilisera pas.<br>Utilisez ce paramètre pour configurer Soft 3D.<br>L'hôte ESXi alloue de la VRAM à une machine virtuelle en fonction de la valeur définie dans la boîte de dialogue Configurer VRAM pour des clients 3D. |

**Tableau 12-12.** Options du convertisseur 3D pour les pools exécutés sur vSphere 5.1 ou supérieur (suite)

| Option | Description |
|---|---|
| Matériel | Le rendu 3D est activé. L'hôte ESXi réserve des ressources matérielles de processeur graphique sur la base « premier arrivé, premier servi » à mesure que les machines virtuelles sont activées.<br>Ce paramètre est une option lors de la configuration de vSGA.<br>L'hôte ESXi alloue de la VRAM à une machine virtuelle en fonction de la valeur définie dans la boîte de dialogue Configurer VRAM pour des clients 3D.<br>**Important** Si vous configurez l'option **Matériel**, tenez compte des contraintes potentielles suivantes :<br>■ Si un utilisateur tente de se connecter à une machine lorsque toutes les ressources matérielles de processeur graphique sont réservées, la machine virtuelle n'est pas mise sous tension et l'utilisateur reçoit un message d'erreur.<br>■ Si vous utilisez vMotion pour déplacer la machine vers un hôte ESXi sur lequel aucun matériel GPU n'est configuré, la machine virtuelle ne se met pas sous tension.<br>Lorsque vous configurez le rendu 3D basé sur le matériel, vous pouvez examiner les ressources de processeur graphique qui sont allouées à chaque machine virtuelle sur un hôte ESXi. Pour plus d'informations, reportez-vous à « Examen des ressources de processeur graphique sur un hôte ESXi », page 183. |
| NVIDIA GRID vGPU | Le rendu 3D est activé pour NVIDIA GRID vGPU. L'hôte ESXi réserve des ressources matérielles de processeur graphique sur la base « premier arrivé, premier servi » à mesure que les machines virtuelles sont activées. Si un utilisateur tente de se connecter à une machine virtuelle lorsque toutes les ressources matérielles GPU sont utilisées par d'autres machines virtuelles sur l'hôte, le Serveur de connexion View tentera de déplacer la machine virtuelle vers un autre hôte ESXi du cluster avant la mise sous tension.<br>Utilisez ce paramètre lors de la configuration de NVIDIA GRID vGPU.<br>Lorsque vous sélectionnez l'option **NVIDIA GRID vGPU**, les paramètres **Configurer VRAM pour des clients 3D**, **Nombre max. d'écrans** et **Résolution max. d'un écran** sont inactifs dans View Administrator. Lorsque vous configurez la machine virtuelle parente ou un modèle de machine virtuelle avec vSphere Web Client, un message vous invite à réserver toute la mémoire.<br>**Important** Si vous configurez l'option **NVIDIA GRID vGPU**, tenez compte des contraintes potentielles suivantes :<br>■ La machine virtuelle ne peut pas être interrompue ou reprise. Par conséquent, l'option Stratégie d'alimentation de machine distante pour l'interruption de la machine virtuelle n'est pas disponible.<br>■ Si vous utilisez vMotion pour déplacer la machine vers un hôte ESXi sur lequel aucun matériel GPU n'est configuré, la machine virtuelle ne se met pas sous tension. Live vMotion n'est pas disponible.<br>■ Tous les hôtes ESXi du cluster doivent être de version 6.0 ou ultérieure, et les machines virtuelles doivent être de version matérielle 11 ou ultérieure.<br>■ Si un cluster ESXi contient un hôte sur lequel NVIDIA GRID vGPU est activé et un hôte sur lequel NVIDIA GRID vGPU n'est pas activé, les hôtes affichent un état jaune (avertissement) dans le tableau de bord View Administrator. Si un utilisateur tente de se connecter à une machine virtuelle lorsque toutes les ressources matérielles GPU sont utilisées par d'autres machines virtuelles sur l'hôte, le Serveur de connexion View tentera de déplacer la machine virtuelle vers un autre hôte ESXi du cluster avant la mise sous tension. Dans ce cas, les hôtes sur lesquels NVIDIA GRID vGPU n'est pas activé ne peuvent pas être utilisés pour ce type de migration dynamique. |
| Désactivé | Le rendu 3D est inactif. |

**Tableau 12-13.** Options du convertisseur 3D pour les pools exécutés sur vSphere 5.0

| Option | Description |
|---|---|
| Activé | L'option **Convertisseur 3D** est activée. L'hôte ESXi utilise le rendu graphique 3D logiciel.<br>Lorsque le rendu logiciel est configuré, la taille VRAM par défaut est de 64 Mo, la taille minimale. Dans la boîte de dialogue Configurer VRAM pour des clients 3D, vous pouvez utiliser le curseur pour augmenter la quantité de VRAM réservée. Avec le rendu logiciel, l'hôte ESXi alloue jusqu'à 128 Mo maximum par machine virtuelle. Si vous définissez une taille VRAM supérieure, elle est ignorée. |
| Désactivé | Le rendu 3D est inactif. |

Si un pool de postes de travail est exécuté sur une version de vSphere antérieure à 5.0, le paramètre **Convertisseur 3D** est inactif et n'est pas disponible dans View Administrator.

## Meilleures pratiques pour la configuration du rendu 3D

Les options de rendu 3D et d'autres paramètres de pool présentent divers avantages et inconvénients. Sélectionnez l'option la plus adaptée à votre infrastructure matérielle vSphere et aux exigences de vos utilisateurs pour le rendu graphique.

**Remarque** Cette rubrique présente une vue d'ensemble des contrôles disponibles dans View Administrator. Pour plus d'informations sur les différents choix et sur les configurations requises du rendu 3D, reportez-vous au Livre blanc VMware sur l'accélération graphique.

### Quand choisir l'option Automatique

L'option **Automatique** est le meilleur choix pour les déploiements de View qui exigent le rendu 3D. Les machines virtuelles vSGA (Virtual Shared Graphics Acceleration) peuvent basculer de manière dynamique entre le rendu 3D matériel ou logiciel sans reconfiguration. Cette option garantit qu'un certain type de rendu 3D a lieu même lorsque des ressources de processeur graphique sont entièrement réservées. Dans un cluster mélangé d'hôtes ESXi 5.1 et ESXi 5.0, cette option garantit qu'une machine virtuelle est activée correctement et qu'elle utilise le rendu 3D même si, par exemple, vMotion a déplacé la machine virtuelle vers un hôte ESXi 5.0.

Le seul inconvénient de l'option **Automatique** est que vous ne pouvez pas facilement voir si une machine virtuelle utilise le rendu 3D matériel ou logiciel.

### Quand choisir l'option Matériel

L'option **Matériel** garantit que chaque machine virtuelle dans le pool utilise le rendu 3D matériel, à condition que des ressources de processeur graphique soient disponibles sur les hôtes ESXi. Cette option peut représenter le meilleur choix lorsque tous les utilisateurs exécutent des applications gourmandes en ressources graphiques. Vous pouvez choisir cette option lors de la configuration de vSGA (Virtual Shared Graphics Acceleration).

Avec l'option **Matériel**, vous devez contrôler votre environnement vSphere de façon stricte. La version de tous les hôtes ESXi doit être la version 5.1 ou supérieure et des cartes de processeur graphique doivent être installées sur ces hôtes.

Lorsque toutes les ressources de processeur graphique sur un hôte ESXi sont réservées, View ne peut pas activer une machine virtuelle pour l'utilisateur suivant qui tente de se connecter à un poste de travail. Vous devez gérer l'allocation de ressources de processeur graphique et l'utilisation de vMotion afin de garantir que des ressources sont disponibles pour vos postes de travail.

## Quand choisir l'option Gérer à l'aide de vSphere Client

Lorsque vous sélectionnez l'option **Gérer à l'aide de vSphere Client**, vous pouvez utiliser vSphere Web Client pour configurer des machines virtuelles individuelles avec différentes options et valeurs VRAM.

- Pour vSGA (Virtual Shared Graphics Acceleration), vous pouvez prendre en charge une configuration mixte de rendu 3D et de tailles de VRAM pour les machines virtuelles d'un pool.
- Pour vDGA (Virtual Dedicated Graphics Acceleration), chaque machine virtuelle doit être configurée individuellement pour partager un périphérique PCI spécifique avec l'autre ESXi et toute la mémoire doit être réservée. Pour plus d'informations, reportez-vous à la section « Préparation des capacités vDGA », page 179.

  La version de tous les hôtes ESXi doit être la version 5.5 ou supérieure et des cartes de processeur graphique doivent être installées sur ces hôtes.

  **Remarque** Certaines cartes Intel vDGA requièrent une version spécifique de vSphere 6. Consultez la liste de compatibilité matérielle VMware à l'adresse http://www.vmware.com/resources/compatibility/search.php. De plus, pour Intel vDGA, le GPU intégré Intel est utilisé à la place de GPU discrets, comme c'est le cas avec d'autres fournisseurs.

- Pour GPU multi-utilisateur AMD utilisant vDGA, chaque machine virtuelle doit être configurée individuellement pour partager un périphérique PCI spécifique avec l'hôte ESXi et toute la mémoire doit être réservée. Cette fonctionnalité permet à un périphérique PCI d'apparaître sous la forme de plusieurs périphériques PCI physiques séparés afin que le GPU puisse être partagé entre 2 à 15 utilisateurs. Pour plus d'informations, reportez-vous à la section « Préparation de l'utilisation des capacités du GPU multi-utilisateur AMD utilisant vDGA », page 181.

  La version de tous les hôtes ESXi doit être la version 6.0 ou supérieure et des cartes de processeur graphique doivent être installées sur ces hôtes.

Vous pouvez également choisir cette option si vous souhaitez gérer explicitement les paramètres graphiques de clones et de clones liés en faisant en sorte que les clones héritent des paramètres de la machine virtuelle parente.

## Quand choisir l'option NVIDIA GRID vGPU

Lorsque l'option **NVIDIA GRID vGPU** est activée sur un hôte ESXi, vous pouvez obtenir un ratio de consolidation de machines virtuelles plus élevé que celui possible lors de l'utilisation de vDGA, tout en maintenant le même niveau de performance. Comme avec vDGA (Dedicated Virtual Graphics), l'hôte ESXi et la machine virtuelle utilisent également le relais GPU pour NVIDIA GRID vGPU.

**Remarque** Pour améliorer les ratios de consolidation de la machine virtuelle, vous pouvez définir l'hôte ESXi afin d'utiliser le mode de consolidation. Modifiez le fichier `/etc/vmware/config` sur l'hôte ESXi et ajoutez l'entrée suivante :

```
vGPU.consolidation = "true"
```

Par défaut, l'hôte ESXi attribue des machines virtuelles au GPU physique contenant le moins de machines virtuelles déjà attribuées. Il s'agit du mode de performances. Si vous préférez que l'hôte ESXi attribue des machines virtuelles au même GPU physique jusqu'à atteindre le nombre maximal de machines virtuelles avant de placer des machines virtuelles sur le prochain GPU physique, vous pouvez utiliser le mode de consolidation.

Comme une ressource GPU ne doit pas nécessairement être dédiée à une machine virtuelle spécifique, vous pouvez créer et configurer une machine virtuelle parente ou un modèle de machine virtuelle en activant l'option **NVIDIA GRID vGPU**, puis créer un pool de postes de travail de machines virtuelles pouvant partager la même ressource GPU physique.

Si toutes les ressources GPU sur un hôte ESXi sont utilisées par d'autres machines virtuelles, lorsque l'utilisateur suivant tente de se connecter à un poste de travail, View peut déplacer la machine virtuelle vers un autre serveur ESXi du cluster sur lequel l'option NVIDIA GRID vGPU est activée, puis mettre sous tension la machine virtuelle. La version de tous les hôtes ESXi doit être la version 6.0 ou supérieure et des cartes de processeur graphique doivent être installées sur ces hôtes.

Pour plus d'informations, reportez-vous à la section « Préparation pour les capacités de NVIDIA GRID vGPU », page 180.

### Quand choisir l'option Logiciel

Sélectionnez l'option **Logiciel** si vous disposez uniquement d'hôtes ESXi 5.0, si les hôtes ESXi 5.1 ou version ultérieure ne disposent pas de carte de processeur graphique ou si vos utilisateurs exécutent uniquement des applications, telles qu'AERO et Microsoft Office, qui ne nécessitent pas l'accélération graphique matérielle.

### Configuration de paramètres de poste de travail pour gérer des ressources de processeur graphique

Vous pouvez configurer d'autres paramètres de poste de travail pour garantir que les ressources de processeur graphique ne sont pas gaspillées lorsque les utilisateurs ne les utilisent pas activement.

Pour les pools flottants, définissez un délai d'expiration de session pour que les ressources de processeur graphique soient libérées pour les autres utilisateurs lorsqu'un utilisateur n'utilise pas le poste de travail.

Pour les pools dédiés, vous pouvez configurer le paramètre **Fermeture de session automatique après la déconnexion** sur **Immédiatement** et une règle d'alimentation **Interrompre** si ces paramètres sont appropriés pour vos utilisateurs. Par exemple, n'utilisez pas ces paramètres pour un groupe de chercheurs qui exécutent de longues simulations. Notez que la stratégie d'alimentation **Interrompre** n'est pas disponible si vous utilisez l'option **NVIDIA GRID vGPU**.

## Préparation des capacités vDGA

vDGA (Virtual Dedicated Graphics Acceleration) fournit un relais direct vers un GPU physique, ce qui offre aux utilisateurs un accès dédié sans limite à un seul vGPU. Avant de pouvoir créer un pool de postes de travail avec des capacités vDGA, vous devez effectuer certaines tâches de configuration sur les machines virtuelles et les hôtes ESXi.

Cette présentation décrit les tâches que vous devez effectuer dans vSphere avant de pouvoir créer ou configurer des pools de postes de travail dans View Administrator. Pour obtenir des informations complètes et des procédures détaillées, reportez-vous au Livre blanc VMware sur l'accélération graphique.

---

**Remarque** Certaines cartes Intel vDGA requièrent une version spécifique de vSphere 6. Consultez la liste de compatibilité matérielle VMware à l'adresse http://www.vmware.com/resources/compatibility/search.php. De plus, pour Intel vDGA, le GPU intégré Intel est utilisé à la place de GPU discrets, comme c'est le cas avec d'autres fournisseurs.

---

1. Installez la carte graphique sur l'hôte ESXi.
2. Installez VIB (vSphere Installation Bundle) de GPU.
3. Vérifiez que VT-d ou AMD IOMMU est activé sur l'hôte ESXi.
4. Ajoutez un périphérique PCI à la machine virtuelle et sélectionnez le périphérique PCI approprié pour activer le relais GPU sur la machine virtuelle.
5. Réservez toute la mémoire lors de la création de la machine virtuelle.
6. Configurez les capacités 3D de la carte vidéo de la machine virtuelle.

7 Obtenez les pilotes GPU du fournisseur de la GPU, puis installez les pilotes du périphérique GPU dans le système d'exploitation invité de la machine virtuelle.

8 Installez VMware Tools et Horizon Agent dans le système d'exploitation invité et redémarrez.

Dès que vous avez effectué ces tâches, vous devez ajouter la machine virtuelle à un pool de postes de travail manuel afin de pouvoir accéder au système d'exploitation invité à l'aide de PCoIP ou VMware Blast Extreme. Dans une session PCoIP ou VMware Blast, vous pouvez ensuite activer la carte vidéo NVIDIA, AMD ou Intel dans le système d'exploitation invité.

## Préparation pour les capacités de NVIDIA GRID vGPU

NVIDIA GRID vGPU fournit un accès direct au GPU physique sur un hôte ESXi, donc plusieurs utilisateurs peuvent partager un seul GPU, à l'aide de pilotes de carte graphique natifs. Avant de pouvoir créer un pool de postes de travail avec des capacités de NVIDIA GRID vGPU, vous devez effectuer certaines tâches de configuration sur les machines virtuelles et les hôtes ESXi.

Cette présentation décrit les tâches que vous devez effectuer dans vSphere avant de pouvoir créer ou configurer des pools de postes de travail dans View Administrator. Pour obtenir des informations complètes et des procédures détaillées, consultez le Guide de déploiement de NVIDIA GRID vGPU pour VMware Horizon 6.1.

1 Installez la carte graphique sur l'hôte ESXi.

2 Installez VIB (vSphere Installation Bundle) de GPU.

3 Vérifiez que VT-d ou AMD IOMMU est activé sur l'hôte ESXi.

4 Activez le relais de périphérique GPU sur l'hôte ESXi.

5 Ajoutez un périphérique PCI partagé à la machine virtuelle et sélectionnez le périphérique PCI approprié pour activer le relais GPU sur la machine virtuelle.

   Lorsque vous ajoutez un périphérique PCI, vous voyez une liste de tous les types de profils graphiques pris en charge disponibles sur la carte GPU de l'hôte ESXi.

6 Réservez toute la mémoire lors de la création de la machine virtuelle.

7 Configurez les capacités 3D de la carte vidéo de la machine virtuelle.

8 Obtenez les pilotes GPU du fournisseur de la GPU, puis installez les pilotes du périphérique GPU dans le système d'exploitation invité de la machine virtuelle.

9 Installez VMware Tools et Horizon Agent dans le système d'exploitation invité et redémarrez.

Dès que vous avez effectué ces tâches, vous devez ajouter la machine virtuelle à un pool de postes de travail View manuel afin de pouvoir accéder au système d'exploitation invité à l'aide de PCoIP. Dans une session PCoIP, vous pouvez ensuite activer la carte vidéo NVIDIA dans le système d'exploitation invité.

À ce stade, vous pouvez configurer la machine virtuelle comme un modèle ou prendre un snapshot de la machine virtuelle à utiliser comme image de base dans un pool de clone lié View Composer. (Vous devez mettre la machine virtuelle hors tension avant de prendre le snapshot.) Lorsque vous utilisez l'assistant Ajouter un pool de postes de travail, après la sélection de l'option **NVIDIA GRID vGPU** pour **Convertisseur 3D**, seuls les hôtes ESXi et les modèles de machines virtuelles sur lesquels NVIDIA GRID vGPU est activé ainsi que les snapshots s'affichent pour sélection dans l'assistant.

## Préparation de l'utilisation des capacités du GPU multi-utilisateur AMD utilisant vDGA

Le GPU multi-utilisateur AMD utilisant vDGA fournit un relais direct vers un GPU physique, ce qui offre aux utilisateurs un accès dédié sans limite à un seul GPU. Avant de pouvoir créer un pool de postes de travail avec des capacités pour utiliser le GPU multi-utilisateur AMD utilisant vDGA, vous devez effectuer certaines tâches de configuration sur les machines virtuelles et les hôtes ESXi.

Cette présentation décrit les tâches que vous devez effectuer dans vSphere avant de pouvoir créer ou configurer des pools de postes de travail dans View Administrator. Pour plus d'informations sur l'activation du relais de périphérique GPU et sur l'ajout d'un périphérique PCI à une machine virtuelle, consultez le Livre blanc VMware sur l'accélération graphique.

1. Installez la carte graphique sur l'hôte ESXi.
2. Installez VIB (vSphere Installation Bundle) de GPU.
3. Vérifiez que VT-d ou AMD IOMMU est activé sur l'hôte ESXi.
4. Utilisez la commande `esxcfg-module` pour configurer la carte graphique pour SR-IOV (virtualisation d'E/S d'une racine unique).

   Reportez-vous à la section « Configuration d'un GPU multi-utilisateur AMD utilisant vDGA », page 181.
5. Redémarrez l'hôte ESXi.
6. Ajoutez un périphérique PCI à la machine virtuelle et sélectionnez le périphérique PCI approprié pour activer le relais GPU sur la machine virtuelle.
7. Réservez toute la mémoire lors de la création de la machine virtuelle.
8. Configurez les capacités 3D de la carte vidéo de la machine virtuelle.
9. Obtenez les pilotes GPU du fournisseur de la GPU, puis installez les pilotes du périphérique GPU dans le système d'exploitation invité de la machine virtuelle.
10. Installez VMware Tools et Horizon Agent dans le système d'exploitation invité et redémarrez.

Dès que vous avez effectué ces tâches, vous devez ajouter la machine virtuelle à un pool de postes de travail manuel afin de pouvoir accéder au système d'exploitation invité à l'aide de PCoIP ou VMware Blast Extreme. Si vous tentez d'accéder à la machine virtuelle à l'aide de vSphere, un écran noir s'affichera.

## Configuration d'un GPU multi-utilisateur AMD utilisant vDGA

Vous utilisez la commande de ligne de commande `esxcfg-module` pour configurer des paramètres tels que le nombre d'utilisateurs pouvant partager le GPU, la quantité de tampon de trame allouée à chaque utilisateur et des contrôles de performances.

### Syntaxe

```
esxcfg-module -s "adapter1_conf=bus#,device#,function#,number_of_VFs,FB_size,time_slice,mode"
amdgpuv
```

### Notes d'utilisation

La commande `vicfg-module` prend en charge la définition et la récupération des options de module VMkernel sur un hôte ESXi. Pour des informations de référence générales sur cette commande, visitez la page http://pubs.vmware.com/vsphere-60/topic/com.vmware.vcli.ref.doc/vicfg-module.html.

## Indicateurs requis

Vous devez spécifier plusieurs indicateurs lors de la configuration du GPU multi-utilisateur AMD utilisant vDGA. Si la commande n'inclut pas tous les indicateurs requis, aucun message d'erreur n'apparaît, mais la configuration devient par défaut une simple configuration à 4 périphériques SR-IOV.

**Tableau 12-14.** Indicateurs pour la configuration de SR-IOV AMD

| Indicateur | Description |
|---|---|
| *bus#* | Numéro de bus au format décimal. |
| *device#* | ID du périphérique PCIe pour la carte AMD prise en charge, au format décimal. Pour voir une liste, utilisez la commande `lspci \| grep -i display`.<br>Par exemple, pour un système avec deux cartes GPU AMD, vous pouvez voir la sortie suivante lorsque vous exécutez cette commande :<br>`[root@host:~] lspci \| grep -i display`<br>`0000:04:00.0 Display controller:`<br>`0000:82:00.0 Display controller:`<br>Dans cet exemple, les ID de périphérique PCIe sont 04 et 82. Notez que ces ID sont répertoriés au format hexadécimal et qu'ils doivent être convertis au format décimal pour être utilisés dans la commande `vicfg-module`.<br>Les cartes S7150 AMD ne prennent en charge qu'un seul GPU par carte. L'ID de périphérique et l'ID de fonction sont donc 0 pour ces cartes. |
| *function#* | Numéro de fonction au format décimal. |
| *number_of_VFs* | Nombre de VF (fonctions virtuelles), de 2 à 15. Ce nombre représente le nombre d'utilisateurs qui partageront le GPU. |
| *FB_size* | Quantité de mémoire tampon de trame, en Mo, allouée à chaque VF. Pour déterminer la taille, prenez la quantité totale de mémoire vidéo sur la carte et divisez cette quantité par le nombre de VF. Arrondissez ce nombre au nombre le plus proche qui est un multiple de 8. Par exemple, pour une carte S7150 AMD, qui contient 8 000 Mo, vous pourriez utiliser les paramètres suivants :<br>■ Pour 2 VF, utilisez 4 096.<br>■ Pour 4 VF, utilisez 2 048.<br>■ Pour 8 VF, utilisez 1 024.<br>■ Pour 15 VF, utilisez 544. |
| *time_slice* | Intervalle entre les commutateurs de VF, en microsecondes. Ce paramètre ajuste le retard de la mise en file d'attente et du traitement des commandes entre les périphériques SR-IOV. Utilisez une valeur comprise entre 3 000 et 40 000. Ajustez cette valeur si vous voyez une interruption importante lorsque plusieurs périphériques SR-IOV sont actifs. |
| *mode* | Voici les valeurs valides : 0 = performances récupérées ; 1 = performances en pourcentage fixe. |

**Important** Après avoir exécuté la commande `esxcfg-module`, vous devez redémarrer l'hôte ESXi pour que les paramètres prennent effet.

## Exemples

1 Pour une seule carte S7150 AMD sur PCI ID 4 partagée par 8 utilisateurs :

```
esxcfg-module -s "adapter1_conf=4,0,0,8,1024,4000" amdgpuv
```

2 Pour un seul serveur avec deux cartes S7150 AMD sur PCI ID 4 et PCI ID 82 partagées par 4 utilisateurs expérimentés :

```
esxcfg-module -s "adapter1_conf=3,0,0,2,4096,4000 adapter2_conf=130,0,0,2,4096,4000" amdgpuv
```

3 Pour un seul serveur avec deux cartes S7150 AMD, vous pouvez régler chaque carte avec différents paramètres. Par exemple, si votre environnement View doit prendre en charge 2 utilisateurs expérimentés et 16 exécutants de tâches :

```
esxcfg-module -s "adapter1_conf=3,0,0,2,4096,4000 adapter2_conf=130,0,0,15,544,7000" amdgpuv
```

4 Activez l'option SR-IOV sur l'hôte ESXi.

Certains hôtes disposent de SR-IOV sous la forme d'une option configurable dans le BIOS.

### Examen des ressources de processeur graphique sur un hôte ESXi

Pour mieux gérer les ressources de processeur graphique disponibles sur un hôte ESXi, vous pouvez examiner la réservation de ressources de processeur graphique actuelle. L'utilitaire de requête de ligne de commande ESXi, `gpuvm`, répertorie les processeurs graphiques installés sur un hôte ESXi et affiche la quantité de mémoire de processeur graphique réservée pour chaque machine virtuelle sur l'hôte. Notez que cette réservation de mémoire de processeur graphique n'est pas la même que la taille VRAM de machine virtuelle.

Pour exécuter l'utilitaire, tapez **`gpuvm`** dans une invite du shell sur l'hôte ESXi. Vous pouvez utiliser une console sur l'hôte ou une connexion SSH.

Par exemple, l'utilitaire peut afficher la sortie suivante :

```
~ # gpuvm
Xserver unix:0, GPU maximum memory 2076672KB
        pid 118561, VM "JB-w7-64-FC3", reserved 131072KB of GPU memory.
        pid 64408, VM "JB-w7-64-FC5", reserved 261120KB of GPU memory.
        GPU memory left 1684480KB.
```

De même, vous pouvez utiliser la commande `nvidia-smi` sur l'hôte ESXi pour voir la liste de machines virtuelles sur lesquelles NVIDIA GRID vGPU est activé, la quantité de mémoire tampon de trame consommée et l'ID d'emplacement de la GPU physique utilisée par la machine virtuelle.

## Empêcher l'accès à des postes de travail View via RDP

Dans certains environnements View, interdire l'accès à des postes de travail View via le protocole d'affichage RDP est une priorité. Vous pouvez empêcher des utilisateurs et des administrateurs d'utiliser RDP pour accéder à des postes de travail View en configurant des paramètres de pool et un paramètre de stratégie de groupe.

Par défaut, lorsqu'un utilisateur a ouvert une session de poste de travail View, vous pouvez utiliser RDP pour vous connecter à la machine virtuelle à l'extérieur de View. La connexion RDP met fin à la session du poste de travail View et les données et paramètres non enregistrés de l'utilisateur View risquent d'être perdus. L'utilisateur View ne peut pas se connecter au poste de travail tant que la connexion RDP externe est fermée. Pour éviter cette situation, désactivez le paramètre `AllowDirectRDP`.

---

**Remarque** Les services Bureau à distance doivent être démarrés sur la machine virtuelle que vous utilisez pour créer des pools et sur les machines virtuelles qui sont déployées dans les pools. Les services Bureau à distance sont requis pour l'installation d'Horizon Agent, l'authentification unique et d'autres opérations de gestion de session de View.

---

#### Prérequis

Vérifiez que le fichier de modèle d'administration (ADM) de configuration d'Horizon Agent est installé dans Active Directory. Reportez-vous à la section « Utilisation des fichiers de modèle d'administration de stratégie de groupe View », page 306.

### Procédure

1 Sélectionnez PCoIP comme protocole d'affichage que vous souhaitez que le Serveur de connexion View utilise pour communiquer avec des périphériques Horizon Client.

| Option | Description |
|---|---|
| **Créer un pool de postes de travail** | a Dans View Administrator, démarrez l'assistant Ajouter un pool de postes de travail.<br>b Dans la page Paramètres du pool de postes de travail, sélectionnez **VMware Blast** ou **PCoIP** comme protocole d'affichage par défaut. |
| **Modifier un pool de postes de travail existant** | a Dans View Administrator, sélectionnez le pool de postes de travail et cliquez sur **Modifier**.<br>b Dans l'onglet **Paramètres du pool de postes de travail**, sélectionnez **VMware Blast** ou **PCoIP** comme protocole d'affichage par défaut. |

2 Pour le paramètre **Autoriser les utilisateurs à choisir un protocole**, sélectionnez **Non**.

3 Empêcher les périphériques qui n'exécutent pas Horizon Client de se connecter directement à des postes de travail View via RDP en désactivant le paramètre de stratégie de groupe `AllowDirectRDP`.

   a Sur votre serveur Active Directory, ouvrez la Console de gestion des stratégies de groupe et sélectionnez **Configuration ordinateur > Stratégies > Modèles d'administration > Modèles d'administration classiques (ADM) > Configuration de VMware Horizon Agent**.

   b Désactivez le paramètre `AllowDirectRDP`.

# Déploiement de pools de postes de travail volumineux

Lorsque de nombreux utilisateurs requièrent la même image de poste de travail, vous pouvez créer un pool automatisé volumineux à partir d'un modèle ou d'une machine virtuelle parente. L'utilisation d'une image de base et d'un nom de pool uniques vous permet d'éviter d'avoir à diviser les machines de manière arbitraire en plus petits groupes devant être gérés séparément Cette stratégie simplifie vos tâches de déploiement et d'administration.

Pour prendre en charge des pools volumineux, vous pouvez créer des pools sur des clusters ESXi contenant jusqu'à 32 hôtes ESXi. Vous pouvez également configurer un pool afin qu'il utilise plusieurs étiquettes réseau, en rendant les adresses IP de plusieurs groupes de ports disponibles pour les machines virtuelles du pool.

**Remarque** La fonctionnalité d'étiquettes de réseau multiples n'est pas disponible pour les clones instantanés.

## Configuration de pools de postes de travail sur des clusters comportant plus de huit hôtes

Dans vSphere 5.1 et supérieur, vous pouvez déployer un pool de postes de travail de clone lié sur un cluster contenant jusqu'à 32 hôtes ESXi. La version de tous les hôtes ESXi dans le cluster doit être la version 5.1 ou supérieure. Les hôtes peuvent utiliser des magasins de données VMFS ou NFS. La version des magasins de données VMFS doit être VMFS5 ou supérieur.

Dans vSphere 5.0, vous pouvez déployer des clones liés sur un cluster contenant plus de huit hôtes ESXi, mais vous devez stocker les disques de réplica sur des magasins de données NFS. Vous pouvez stocker des disques de réplica sur des magasins de données VMFS uniquement avec des clusters qui contiennent huit hôtes ou moins.

Dans vSphere 5.0, les règles suivantes s'appliquent lorsque vous configurez un pool de clone lié sur un cluster contenant plus de huit hôtes :

- Si vous stockez des disques de réplica sur les mêmes magasins de données que les disques du système d'exploitation, vous devez stocker les disques de réplica et du système d'exploitation sur des magasins de données NFS.
- Si vous stockez des disques de réplica sur des magasins de données séparés des disques du système d'exploitation, les disques de réplica doivent être stockés sur des magasins de données NFS. Les disques du système d'exploitation peuvent être stockés sur des magasins de données NFS ou VMFS.
- Si vous stockez des disques persistants de View Composer sur des magasins de données séparés, les disques persistants peuvent être configurés sur des magasins de données NFS ou VMFS.

Dans vSphere 4.1 et versions antérieures, vous pouvez déployer des pools de postes de travail uniquement avec des clusters contenant huit hôtes ou moins.

## Affectation de plusieurs étiquettes de réseau à un pool de postes de travail

Dans View 5.2 et version ultérieure, vous pouvez configurer un pool de postes de travail automatisé pour utiliser plusieurs étiquettes réseau. Vous pouvez affecter plusieurs étiquettes de réseau à un pool de clone lié ou un pool automatisé contenant des machines virtuelles complètes.

---

**Remarque** La fonctionnalité d'étiquettes de réseau multiples n'est pas disponible pour les clones instantanés.

---

Dans les versions précédentes, les machines virtuelles dans le pool héritaient des étiquettes de réseau qui étaient utilisées par les cartes réseau sur la machine virtuelle parente ou le modèle. Une machine virtuelle parente ou un modèle classique contient une carte réseau et une étiquette de réseau. Une étiquette de réseau définit un groupe de ports et un VLAN. En général, le masque de réseau d'un VLAN fournit une plage limitée d'adresses IP disponibles.

Dans View 5.2 et versions supérieures, vous pouvez affecter des étiquettes de réseau disponibles dans vCenter Server pour tous les hôtes ESXi dans le cluster sur lequel le pool de postes de travail est déployé. En configurant plusieurs étiquettes de réseau pour le pool, vous augmentez considérablement le nombre d'adresses IP pouvant être affectées aux machines virtuelles dans le pool.

Vous devez utiliser des cmdlets View PowerCLI pour affecter plusieurs étiquettes de réseau à un pool. Vous ne pouvez pas effectuer cette tâche dans View Administrator.

Pour plus d'informations sur l'utilisation de View PowerCLI pour effectuer cette tâche, consultez la section « Attribuer plusieurs étiquettes réseau à un pool de postes de travail » dans le chapitre « Utilisation de View PowerCLI » du document *Intégration de View*.

# Autorisation d'utilisateurs et de groupes 13

Vous pouvez configurer des droits d'accès pour contrôler les applications et les postes de travail distants auxquels vos utilisateurs ont accès. Vous pouvez également configurer la fonctionnalité de droits d'accès limités pour contrôler l'accès aux postes de travail en fonction de l'instance du Serveur de connexion View à laquelle les utilisateurs se connectent lorsqu'ils sélectionnent des postes de travail distants.

Dans un environnement Cloud Pod Architecture, vous créez des droits d'accès globaux pour autoriser les utilisateurs ou les groupes à utiliser plusieurs postes de travail dans plusieurs espaces d'une fédération d'espaces. Lorsque vous utilisez des droits d'accès globaux, vous n'avez pas besoin de configurer ni de gérer les droits d'accès locaux aux postes de travail distants. Pour plus d'informations sur des droits d'accès globaux et la configuration d'un environnement Cloud Pod Architecture, reportez-vous au document *Administering View Cloud Pod Architecture*.

Ce chapitre aborde les rubriques suivantes :



## Ajouter des droits d'accès à un pool de postes de travail ou d'applications

Avant que les utilisateurs puissent accéder à des applications ou des postes de travail distants, ils doivent être autorisés à utiliser un pool de postes de travail ou d'applications.

### Prérequis

Créez un pool de postes de travail ou d'applications.

### Procédure

1 Sélectionnez le pool de postes de travail ou d'applications.

| Option | Action |
|---|---|
| **Ajouter un droit d'accès à un pool de postes de travail** | Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail** et cliquez sur le nom du pool de postes de travail. |
| **Ajouter un droit d'accès à un pool d'applications** | Dans View Administrator, sélectionnez **Catalogue > Pools d'applications** et cliquez sur le nom du pool d'applications. |

2 Sélectionnez **Ajouter un droit** dans le menu déroulant **Autorisations**.

3 Cliquez sur **Ajouter**, sélectionnez un ou plusieurs critères de recherche, puis cliquez sur **Rechercher** pour rechercher des utilisateurs ou des groupes en fonction de vos critères de recherche.

**Remarque** Les groupes locaux de domaine sont filtrés dans les résultats de recherche pour des domaines en mode mixte. Vous ne pouvez pas autoriser des utilisateurs dans des groupes locaux de domaine si votre domaine est configuré en mode mixte.

4 Sélectionnez les utilisateurs ou les groupes auxquels vous souhaitez autoriser l'accès aux postes de travail ou aux applications du pool et cliquez sur **OK**.

5 Cliquez sur **OK** pour enregistrer vos modifications.

## Supprimer les droits d'accès d'un pool de postes de travail ou d'applications

Vous pouvez supprimer les droits d'accès d'un pool de postes de travail ou d'applications pour empêcher des utilisateurs ou des groupes spécifiques d'accéder à un poste de travail ou à une application.

### Procédure

1 Sélectionnez le pool de postes de travail ou d'applications.

| Option | Description |
|---|---|
| **Supprimer un droit d'accès à un pool de postes de travail** | Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail** et cliquez sur le nom du pool de postes de travail. |
| **Supprimer un droit d'accès d'un pool d'applications** | Dans View Administrator, sélectionnez **Catalogue > Pools d'applications** et cliquez sur le nom du pool d'applications. |

2 Sélectionnez **Supprimer une autorisation** dans le menu déroulant **Autorisations**.

3 Sélectionnez l'utilisateur ou le groupe pour lequel vous souhaitez supprimer l'autorisation et cliquez sur **Supprimer**.

4 Cliquez sur **OK** pour enregistrer vos modifications.

## Vérifier les droits d'accès de pools de postes de travail ou d'applications

Vous pouvez vérifier les pools de postes de travail ou d'applications auxquels un utilisateur ou un groupe est autorisé à accéder.

### Procédure

1 Dans View Administrator, sélectionnez **Utilisateurs et groupes** et cliquez sur le nom de l'utilisateur ou du groupe.

2 Cliquez sur l'onglet **Autorisations** et vérifiez les pools de postes de travail ou d'applications auxquels un utilisateur ou un groupe est autorisé à accéder.

| Option | Action |
|---|---|
| **Lister les pools de postes de travail auxquels un utilisateur ou un groupe est autorisé à accéder** | Cliquez sur **Pool de postes de travail**. |
| **Lister les pools d'applications auxquels un utilisateur ou un groupe est autorisé à accéder** | Cliquez sur **Pools d'applications**. |

# Restriction de l'accès aux postes de travail distants

Vous pouvez configurer la fonctionnalité de droits d'accès limités pour limiter l'accès aux postes de travail distants en fonction de l'instance du Serveur de connexion View à laquelle les utilisateurs se connectent lorsqu'ils sélectionnent des postes de travail.

Avec des autorisations limitées, vous affectez une ou plusieurs balises à une instance du Serveur de connexion View. Ensuite, lorsque vous configurez un pool de postes de travail, vous sélectionnez les balises des instances du Serveur de connexion View que vous voulez rendre capables d'accéder au pool de postes de travail.

Lorsque les utilisateurs ouvrent une session via une instance marquée du Serveur de connexion View, ils ne peuvent accéder qu'à ces pools de postes de travail qui ont au moins une balise correspondante ou qui n'ont aucune balise.

---

**Remarque** Vous ne pouvez pas configurer la fonctionnalité de droits d'accèss limités pour limiter l'accès à des applications distantes.

---



## Exemple d'autorisation limitée

Cet exemple montre un déploiement de View comportant deux instances du Serveur de connexion View. La première instance prend en charge les utilisateurs internes. La deuxième instance est couplée avec un serveur de sécurité et prend en charge les utilisateurs externes.

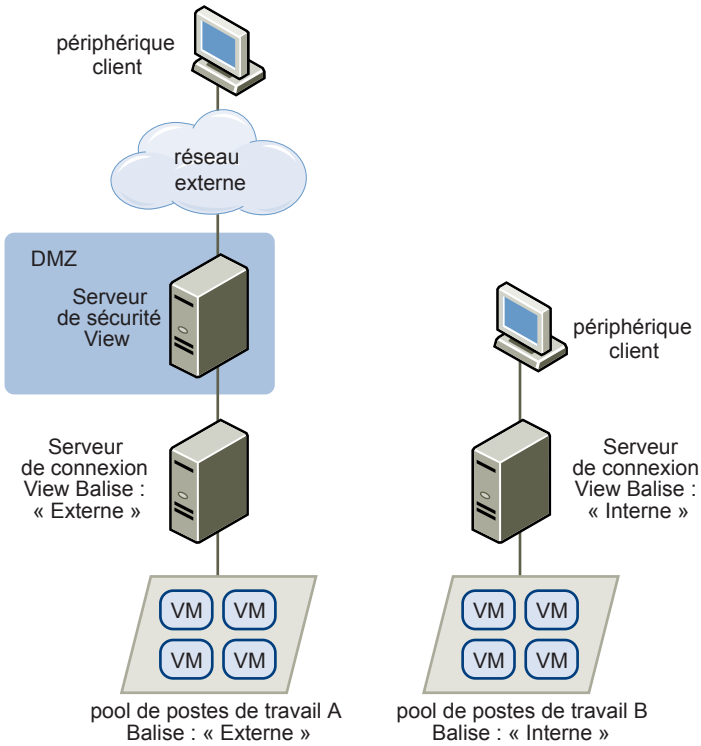
Pour empêcher les utilisateurs externes d'accéder à certains postes de travail, vous pouvez configurer des autorisations limitées comme suit :

- Affectez la balise « Internal » à l'instance du Serveur de connexion View qui prend en charge les utilisateurs internes.
- Affectez la balise « External » à l'instance du Serveur de connexion View qui est couplée avec le serveur de sécurité et qui prend en charge les utilisateurs externes.
- Affectez la balise « Internal » aux pools de postes de travail auxquels ne doivent accéder que les utilisateurs internes.

- Affectez la balise « External » aux pools de postes de travail auxquels ne doivent accéder que les utilisateurs externes.

Les utilisateurs externes ne peuvent pas voir les pools de postes de travail marqués comme « Internal » car ils ouvrent une session via le Serveur de connexion View marqué comme « External ». Les utilisateurs internes ne peuvent pas voir les pools de postes de travail marqués comme « External » car ils ouvrent une session via le Serveur de connexion View marqué comme « Internal ». Figure 13-1 illustre cette configuration.

**Figure 13-1.** Configuration d'une autorisation limitée




Vous pouvez également utiliser des autorisations limitées pour contrôler l'accès à des postes de travail en fonction de la méthode d'authentification utilisateur que vous configurez pour une instance du Serveur de connexion View particulière. Par exemple, vous pouvez rendre certains pools de postes de travail disponibles pour des utilisateurs qui se sont authentifiés avec une carte à puce.

## Correspondance de balise

La fonction d'autorisations limitées utilise la correspondance de balise pour déterminer si une instance du Serveur de connexion View peut accéder à un pool de postes de travail particulier.

Au niveau le plus basique, la correspondance de balise détermine qu'une instance du Serveur de connexion View avec une balise spécifique peut accéder à un pool de postes de travail qui a la même balise.

L'absence d'affectation de balise peut également affecter si une instance du Serveur de connexion View peut accéder à un pool de postes de travail. Par exemple, des instances du Serveur de connexion View qui ne contiennent aucune balise ne peuvent accéder qu'à des pools de postes de travail qui ne contiennent aucune balise.

Tableau 13-1 montre comment la fonction d'autorisations limitées détermine quand un Serveur de connexion View peut accéder à un pool de postes de travail.

**Tableau 13-1.** Règles de correspondance de balise

| Serveur de connexion View | Pool de postes de travail | Accès autorisé ? |
|---|---|---|
| Pas de balise | Pas de balise | Oui |
| Pas de balise | Une ou plusieurs balises | Non |
| Une ou plusieurs balises | Pas de balise | Oui |
| Une ou plusieurs balises | Une ou plusieurs balises | Uniquement quand les balises correspondent |

La fonction d'autorisations limitées ne fait qu'appliquer la correspondance de balise. Vous devez concevoir votre topologie de réseau pour forcer certains clients à se connecter via une instance du Serveur de connexion View particulière.

## Considérations et limites des autorisations limitées

Avant d'implémenter des autorisations limitées, vous devez connaître certaines considérations et limites.

- Une instance du Serveur de connexion View ou un pool de postes de travail peut contenir plusieurs balises.
- Plusieurs instances du Serveur de connexion View et pools de postes de travail peuvent avoir la même balise.
- Des pools de postes de travail qui ne contiennent aucune balise peuvent être accédés par n'importe quelle instance du Serveur de connexion View.
- Des instances du Serveur de connexion View qui ne contiennent aucune balise ne peuvent accéder qu'à des pools de postes de travail qui ne contiennent aucune balise.
- Si vous utilisez un serveur de sécurité, vous devez configurer des autorisations limitées sur l'instance du Serveur de connexion View à laquelle le serveur de sécurité est couplé. Vous ne pouvez pas configurer des autorisations limitées sur un serveur de sécurité.
- Vous ne pouvez pas modifier ou supprimer une balise d'une instance du Serveur de connexion View si cette balise est toujours affectée à un pool de postes de travail et qu'aucune autre instance n'a de balise correspondante.
- Les droits droit d'accès limités sont prioritaires par rapport aux autres droits d'accès ou attributions de poste de travail. Par exemple, même si un utilisateur se voit attribuer une machine particulière, il ne pourra pas accéder à celle-ci si la balise du pool de postes de travail ne correspond pas à celle attribuée à l'instance du Serveur de connexion View à laquelle l'utilisateur est connecté.
- Si vous prévoyez de fournir un accès à vos postes de travail via VMware Identity Manager et si vous configurez des limitations du Serveur de connexion View, il est possible que l'application VMware Identity Manager affiche les postes de travail aux utilisateurs alors que ces postes de travail sont en réalité limités. Lorsqu'un utilisateur VMware Identity Manager tente d'ouvrir une session sur un poste de travail, celui-ci ne se lance pas si la balise du pool de postes de travail ne correspond pas à celle attribuée à l'instance du Serveur de connexion View à laquelle l'utilisateur est connecté.

## Affecter une balise à une instance du Serveur de connexion View

Lorsque vous affectez une balise à une instance du Serveur de connexion View, les utilisateurs qui se connectent à ce serveur Serveur de connexion View ne peuvent accéder qu'aux pools de postes de travail qui ont une balise correspondante ou aucune balise.

### Procédure

1 Dans View Administrator, sélectionnez **Configuration de View > Serveurs**.

2 Dans l'onglet **Serveurs de connexion**, sélectionnez une instance du Serveur de connexion View et cliquez sur **Modifier**.

3 Saisissez une ou plusieurs balises dans le champ **Balises**.

   Séparez les balises avec une virgule ou un point-virgule.

4 Cliquez sur **OK** pour enregistrer vos modifications.

### Suivant

Affectez la balise à des pools de postes de travail.

## Affecter une balise à un pool de postes de travail

Lorsque vous affectez une balise à un pool de postes de travail, seuls les utilisateurs qui se connectent à une instance du Serveur de connexion View ayant une balise correspondante peuvent accéder aux postes de travail de ce pool.

Vous pouvez affecter une balise quand vous ajoutez ou modifiez un pool de postes de travail.

### Prérequis

Affectez des balises à une ou plusieurs instances du Serveur de connexion View.

### Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

2 Sélectionnez le pool auquel vous souhaitez affecter une balise.

| Option | Action |
|---|---|
| **Affecter une balise à un nouveau pool** | Cliquez sur **Ajouter** pour démarrer l'assistant Ajouter un pool de postes de travail, puis définissez et identifiez le pool. |
| **Affecter une balise à un pool existant** | Sélectionnez le pool et cliquez sur **Modifier**. |

3 Allez à la page Paramètres de pool de postes de travail.

| Option | Action |
|---|---|
| **Paramètres de pool pour un nouveau pool** | Cliquez sur **Paramètres du pool de postes de travail** dans l'assistant Ajouter un pool de postes de travail. |
| **Paramètres de pool pour un pool existant** | Cliquez dans l'onglet **Paramètres du pool de postes de travail**. |

4 Cliquez sur **Parcourir** à côté de **Restrictions du serveur de connexion** et configurez les instances du Serveur de connexion View pouvant accéder au pool de postes de travail.

| Option | Action |
|---|---|
| **Rendre le pool accessible à n'importe quelle instance du Serveur de connexion View** | Sélectionnez **Aucune restriction**. |
| **Rendre le pool accessible uniquement à des instances du Serveur de connexion View possédant ces balises** | Sélectionnez **Limiter à ces balises** et sélectionnez une ou plusieurs balises. Vous pouvez utiliser les cases à cocher pour sélectionner plusieurs balises. |

5 Cliquez sur **OK** pour enregistrer vos modifications.

# Configuration des fonctionnalités de poste de travail distant 14

Certaines fonctionnalités de poste de travail distant qui sont installées avec Horizon Agent peuvent être mises à jour dans des versions Feature Pack Update ainsi que dans des versions principales d'View. Vous pouvez configurer ces fonctionnalités afin d'améliorer l'expérience de vos utilisateurs finaux sur les postes de travail distants.

Parmi ces fonctionnalités, citons notamment HTML Access, Unity Touch, la redirection d'URL Flash, l'Audio/Vidéo en temps réel, la redirection multimédia (MMR) Windows Media, la redirection USB, la redirection de scanner et la redirection de port série.

Pour plus d'informations sur HTML Access, reportez-vous au document *Utilisation de HTML Access*, disponible dans la page Web de documentation de VMware Horizon Client.

Pour plus d'informations sur la Redirection USB, reportez-vous à Chapitre 15, « Utilisation de périphériques USB avec des applications et postes de travail distants », page 249.

Ce chapitre aborde les rubriques suivantes :

# Configuration d'Unity Touch

Avec Unity Touch, les utilisateurs de tablettes et de smartphones peuvent facilement parcourir, rechercher et ouvrir des applications et des fichiers Windows, choisir des applications et des fichiers préférés et passer d'une application en cours d'exécution à une autre, le tout sans utiliser le menu Démarrer ou la barre des tâches. Vous pouvez configurer une liste par défaut d'applications favorites qui s'affichent dans la barre latérale Unity Touch.

Vous pouvez désactiver ou activer la fonctionnalité Unity Touch après son installation en configurant le paramètre de stratégie de groupe **Activer Unity Touch**. Reportez-vous à la section « Paramètres du modèle d'administration pour la configuration d'Horizon Agent », page 308.

Les documents de VMware Horizon Client pour les périphériques iOS et Android offrent plus d'informations sur les fonctions destinées aux utilisateurs d'Unity Touch.

## Configuration système requise pour Unity Touch

Le logiciel Horizon Client et les périphériques mobiles sur lesquels vous installez Horizon Client doivent respecter certaines exigences de version pour prendre en charge Unity Touch.

**Poste de travail View**

Pour prendre en charge Unity Touch, les logiciels suivants doivent être installés sur la machine virtuelle accédée par l'utilisateur :

- Vous pouvez installer la fonctionnalité Unity Touch en installant View Agent 6.0 ou version ultérieure. Reportez-vous à la section « Installer Horizon Agent sur une machine virtuelle », page 33.
- Systèmes d'exploitation : Windows 7 (32 ou 64 bits), Windows 8 (32 ou 64 bits), Windows 8.1 (32 ou 64 bits), Windows Server 2008 R2 ou Windows Server 2012 R2, Windows 10 (32 ou 64 bits)

**Logiciel Horizon Client**

Unity Touch est pris en charge par les versions Horizon Client suivantes :

- Horizon Client 2.0 pour iOS ou versions ultérieures
- Horizon Client 2.0 pour Android ou versions ultérieures

**Systèmes d'exploitation des appareils portables**

Unity Touch est pris en charge sur les systèmes d'exploitation des appareils portables :

- iOS 5.0 et versions ultérieures
- Android 3 (Honeycomb), Android 4 (Ice Cream Sandwich) et Android 4.1 et 4.2 (Jelly Bean).

## Configurer les applications préférées affichées par Unity Touch

Grâce à la fonctionnalité Unity Touch, les utilisateurs de tablettes et de smartphones peuvent naviguer rapidement vers une application ou un fichier d'un poste de travail View à partir d'une barre latérale Unity Touch. Même si les utilisateurs peuvent spécifier les applications préférées qui apparaissent dans la barre latérale, pour une utilisation plus aisée, les administrateurs peuvent configurer une liste d'applications préférées par défaut.

Si vous utilisez des pools de postes de travail à attribution flottante, les applications et fichiers préférés spécifiés par les utilisateurs finaux seront perdus à chaque déconnexion du poste de travail, sauf si les profils d'utilisateur itinérant sont activés dans Active Directory.

La liste par défaut des applications préférées reste utilisable lorsqu'un utilisateur se connecte pour la première fois à un poste de travail sur lequel Unity Touch est activé. Mais si l'utilisateur configure sa propre liste d'applications préférées, la liste par défaut sera ignorée. La liste d'applications préférées de l'utilisateur, qui est conservée dans le profil itinérant de l'utilisateur, est disponible lorsque l'utilisateur se connecte à d'autres machines d'un pool flottant ou dédié.

Si vous créez une liste d'applications préférées par défaut et qu'une ou plusieurs applications ne sont pas installées sur le système d'exploitation du poste de travail View, ou que les chemins de ces applications sont introuvables dans le menu Démarrer, les applications n'apparaissent pas dans la liste des applications préférées. Vous pouvez utiliser ce comportement pour configurer une liste de référence par défaut des applications préférées pouvant être appliquée à plusieurs images de machine virtuelle ayant différents ensembles d'applications installées.

Par exemple, si Microsoft Office et Microsoft Visio sont installés sur une machine virtuelle, et que Windows Powershell et VMware vSphere Client sont installés sur une deuxième machine virtuelle, vous pouvez créer une liste comprenant les quatre applications. Seules les applications installées apparaissent en tant qu'applications préférées par défaut sur chaque poste de travail.

Il existe d'autres méthodes permettant de spécifier une liste d'applications préférées par défaut :

- Ajouter une valeur au Registre Windows sur les machines virtuelles de pool de postes de travail
- Créer un module d'installation administrative à partir du programme d'installation d'Horizon Agent et distribuer le module aux machines virtuelles
- Exécuter le programme d'installation d'Horizon Agent à partir de la ligne de commande sur les machines virtuelles

---

**Remarque** Unity Touch suppose que les raccourcis des applications sont situés dans le dossier Programmes du menu **Démarrer**. Si un raccourci est situé en dehors du dossier Programmes, ajoutez le préfixe **`Programs`** au chemin du raccourci. Par exemple, `Windows Update.lnk` se trouve dans le dossier `ProgramData\Microsoft\Windows\Menu Démarrer`. Pour publier ce raccourci sous forme d'application préférée par défaut, ajoutez le préfixe **`Programs`** au chemin du raccourci. Par exemple : `"Programs/Windows Update.lnk"`.

---

### Prérequis

- Vérifiez qu'Horizon Agent est installé sur la machine virtuelle.
- Vérifiez que vous disposez des droits d'administration sur la machine virtuelle. Pour cette procédure, vous devrez peut-être modifier un paramètre de registre.
- Si vous disposez de pools de postes de travail à attribution flottante, utilisez Active Directory pour configurer les profils d'utilisateur itinérant. Suivez les instructions fournies par Microsoft.

  Les utilisateurs de pools de postes de travail à attribution flottante pourront consulter leur liste d'applications et de fichiers préférés à chaque connexion.

### Procédure

- (Facultatif) Créez une liste d'applications préférées par défaut en ajoutant une valeur au registre Windows.

  a Ouvrez `regedit` et accédez au paramètre de registre `HKLM\Software\VMware, Inc.\VMware Unity`.

  Sur une machine virtuelle 64 bits, accédez au dossier `HKLM\Software\Wow6432Node\VMware, Inc.\VMware Unity`.

  b Créez une valeur de chaîne appelée `FavAppList`.

  c Spécifiez les applications préférées par défaut.

  Utilisez le format suivant pour spécifier les chemins de raccourci vers les applications utilisées dans le menu Démarrer.

  *path-to-app-1|path-to-app-2|path-to-app-3|…*

  Par exemple :

  `Programs/Accessories/Accessibility/Speech Recognition.lnk|Programs/VMware/VMware vSphere Client.lnk|Programs/Microsoft Office/Microsoft Office 2010 Tools/Microsoft Office 2010 Language Preferences.lnk`

- (Facultatif) Créez une liste d'applications préférées par défaut en créant un module d'installation administrative à partir du programme d'installation d'Horizon Agent.

  a A partir de la ligne de commande, utilisez le format suivant pour créer le package d'installation administrative.

  `VMware-viewagent-x86_64-`*`y.y.y-xxxxxx`*`.exe /s /a /v"/qn TARGETDIR=""`*`partage de réseau pour stocker le module d'installation administrative`*`"" UNITY_DEFAULT_APPS=""`*`liste d'applications favorites par défaut devant être définies dans le registre`*`"""`

  Par exemple :

  `VMware-viewagent-x86_x64-`*`y.y.y-xxxxxx`*`.exe /s /a /v"/qn TARGETDIR=""\\foo-installer-share\ViewFeaturePack\"" UNITY_DEFAULT_APPS=""Programs/Accessories/Accessibility/Ease of Access.lnk|Programs/Accessories/System Tools/Character Map.lnk|Programs/Accessories/Windows PowerShell/Windows PowerShell.lnk|Programs/Internet Explorer (64-bit).lnk|Programs/Google Chrome/Google Chrome.lnk|Programs/iTunes/iTunes.lnk|Programs/Microsoft Office/Microsoft SharePoint Workspace 2010.lnk|Programs/PuTTY/PuTTY.lnk|Programs/Skype/Skype.lnk|Programs/WebEx/Productivity Tools/WebEx Settings.lnk|"""`

  b Distribuez le package d'installation administrative à partir du partage de réseau vers les machines virtuelles de poste de travail à l'aide d'une méthode de déploiement MSI (Microsoft Windows Installer) standard utilisée dans votre organisation.

- (Facultatif) Créez une liste d'applications préférées par défaut en exécutant le programme d'installation d'Horizon Agent directement sur une ligne de commande d'une machine virtuelle.

  Utilisez le format suivant.

  `VMware-viewagent-x86_x64-`*`y.y.y-xxxxxx`*`.exe /s /v"/qn UNITY_DEFAULT_APPS=""`*`liste d'applications favorites par défaut devant être définies dans le registre`*`"""`

  **Remarque** La commande précédente combine l'installation d'Horizon Agent à la spécification de la liste d'applications préférées par défaut. Vous n'avez pas à installer Horizon Agent avant d'exécuter cette commande.

### Suivant

Si vous avez effectué cette tâche directement sur une machine virtuelle (en modifiant le Registre Windows ou en installant Horizon Agent à partir de la ligne de commande), vous devez déployer la machine virtuelle que vous venez de configurer. Vous pouvez créer un snapshot ou un modèle et créer un pool de postes de travail ou recomposer un pool existant. Vous pouvez également créer une stratégie de groupe Active Directory pour déployer la nouvelle configuration.

## Configuration de la redirection d'URL flash pour les flux de multidiffusion ou de monodiffusion

Les clients peuvent désormais utiliser Adobe Media Server et la multidiffusion ou la monodiffusion pour diffuser des événements vidéo en direct dans un environnement d'infrastructure de poste de travail virtuel (VDI). Pour fournir des flux vidéo en direct en multidiffusion ou en monodiffusion dans un environnement VDI, le flux de données multimédia doit être envoyé directement de la source multimédia aux points de terminaison, en contournant les postes de travail distants. La fonctionnalité Redirection d'URL Flash permet d'effectuer cette opération en interceptant et en redirigeant le fichier Shockwave Flash (SWF) du poste de travail distant vers le point de terminaison client.

Les contenus Flash peuvent être affichés à l'aide des lecteurs multimédias flash locaux des clients.

La diffusion de contenus Flash directement à partir d'Adobe Media Server vers les points de terminaison client soulage l'hôte ESXi du datacenter, supprime les routages supplémentaires via le datacenter et réduit la bande passante nécessaire pour écouter simultanément un contenu Flash sur plusieurs points de terminaison client.

La fonctionnalité de redirection d'URL Flash utilise un JavaScript incorporé dans le HTML d'une page Web par l'administrateur de la page Web. Chaque fois que l'utilisateur d'un poste de travail distant clique sur le lien URL désigné sur une page Web, JavaScript intercepte et redirige le fichier SWF à partir de la session de poste de travail distant vers le point de terminaison client. Le point de terminaison ouvre alors un projecteur Flash local hors de la session de poste de travail distant pour lire le flux multimédia en local.

Pour configurer la redirection d'URL Flash, vous devez configurer le HTML de votre page Web et vos périphériques client.

### Procédure

1. Configuration système requise pour la redirection d'URL flash page 198

   Pour prendre en charge la redirection d'URL Flash, le déploiement de votre View doit répondre à certaines exigences matérielles et logicielles.

2. Vérifier que la fonctionnalité redirection d'URL flash est installée page 199

   Avant d'utiliser cette fonctionnalité, vérifiez que la fonctionnalité Redirection d'URL Flash est installée et en cours d'exécution sur vos postes de travail virtuels.

3. Configurer les pages Web qui fournissent des flux de multidiffusion ou de monodiffusion page 199

   Pour permettre la redirection d'URL Flash, vous devez inclure une commande JavaScript dans les pages Web MIME HTML (MHTML) qui fournissent les liens vers les flux de multidiffusion ou de monodiffusion. Les utilisateurs peuvent afficher ces pages Web dans les navigateurs de leurs postes de travail distants pour accéder aux flux vidéo.

4. Configurer des périphériques client pour la redirection d'URL Flash page 200

   La fonctionnalité Redirection d'URL Flash redirige le fichier SWF des postes de travail distants vers les périphériques clients. Pour que ces périphériques client puissent lire des vidéos Flash à partir d'un flux de multidiffusion ou de monodiffusion, vous devez vérifier qu'Adobe Flash Player est installé sur les périphériques client. Les clients doivent également avoir une connectivité IP vers la source multimédia.

5 Activer/désactiver la redirection d'URL Flash page 200

La redirection d'URL Flash est activée lorsque vous effectuez une installation silencieuse d' Horizon Agent avec la propriété `VDM_FLASH_URL_REDIRECTION=1`. Vous pouvez désactiver ou réactiver la fonctionnalité Redirection d'URL Flash sur certains postes de travail distants en définissant une valeur sur une clé de Registre Windows sur ces machines virtuelles.

## Configuration système requise pour la redirection d'URL flash

Pour prendre en charge la redirection d'URL Flash, le déploiement de votre View doit répondre à certaines exigences matérielles et logicielles.

**Poste de travail View**

- Vous installez la redirection d'URL Flash en saisissant la propriété `VDM_FLASH_URL_REDIRECTION` sur la ligne de commande lors d'une installation silencieuse de View Agent 6.0 ou version ultérieure. Reportez-vous à la section « Propriétés de l'installation silencieuse pour Horizon Agent », page 41.
- Les postes de travail doivent tourner sur des systèmes d'exploitation Windows 7, 64 ou 32 bits.
- Internet Explorer 8, 9 et 10, Chrome 29.*x* et Firefox 20.*x* sont parmi les navigateurs de poste de travail pris en charge.

**Lecteur multimédia flash et ShockWave Flash (SWF)**

Vous devez intégrer un lecteur multimédia Flash approprié tel que Strobe Media Playback dans votre site Web. Pour délivrer un contenu multidiffusion, vous pouvez utiliser `multicastplayer.swf` ou `StrobeMediaPlayback.swf` dans vos pages Web. Pour délivrer un contenu monodiffusion, vous devez utiliser `StrobeMediaPlayback.swf`. Vous pouvez également utiliser `StrobeMediaPlayback.swf` pour d'autres fonctionnalités prises en charge telles que la diffusion de flux RTMP et la diffusion dynamique HTTP.

**Logiciel Horizon Client**

Les versions suivantes d'Horizon Client prennent en charge la multidiffusion et la monodiffusion :

- Horizon Client 2.2 pour Linux ou versions ultérieures
- Horizon Client 2.2 pour Windows ou versions ultérieures

Les versions suivantes d'Horizon Client ne prennent en charge que la multidiffusion :

- Horizon Client 2.0 ou 2.1 pour Linux
- Horizon Client 5.4 pour Windows

**Ordinateur Horizon Client ou périphérique d'accès client**

- La redirection d'URL Flash est prise en charge par tous les systèmes d'exploitation qui exécutent Horizon Client pour Linux sur les périphériques client légers x86. Cette fonctionnalité n'est pas prise en charge par les processeurs ARM.
- La redirection d'URL Flash est prise en charge par tous les systèmes d'exploitation qui exécutent Horizon Client pour Windows. Pour plus de détails, reportez-vous au document *Utilisation de VMware Horizon Client pour Windows*.
- Sur les périphériques client Windows, vous devez installer Adobe Flash Player 10.1 ou versions ultérieures pour Internet Explorer.

- Sur les périphériques clients légers Linux, vous devez installer les fichiers `libexpat.so.0` et `libflashplayer.so`. Reportez-vous à la section « Configurer des périphériques client pour la redirection d'URL Flash », page 200.

**Remarque** Avec la redirection d'URL Flash, le flux de multidiffusion ou de monodiffusion est redirigé vers les périphériques clients qui pourraient être en dehors du pare-feu de votre organisation. Vos clients doivent avoir accès au serveur Web d'Adobe hébergeant le fichier Shockwave Flash (SWF) qui initie les flux de multidiffusion ou de monodiffusion. Si nécessaire, configurez votre pare-feu pour ouvrir les ports appropriés afin de permettre aux périphériques client d'accéder à ce serveur.

## Vérifier que la fonctionnalité redirection d'URL flash est installée

Avant d'utiliser cette fonctionnalité, vérifiez que la fonctionnalité Redirection d'URL Flash est installée et en cours d'exécution sur vos postes de travail virtuels.

La fonctionnalité de redirection d'URL Flash doit être présente sur chaque poste de travail avec lequel vous souhaitez prendre en charge la redirection de multidiffusion ou de monodiffusion. Pour obtenir des instructions d'installation d'Horizon Agent, consultez le document « Propriétés de l'installation silencieuse pour Horizon Agent », page 41.

### Procédure

1. Démarrez une session de poste de travail distant qui utilise PCoIP.
2. Ouvrez le Gestionnaire des tâches.
3. Vérifiez que le processus `ViewMPServer.exe` est en cours d'exécution sur le poste de travail.

## Configurer les pages Web qui fournissent des flux de multidiffusion ou de monodiffusion

Pour permettre la redirection d'URL Flash, vous devez inclure une commande JavaScript dans les pages Web MIME HTML (MHTML) qui fournissent les liens vers les flux de multidiffusion ou de monodiffusion. Les utilisateurs peuvent afficher ces pages Web dans les navigateurs de leurs postes de travail distants pour accéder aux flux vidéo.

En outre, vous pouvez personnaliser le message d'erreur en anglais que voient les utilisateurs en cas de problème avec la redirection d'URL Flash. Choisissez cette option si vous souhaitez afficher un message d'erreur dans la langue locale pour les utilisateurs finaux. Vous devez incorporer la configuration `var vmwareScriptErroMessage` ainsi que votre chaîne de texte localisé dans la page Web MHTML.

### Prérequis

Assure-vous que la bibliothèque `swfobject.js` est importée dans la page Web MHTML.

### Procédure

1. Insérez la commande JavaScript `viewmp.js` dans la page Web MHTML.

   Par exemple : `<script type="text/javascript" src="http://localhost:33333/viewmp.js"></script>`

2. (Facultatif) Personnalisez le message d'erreur de redirection d'URL Flash envoyé aux utilisateurs finaux.

   Par exemple : "`var vmwareScriptErroMessage=`*`message d'erreur localisé`*"

3 Veillez à incorporer la commande JavaScript `viewmp.js` et personnalisez éventuellement le message d'erreur de redirection d'URL Flash avant que le fichier ShockWave Flash (SWF) ne soit importé dans la page Web MHTML.

Lorsqu'un utilisateur affiche la page Web dans un poste de travail distant, la commande JavaScript `viewmp.js` invoque sur le poste de travail distant le mécanisme de redirection d'URL Flash qui redirige le fichier SWF du poste de travail vers le périphérique d'hébergement client.

## Configurer des périphériques client pour la redirection d'URL Flash

La fonctionnalité Redirection d'URL Flash redirige le fichier SWF des postes de travail distants vers les périphériques clients. Pour que ces périphériques client puissent lire des vidéos Flash à partir d'un flux de multidiffusion ou de monodiffusion, vous devez vérifier qu'Adobe Flash Player est installé sur les périphériques client. Les clients doivent également avoir une connectivité IP vers la source multimédia.

**Remarque** Avec la redirection d'URL Flash, le flux de multidiffusion ou de monodiffusion est redirigé vers les périphériques clients qui pourraient être en dehors du pare-feu de votre organisation. Vos clients doivent avoir accès au serveur Web d'Adobe qui héberge le fichier SWF qui initie les flux de multidiffusion ou de monodiffusion. Si nécessaire, configurez votre pare-feu pour ouvrir les ports appropriés afin de permettre aux périphériques client d'accéder à ce serveur.

### Procédure

◆ Installer Adobe Flash Player sur vos périphériques client.

| Système d'exploitation | Action |
|---|---|
| **Windows** | Installez Adobe Flash Player 10.1 ou versions ultérieures pour Internet Explorer. |
| **Linux** | a Installez le fichier `libexpat.so.0` ou assurez-vous que ce fichier est déjà installé.<br>Vérifiez que le fichier est installé dans le répertoire `/usr/lib` ou `/usr/local/lib`.<br>b Installez le fichier `libflashplayer.so`, ou assurez-vous que ce fichier est déjà installé.<br>Assurez-vous que le fichier est installé dans le répertoire du plug-in Flash approprié de votre système d'exploitation Linux.<br>c Installez le programme `wget`, ou assurez-vous que le fichier de ce programme est déjà installé. |

## Activer/désactiver la redirection d'URL Flash

La redirection d'URL Flash est activée lorsque vous effectuez une installation silencieuse d'Horizon Agent avec la propriété `VDM_FLASH_URL_REDIRECTION=1`. Vous pouvez désactiver ou réactiver la fonctionnalité Redirection d'URL Flash sur certains postes de travail distants en définissant une valeur sur une clé de Registre Windows sur ces machines virtuelles.

### Procédure

1 Démarrez l'éditeur du Registre Windows sur la machine virtuelle.

2 Accédez à la clé du Registre Windows qui commande la Redirection d'URL Flash.

| Option | Description |
|---|---|
| **Windows 7 64 bits** | `HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware ViewMP\enabled = value` |
| **Windows 7 32 bits** | `HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware ViewMP\enabled = value` |

3 Définissez la valeur pour désactiver ou activer Redirection d'URL Flash.

| Option | Valeur |
|---|---|
| **Désactivé** | `0` |
| **Activé** | `1` |

Par défaut, la valeur est définie sur `1`.

# Configuration de la redirection Flash

Avec la fonctionnalité de redirection Flash, le contenu Flash est envoyé au système client et lu dans une fenêtre de conteneur Flash à l'aide de la version ActiveX de Flash Player.

**Remarque** Dans cette version, la redirection Flash est disponible uniquement comme fonctionnalité de la version d'évaluation technique.

Même si le nom de cette fonctionnalité est semblable à celui de la fonctionnalité Redirection d'URL Flash, il existe des différences importantes, comme décrit dans le tableau suivant.

**Tableau 14-1.** Comparaison entre les fonctionnalités Redirection Flash et Redirection d'URL Flash

| Élément de différenciation | Redirection Flash | Redirection d'URL Flash |
|---|---|---|
| Niveau de prise en charge | En tant que fonctionnalité de la version d'évaluation technique, aucune prise en charge n'est offerte | Entièrement prise en charge |
| Types d'Horizon Client prenant en charge cette fonctionnalité | Client Windows uniquement | Client Windows et client Linux |
| Protocole d'affichage requis | PCoIP | PCoIP |
| Navigateurs | Internet Explorer 9, 10 ou 11 pour l'agent (poste de travail distant) | Tous les navigateurs qui sont actuellement pris en charge sur Horizon Client et Horizon Agent |
| Mécanisme de configuration | Utilisez un GPO côté agent pour spécifier une liste blanche de sites Web qui utiliseront la redirection Flash | Modifiez le code source sur la page Web pour intégrer le JavaScript requis |

## Limites des fonctionnalités

La fonctionnalité de redirection Flash présente les limites suivantes :

- Cliquer sur un lien URL dans la fenêtre de Flash Player ouvre un navigateur sur le client plutôt que sur le poste de travail distant (côté agent).
- Les fonctionnalités Flash suivantes ne sont pas opérationnelles avec la redirection Flash : Lecture automatique, les boutons Suivant et Précédent ainsi que le mode cinéma.

- Certains sites Web ne fonctionnent pas avec la redirection Flash sur certaines versions de navigateur. Par exemple, le site vimeo.com ne fonctionne pas si vous utilisez Internet Explorer 11.
- Il est possible que Flash et le script Java ne fonctionnent pas comme prévu.
- Il est possible que la fenêtre de Flash Player ne se redimensionne pas correctement si vous redimensionnez la fenêtre du navigateur ou la fenêtre d'Horizon Client.
- La fenêtre d'Horizon Client peut se figer lors de la lecture du contenu Flash, même si vous pouvez définir une clé de registre Windows pour résoudre ce problème.

  Sur un client 32 bits, définissez la valeur `HKLM\Software\VMware, Inc.\VMware VDM\Client\EnableD3DRenderer` sur « FALSE » et, sur un client 64 bits, définissez `HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\EnableD3DRenderer` sur « FALSE ».

## Configuration requise pour la redirection Flash (Tech Preview)

Avec la redirection Flash, si vous utilisez un navigateur Internet Explorer 9, 10 ou 11, le contenu Flash est envoyé au système client. Le système client effectue la lecture du contenu multimédia, déchargeant ainsi la demande sur l'hôte ESXi.

La redirection Flash est disponible en tant que fonction de la version d'évaluation technique avec Horizon 7 et Horizon Client 4.0.

| | |
|---|---|
| **Poste de travail distant** | ■ Horizon Agent 7.0 ou version ultérieure doit être installé sur un poste de travail distant mono-utilisateur (VDI), avec l'option de redirection Flash (cette option n'est pas sélectionnée par défaut).<br>Reportez-vous à la section « Options d'installation personnalisée d'Horizon Agent », page 35.<br>■ Les paramètres de stratégie de groupe appropriés doivent être configurés. Reportez-vous à la section « Installer et configurer la redirection Flash », page 203.<br>■ La redirection Flash est prise en charge sur les systèmes d'exploitation Windows 7, Windows 8 et Windows 8.1 installés sur des postes de travail distants mono-utilisateur.<br>■ Internet Explorer 9, 10 ou 11 doit être installé avec le plug-in Flash ActiveX correspondant.<br>■ Après l'installation, dans Internet Explorer, le composant complémentaire VMware View FlashMMR Server doit être activé. |
| **Ordinateur Horizon Client ou périphérique d'accès client** | ■ Horizon Client 4.0 ou version ultérieure doit être installé. (L'option de redirection Flash est activée par défaut.)<br>Consultez la rubrique sur l'installation d'Horizon Client dans le document *Utilisation de VMware Horizon Client pour Windows*.<br>■ La redirection Flash est prise en charge sur les systèmes d'exploitation clients Windows 7, Windows 8 et Windows 8.1.<br>■ Le plug-in Flash ActiveX doit être installé et activé |
| **Protocole d'affichage de la session distante** | PCoIP |

## Installer et configurer la redirection Flash

La redirection du contenu Flash à partir d'un poste de travail distant vers une fenêtre de Flash Player sur le système client local requiert l'installation de la fonctionnalité de redirection Flash et d'Internet Explorer sur le poste de travail distant et sur le système client ainsi que la spécification des sites Web qui utiliseront cette fonctionnalité.

Pour installer cette fonctionnalité sur le système client, vous devez utiliser un programme d'installation Horizon Client 4.0 ou version ultérieure. Pour installer cette fonctionnalité sur un poste de travail distant, vous devez utiliser un programme d'installation Horizon Agent 7.0 ou version ultérieure et sélectionner l'option d'installation correcte, qui n'est pas sélectionnée par défaut. Pour activer cette fonctionnalité et spécifier quels sites Web l'utiliseront, vous utilisez une stratégie de groupe.

---

**Remarque** Vous pouvez également utiliser des paramètres de registre Windows sur le poste de travail distant pour configurer une liste blanche de sites Web à utiliser pour la redirection Flash. Reportez-vous à la section « Utiliser des paramètres de registre Windows pour configurer la redirection Flash », page 205.

---

### Prérequis

- Vérifiez que vous pouvez vous connecter en tant qu'utilisateur de domaine Administrateur sur la machine qui héberge votre serveur Active Directory.
- Vérifiez que les composants logiciels enfichables MMC (Microsoft Management Console) et l'Éditeur d'objets de stratégie de groupe sont disponibles sur votre serveur Active Directory.
- Vérifiez que le modèle d'administration de configuration d'Horizon Agent (fichier `vdm_agent.adm`) a été ajouté à l'UO pour le poste de travail distant. Reportez-vous à la section « Ajouter des modèles d'administration View à un GPO », page 349.
- Compilez une liste des sites Web qui utiliseront cette fonctionnalité pour rediriger le contenu Flash. Cette liste est une liste blanche, ce qui signifie que seules les URL spécifiées dans cette liste pourront utiliser cette fonctionnalité.

### Procédure

1. Sur un système client Windows 7, Windows 8 ou Windows 8.1, installez la version requise d'Horizon Client et Flash Player version ActiveX.
   - Installez Horizon Client 4.0 ou version ultérieure. Consultez la rubrique sur l'installation d'Horizon Client dans le document *Utilisation de VMware Horizon Client pour Windows*.
   - Si nécessaire, installez la version ActiveX de Flash Player (plutôt que la version NPAPI). Flash Player est installé par défaut dans Internet Explorer 10 et 11. Pour Internet Explorer 9, vous devrez peut-être aller sur le site suivant pour télécharger et installer Flash Player : https://get.adobe.com/flashplayer/.
2. Dans un poste de travail distant Windows 7, Windows 8 ou Windows 8.1, installez la version requise d'Horizon Agent et d'Internet Explorer, avec Flash Player.
   - Installez Horizon Agent 7.0 ou version ultérieure et veillez à sélectionner l'option pour la redirection Flash (expérimentale). Cette option n'est pas sélectionnée par défaut.
   - Installez Internet Explorer 9, 10 ou 11.
   - Si nécessaire, installez la version ActiveX de Flash Player (plutôt que la version NPAPI). Flash Player est installé par défaut dans Internet Explorer 10 et 11. Pour Internet Explorer 9, vous devrez peut-être aller sur le site suivant pour télécharger et installer Flash Player : https://get.adobe.com/flashplayer/.

3 Sur le poste de travail distant, dans Internet Explorer, sélectionnez **Outils > Gérer les modules complémentaires** dans la barre de menus et vérifiez que **VMware View FlashMMR Server** est répertorié et activé.

4 Sur le serveur Active Directory, ouvrez l'Éditeur de gestion de stratégie de groupe et modifiez les paramètres de stratégie de redirection Flash sous **Configuration ordinateur**.

   Les paramètres se trouvent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Modèles d'administration classiques > Configuration de VMware Horizon Agent > VMware FlashMMR**.

| Paramètre | Description |
|---|---|
| **Activer la redirection multimédia Flash** | Spécifie si la redirection Flash (FlashMMR) est activée sur le poste de travail distant (côté agent). Lorsqu'elle est activée, cette fonctionnalité transmet les données multimédia Flash depuis les URL désignées via un canal TCP au client, et appelle le Flash Player local sur le système client. Cette fonctionnalité réduit grandement la demande sur le CPU côté agent et sur la bande passante réseau. |
| **Taille minimale du rectangle** | Spécifie la largeur et la hauteur minimales, en pixels, du rectangle dans lequel est lu le contenu Flash. Par exemple, **`400,300`** spécifie une largeur de 400 pixels et une hauteur de 300 pixels. La redirection Flash sera utilisée uniquement si le contenu Flash est égal ou supérieur aux valeurs spécifiées dans cette stratégie. Si ce GPO n'est pas configuré, la valeur par défaut utilisée est **`320,200`**. |

5 Dans l'Éditeur de gestion de stratégie de groupe, modifiez les paramètres de stratégie de redirection Flash sous **Configuration d'utilisateur**.

   Les paramètres se trouvent dans le dossier **Configuration d'utilisateur > Stratégies > Modèles d'administration > Modèles d'administration classiques > Configuration de VMware Horizon Agent > VMware FlashMMR**.

   a Ouvrez le paramètre pour faire une liste des URL d'hôte que vous voulez utiliser avec la redirection Flash et sélectionnez le bouton radio **Activé**.

   b Cliquez sur le bouton **Afficher**.

   c Entrez les URL complètes dans la colonne Nom et laissez la colonne Valeur vide.

      Veillez à inclure **http://** ou **https://**. Vous pouvez utiliser des expressions régulières. Par exemple, vous pouvez spécifier **`https://*.google.com`** et **`http://www.cnn.com`**.

6 Sur la machine agent, ouvrez une invite de commande en tant qu'administrateur et passez les répertoires sur le répertoire suivant :

```
%Program Files%\Common Files\VMware\Remote Experience
```

   Le fichier `mergeflashmmrwhitelist.vbs` se trouve dans ce répertoire.

7 Exécutez la commande suivante pour vérifier que la liste blanche que vous avez configurée est ajoutée aux sites de confiance d'Internet Explorer et à l'affichage de compatibilité.

```
cscript  mergeflashmmrwhitelist.vbs
```

8 Redémarrez Internet Explorer.

   Le ou les sites sont ajoutés. Vous pouvez vérifier les sites de confiance en sélectionnant **Outils > Options Internet** dans la barre de menus d'Internet Explorer et, dans l'onglet **Sécurité**, cliquez sur le bouton **Sites**. Vous pouvez vérifier les paramètres de compatibilité en sélectionnant **Outils > Paramètres d'affichage de compatibilité** dans la barre de menus.

## Utiliser des paramètres de registre Windows pour configurer la redirection Flash

Si vous êtes un utilisateur de domaine sans privilèges d'administrateur sur le serveur Active Directory, vous pouvez également configurer la redirection Flash en définissant les valeurs appropriées dans des clés de registre Windows sur le poste de travail distant.

Vous pouvez utiliser cette procédure comme alternative à l'utilisation des paramètres GPO pour configurer la redirection Flash.

### Prérequis

- Compilez une liste des sites Web qui utiliseront cette fonctionnalité pour rediriger le contenu Flash. Cette liste est une liste blanche, ce qui signifie que seules les URL spécifiées dans cette liste pourront utiliser cette fonctionnalité.
- Vérifiez qu'Horizon Agent 7.0 ou version ultérieure est installé sur le poste de travail distant, ainsi que Flash Player et Internet Explorer 9, 10 ou 11. Reportez-vous à la section « Installer et configurer la redirection Flash », page 203.
- Vérifiez que vous utilisez Horizon Client 4.0 ou version ultérieure, ainsi que la version ActiveX de Flash Player.

### Procédure

1. Utilisez Horizon Client pour accéder au poste de travail distant (machine agent).
2. Ouvrez l'Éditeur du Registre Windows (`regedit.exe`) sur la machine agent, accédez au dossier suivant et définissez **FlashRedirection** sur **`1`** :

   ```
   HKLM\Software\VMware, Inc.\VMware FlashMMR
   ```

   **Remarque** Ce paramètre active la fonctionnalité de redirection Flash, mais si ce paramètre est désactivé (défini sur 0) dans `HKLM\Software\Policies\VMware, Inc.\VMware FlashMMR`, cela signifie que la redirection Flash est désactivée dans tout le domaine et qu'un administrateur de domaine doit l'activer.

3. Accédez au dossier suivant :

   ```
   HKEY_CURRENT_USER\SOFTWARE\VMware, Inc.\VMware FlashMMR
   ```

   Si ce dossier n'existe pas déjà, créez-le.
4. Dans le dossier `VMware FlashMMR`, créez une sous-clé **UrlWhiteList**.
5. Cliquez avec le bouton droit sur la clé **UrlWhiteList**, sélectionnez **Nouveau > Valeur de chaîne** et, pour le nom, entrez l'URL d'un site Web qui utilisera la fonctionnalité de redirection Flash.

   Vous pouvez utiliser des expressions régulières. Par exemple, vous pouvez spécifier **`https://*.google.com`**. Veillez à laisser la valeur **Données** vide.
6. Répétez l'étape précédente pour ajouter des URL supplémentaires et, lorsque vous avez terminé, fermez l'Éditeur du Registre.
7. Sur la machine agent, ouvrez une invite de commande en tant qu'administrateur et passez les répertoires sur le répertoire suivant :

   ```
   %Program Files%\Common Files\VMware\Remote Experience
   ```

   Le fichier `mergeflashmmrwhitelist.vbs` se trouve dans ce répertoire.
8. Exécutez la commande suivante pour vérifier que la liste blanche que vous avez configurée est ajoutée aux sites de confiance d'Internet Explorer et à l'affichage de compatibilité.

   ```
   cscript  mergeflashmmrwhitelist.vbs
   ```

9 Redémarrez Internet Explorer.

Le ou les sites sont ajoutés. Vous pouvez vérifier les sites de confiance en sélectionnant **Outils > Options Internet** dans la barre de menus d'Internet Explorer et, dans l'onglet **Sécurité**, cliquez sur le bouton **Sites**. Vous pouvez vérifier les paramètres de compatibilité en sélectionnant **Outils > Paramètres d'affichage de compatibilité** dans la barre de menus.

## Configuration de la redirection de contenu URL

Avec la redirection de contenuURL, vous pouvez configurer des URL spécifiques pour qu'elles s'ouvrent toujours sur le client ou dans une application ou un poste de travail distant.

Vous pouvez rediriger deux types d'URL :

- Les URL que les utilisateurs saisissent dans la barre d'adresse d'Internet Explorer.
- Les liens dans une application, telle qu'Outlook ou Word, sur lesquels les utilisateurs peuvent cliquer.

Vous pouvez configurer n'importe quel nombre de protocoles, tels qu'HTTP, mailto et callto, pour la redirection. Cette fonctionnalité prend en charge la redirection dans les deux sens :

- Depuis un client vers une application ou un poste de travail distant (client vers agent)

  En fonction des règles que vous configurez, Horizon Client lance un poste de travail distant ou une application distante pour traiter l'URL. Si un poste de travail est lancé, l'application par défaut pour le protocole de l'URL traite l'URL.

- Depuis une application ou un poste de travail distant vers un client (agent vers client)

  Horizon Agent envoie l'URL à Horizon Client, qui lance l'application par défaut pour le protocole qui est spécifié dans l'URL.

Vous pouvez rediriger certaines URL depuis l'application ou le poste de travail distant vers le client et d'autres URL depuis le client vers l'application ou le poste de travail distant.

---

**Remarque** Vous pouvez disposer d'un environnement où Horizon Client est installé sur un poste de travail distant, ce qui signifie qu'Horizon Agent et Horizon Client sont installés sur la même machine. Par exemple, un utilisateur se connecte à un périphérique client léger et est connecté à un poste de travail distant. À partir du poste de travail, l'utilisateur exécute Horizon Client pour accéder à des applications distantes. Sur cette machine de poste de travail, vous pouvez installer Horizon Agent avec la fonctionnalité de redirection de contenu URL ou installer Horizon Client avec la fonctionnalité, mais pas les deux. Par conséquent, sur cette machine, vous pouvez configurer la redirection client vers agent ou la redirection agent vers client, mais pas les deux.

---

Pour configurer cette fonctionnalité, vous devez exécuter les tâches suivantes :

- Pour la redirection client vers agent, installez Horizon Client avec la fonctionnalité de redirection de contenu URL. Reportez-vous à la section « Installation de la fonctionnalité de redirection de contenu URL », page 208.
- Pour la redirection agent vers client, installez Horizon Agent avec la fonctionnalité de redirection de contenu URL. Reportez-vous à la section « Installation de la fonctionnalité de redirection de contenu URL », page 208.
- Configurez des paramètres GPO pour indiquer, pour chaque protocole, comment Horizon Agent ou Horizon Client doit rediriger l'URL. Reportez-vous à la section « Paramètres du modèle de redirection de contenu URL VMware Horizon », page 210.

## Exigences de la fonctionnalité

Cette fonctionnalité a les exigences suivantes :

- Horizon Client 4.0 ou version ultérieure.
- Internet Explorer 9,10 et 11 sont les navigateurs pris en charge dans lesquels vous pouvez taper ou cliquer sur une URL pour qu'elle soit redirigée.
- Le protocole d'affichage pour la session distante doit être VMware Blast ou PCoIP.

## Limites des fonctionnalités

Cette fonctionnalité peut se comporter de façon inattendue, comme dans les exemples suivants :

- Si l'URL ouvre une page spécifique d'un pays basée sur les paramètres régionaux, la page régionale qui s'ouvre est déterminée par la source du lien. Par exemple, si le poste de travail distant (source agent) réside dans un centre de données au Japon et que l'ordinateur de l'utilisateur se trouve aux États-Unis, si l'URL est redirigée depuis l'agent vers la machine cliente, la page qui s'ouvre sur le client aux États-Unis est la page japonaise.
- Si les utilisateurs créent des favoris de pages Web, ils sont créés après la redirection. Par exemple, supposons qu'un utilisateur clique sur un lien sur la machine cliente et que l'URL soit redirigée vers un poste de travail distant (agent). Si l'utilisateur crée un favori pour cette page, le favori est créé sur l'agent. Lorsque l'utilisateur ouvre à nouveau le navigateur sur la machine cliente, il peut s'attendre à trouver le favori sur la machine cliente, mais le favori a été stocké sur l'agent (poste de travail distant).
- Les fichiers que les utilisateurs téléchargent sont placés sur la machine dont le navigateur a été utilisé pour ouvrir l'URL. Par exemple, supposons qu'un utilisateur clique sur un lien sur la machine cliente et que l'URL soit redirigée vers un poste de travail distant. Si le lien était destiné au téléchargement d'un fichier, ou s'il s'agit du lien d'une page Web sur laquelle l'utilisateur télécharge un fichier, le fichier est téléchargé sur le poste de travail distant plutôt que sur la machine cliente.

La redirection de contenu URL ne fonctionne pas dans les circonstances suivantes :

- Les URL raccourcies, telles que `https://goo.gl/abc`, peuvent être redirigées en fonction de règles de filtrage, mais le mécanisme de filtrage ne ressemble pas à l'URL non raccourcie d'origine. Par exemple, si vous disposez d'une règle qui redirige les URL contenant `acme.com`, une URL d'origine telle que `http://www.acme.com/some-really-long-path` et une URL raccourcie de l'URL d'origine telle que `https://goo.gl/xyz`, l'URL d'origine est redirigée mais pas l'URL raccourcie.

  Solution : créez des règles pour bloquer ou rediriger des URL des sites Web connus pour raccourcir souvent les URL.
- Les pages HTML intégrées contournent la redirection URL. Par exemple, supposons qu'un utilisateur atteigne une URL qui ne correspond pas à une règle de redirection URL. Si la page contient une page HTML intégrée (iFrame ou cadre en ligne) dont l'URL ne correspond pas à une règle de redirection, la règle de redirection URL ne fonctionne pas. La règle ne fonctionne que sur l'URL de niveau supérieur.
- La redirection de contenu URL ne fonctionne pas si les plug-ins Internet Explorer sont désactivés, par exemple, lorsque l'utilisateur passe à la navigation InPrivate dans Internet Explorer. (On utilise la navigation privée pour que les pages Web et les fichiers téléchargés depuis des pages Web n'apparaissent pas dans l'historique de navigation et de téléchargement de l'ordinateur.) Cette limite se produit, car la fonctionnalité de redirection URL requiert qu'un certain plug-in Internet Explorer soit activé, et la navigation privée désactive ces plug-ins.

Solution : utilisez le paramètre GPO pour empêcher les utilisateurs de désactiver les plug-ins. Ces paramètres incluent ce qui suit : « Ne pas autoriser les utilisateurs à activer ou désactiver les modules complémentaires » et « Activer automatiquement les modules complémentaires nouvellement installés ». Dans l'Éditeur de la gestion des stratégies de groupes, ces paramètres sont disponibles sous **Configuration ordinateur > Modèles d'administration > Composants Windows > Internet Explorer**.

Solution spécifique pour Internet Explorer : utilisez le paramètre GPO pour désactiver le mode InPrivate. Il s'agit du paramètre « Désactiver la navigation InPrivate ». Dans l'Éditeur de la gestion des stratégies de groupes, ces paramètres sont disponibles sous **Configuration ordinateur > Modèles d'administration > Composants Windows > Internet Explorer > Confidentialité**.

Ces deux solutions sont des recommandations et elles peuvent éviter des problèmes avec la redirection que des situations autres que la navigation privée peuvent provoquer.

- La redirection URL ne fonctionne pas si une application universelle Windows 10 est le gestionnaire par défaut d'un protocole spécifié dans un lien. Les applications universelles, basées sur la plate-forme Windows universelle pour pouvoir être téléchargées vers des PC, des tablettes et des téléphones, incluent le navigateur Microsoft Edge, Courrier, Cartes, Photos, Groove Musique, etc. Par conséquent, si vous cliquez sur un lien pour lequel l'une de ces applications est le gestionnaire par défaut, l'URL ne sera pas redirigée. Par exemple, si un utilisateur clique sur un lien d'e-mail dans une application et que l'application de messagerie par défaut est l'application universelle Courrier, l'URL spécifiée dans le lien ne sera pas redirigée.

  Solution : définissez une autre application comme gestionnaire par défaut du protocole d'URL que vous voulez rediriger. Par exemple, si Edge est le navigateur par défaut, définissez Internet Explorer comme navigateur par défaut.

- Les machines sur lesquelles le démarrage sécurisé est activé laisseront la fonctionnalité de redirection de contenu URL désactivée. Les URL ne peuvent pas être redirigées depuis ces machines. Toutefois, elles peuvent être redirigées vers ces machines.

## Installation de la fonctionnalité de redirection de contenu URL

Ni Horizon Agent, ni l'assistant d'installation d'Horizon Client, ne répertorie la redirection de contenu URL comme une fonctionnalité pouvant être sélectionnée. Vous devez installer cette fonctionnalité en exécutant le programme d'installation avec une option de ligne de commande.

Pour prendre en charge la redirection de contenu URL à partir d'une application ou d'un poste de travail distant vers un client, vous devez installer Horizon Agent avec la fonctionnalité de redirection de contenu URL. Pour prendre en charge la redirection de contenu URL à partir d'un client vers un poste de travail distant, vous devez installer Horizon Client avec la fonctionnalité de redirection de contenu URL.

### Installation d' Horizon Agent avec la fonctionnalité de redirection de contenu URL

Démarrez l'installation en exécutant la commande suivante dans une fenêtre d'invite de commande au lieu de double-cliquer sur le fichier du programme d'installation. Par exemple :

```
VMware-viewagent-x86_64-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

Après avoir suivi les invites et terminé l'installation, vous pouvez vérifier que cette fonctionnalité est installée en contrôlant si les fichiers `vmware-url-protocol-launch-helper.exe` et `vmware-url-filtering-plugin.dll` sont installés dans le répertoire `%PROGRAMFILES%\VMware\VMware View\Agent\bin\UrlRedirection\`. Vérifiez également que le complément additionnel Internet Explorer suivant est activé : Plug-in de filtrage URL VMware Horizon View.

### Installation d' Horizon Client avec la fonctionnalité de redirection de contenu URL

Démarrez l'installation en exécutant la commande suivante dans une fenêtre d'invite de commande au lieu de double-cliquer sur le fichier du programme d'installation. Par exemple :

```
VMware-Horizon-Client-x86-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

Après avoir suivi les invites et terminé l'installation, vous pouvez vérifier que cette fonctionnalité est installée en contrôlant si les fichiers `vmware-url-protocol-launch-helper.exe` et `vmware-url-filtering-plugin.dll` sont installés dans le répertoire `%PROGRAMFILES%\VMware\VMware Horizon View Client\`. Vérifiez également que le complément additionnel Internet Explorer suivant est installé : Plug-in de filtrage URL VMware Horizon View.

## Ajouter le modèle d'administration de redirection de contenu URL à Active Directory

Vous pouvez ajouter les paramètres de stratégie du fichier ADM de redirection de contenu URL `urlRedirection-enUS.adm` aux objets de stratégie de groupe (GPO) dans Active Directory et configurer les paramètres dans l'Éditeur d'objets de stratégie de groupe.

### Prérequis

- Si vous prévoyez de définir des stratégies pour des liens sur lesquels vous cliquez dans des applications ou des postes de travail distants, vérifiez que la fonctionnalité de redirection de contenu URL est incluse lorsque vous installez Horizon Agent. Reportez-vous à la section « Configuration de la redirection de contenu URL », page 206.
- Si vous prévoyez de définir des stratégies pour des liens sur lesquels vous cliquez dans des applications ou des navigateurs clients, vérifiez que la fonctionnalité de redirection de contenu URL est incluse lorsque vous installez Horizon Client. Reportez-vous à la section « Configuration de la redirection de contenu URL », page 206.
- Vérifiez que les objets de stratégie de groupe (GPO) Active Directory sont créés pour les paramètres de stratégie de groupe de redirection de contenu URL. Pour des règles concernant des liens sur lesquels vous cliquez depuis une application ou un poste de travail distant, les GPO doivent être liés à l'UO qui contient vos postes de travail et vos hôtes RDS. Pour les liens sur lesquels vous cliquez à l'intérieur du système client, les GPO doivent être liés à l'UO qui contient les ordinateurs clients.

  Reportez-vous à la section « Exemple de stratégie de groupe Active Directory », page 347.
- Vérifiez que les composants logiciels enfichables MMC (Microsoft Management Console) et l'Éditeur d'objets de stratégie de groupe sont disponibles sur votre serveur Active Directory.
- Familiarisez-vous avec les paramètres de la stratégie de groupe de redirection de contenu URL. Reportez-vous à la section « Paramètres du modèle de redirection de contenu URL VMware Horizon », page 210.

### Procédure

1. Téléchargez le fichier View GPO Bundle `.zip` sur le site de téléchargement de VMware à l'adresse https://my.vmware.com/web/vmware/downloads.

   Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut GPO Bundle.

   Le fichier se nomme `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`, où *x.x.x* est la version et *yyyyyyy* le numéro de build. Tous les fichiers ADM et ADMX qui fournissent des paramètres de stratégie de groupe pour View sont disponibles dans ce fichier.
2. Décompressez le fichier `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` et copiez le fichier ADM de redirection de contenu URL `urlRedirection-enUS.adm` sur votre serveur Active Directory.
3. Sur le serveur Active Directory, modifiez les objets de stratégie de groupe (GPO) en sélectionnant **Démarrer > Outils d'administration > Gestion de stratégie de groupe**, puis en cliquant avec le bouton droit sur GPO et en sélectionnant **Édition**.
4. Dans l'Éditeur d'objets de stratégie de groupe, cliquez avec le bouton droit sur le dossier **Configuration de l'ordinateur > Stratégies > Modèles d'administration**, puis sélectionnez **Ajout/Suppression de modèles**.

5 Cliquez sur **Ajouter**, localisez le fichier `urlRedirection-enUS.adm` et cliquez sur **Ouvrir**.

6 Cliquez sur **Fermer** pour ajouter les paramètres de stratégie dans le fichier ADM au GPO.

   Les paramètres se trouvent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Modèles d'administration classiques > Redirection URL de VMware Horizon**.

7 Configurez les paramètres de la stratégie de groupe de redirection de contenu URL.

Les stratégies de groupe sont configurées pour le groupe d'ordinateurs clients ou de postes de travail distants pour les hôtes RDS inclus dans l'UO.

## Paramètres du modèle de redirection de contenu URL VMware Horizon

Le fichier de modèle ADM de redirection de contenu URL Horizon (`urlRedirection-enUS.adm`) contient des paramètres de stratégie destinés à contrôler si un lien URL est ouvert sur le client ou du côté agent, dans une application ou un poste de travail distant. Par exemple, pour une sécurité accrue, les administrateurs peuvent définir une stratégie pour que tous les liens URL qui pointent vers l'extérieur du réseau d'entreprise soient ouverts dans une application ou un poste de travail distant, et ce pour tous les employés travaillant à l'intérieur du réseau d'entreprise.

Ce fichier ADM est disponible dans un fichier groupé `.zip` nommé `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`, que vous pouvez télécharger sur le site de téléchargement de VMware à l'adresse https://my.vmware.com/web/vmware/downloads. Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut le fichier groupé `.zip`.

La redirection de contenu URL peut se produire lorsque les utilisateurs finaux cliquent sur un lien URL dans un navigateur ou une application, comme un document Microsoft Word ou un e-mail, ou si un utilisateur clique sur une URL ou en saisit une dans un navigateur Internet Explorer 9, 10 ou 11. Les liens URL peuvent être des liens vers des pages Web, des numéros de téléphone, des adresses e-mail, etc.

### Syntaxe pour les règles de redirection de contenu URL

Lorsque vous indiquez les URL à ouvrir sur le client ou l'agent, vous pouvez utiliser des expressions régulières. Séparez les entrées multiples par des points-virgules. Les espaces ne sont pas autorisés entre les entrées.

Voici quelques exemples.

| Entrée | Description |
|---|---|
| `.*` | (Point étoile) Spécifie que toutes les URL doivent être redirigées. Si vous utilisez ce paramètre pour l'option **agentRules**, toutes les URL sont redirigées du côté agent, ce qui signifie que les URL sont ouvertes dans une application ou un poste de travail distant. Si vous utilisez ce paramètre pour l'option **clientRules**, les URL spécifiées sont redirigées vers le client. |
| `.*.acme.com;.*.exemple.com` | Spécifie que toutes les URL contenant le texte `.acme.com` ou `exemple.com` doivent être redirigées. |
| [espace ou laissez vide] | Pour spécifier qu'aucune URL ne doit être dirigée, utilisez un espace ou laissez le paramètre vide. Par exemple, laisser **clientRules** vide spécifie qu'aucune URL ne doit être redirigée vers le client. |

Pour **agentRules**, vous devez également utiliser l'option **brokerHostname** pour spécifier l'adresse IP ou le nom de domaine complet du Serveur de connexion, et vous devez utiliser l'option **remoteItem** pour spécifier le nom complet du pool de postes de travail ou d'applications, comme indiqué dans View Administrator.

## Redirection agent vers client

Ajoutez ce modèle au GPO pour un pool de postes de travail ou d'applications distant si vous voulez que certaines URL soient redirigées vers le client Windows.

Par exemple, la redirection agent vers client peut être utilisée pour conserver des ressources ou en tant que couche de sécurité supplémentaire. Si des employés travaillent sur une application ou un poste de travail distant et qu'ils veulent regarder des vidéos, par exemple, vous pouvez rediriger ces URL vers la machine cliente afin qu'aucune charge supplémentaire ne soit placée sur le centre de données. Ou bien, pour des raisons de sécurité, pour les employés qui travaillent à l'extérieur du réseau d'entreprise, vous pouvez préférer que toutes les URL qui pointent vers des emplacements externes au réseau d'entreprise soient ouvertes sur la propre machine cliente d'un employé.

Vous pouvez, par exemple, configurer des règles pour que le contenu non lié à l'entreprise, c'est-à-dire des URL qui ne pointent pas vers le réseau d'entreprise, soit redirigé pour s'ouvrir sur la machine cliente. Dans ce cas, vous pouvez utiliser les paramètres suivants, qui incluent des expressions régulières :

- Pour **agentRules** : `.*.mycompany.com`

  Cette règle signifie qu'une URL qui contient le texte **`mycompany.com`** doit être ouverte sur l'agent.

- Pour **clientRules** : `.*`

  Cette règle signifie que toutes les URL doivent être ouvertes sur le client, avec le navigateur client par défaut.

La fonctionnalité utilise le processus suivant pour appliquer les règles :

1. Lorsqu'un utilisateur clique sur un lien dans une application ou un poste de travail distant, les règles du client sont vérifiées en premier.
2. Si un modèle dans l'URL correspond à une règle de client, les règles d'agent sont vérifiées par la suite.
3. S'il existe un conflit entre les règles d'agent et les règles de client, le lien est ouvert localement, ce qui signifie dans ce cas sur la machine agent.
4. S'il n'y a pas de conflit, l'URL est redirigée vers le client.

   Dans l'exemple ci-dessus, il existe un conflit de règles, car les URL contenant **`mycompany.com`** sont un sous-ensemble de toutes les URL. À cause de ce conflit, les URL contenant **`mycompany.com`** sont ouvertes localement. Si vous cliquez sur un lien contenant **`mycompany.com`** dans l'URL alors que vous vous trouvez sur un poste de travail distant, l'URL sera ouverte sur ce poste de travail distant. Si vous cliquez sur un lien contenant **`mycompany.com`** dans l'URL alors que vous vous trouvez sur un système client, l'URL sera ouverte sur le client.

## Redirection client vers agent

Ajoutez ce modèle au GPO pour un groupe d'ordinateurs clients si vous voulez que certaines URL soient redirigées vers une application ou un poste de travail distant. Par exemple, pour des raisons de sécurité, vous pourriez vouloir que toutes les URL qui pointent vers le réseau d'entreprise soient ouvertes dans une application ou un poste de travail distant. Dans ce cas, vous pouvez régler **agentRules** sur :

```
.*.mycompany.com
```

Pour rediriger des URL vers un pool de postes de travail ou d'applications distant, vous devez également indiquer le pool à utiliser. Utilisez l'option **brokerHostname** pour spécifier l'adresse IP ou le nom de domaine complet du Serveur de connexion, et utilisez l'option **remoteItem** pour spécifier le nom complet du pool de postes de travail ou d'applications, comme indiqué dans View Administrator.

Si l'URL est redirigée vers un poste de travail distant, le lien est ouvert dans le navigateur par défaut pour ce poste de travail. Si l'URL est redirigée vers une application distante, le lien est ouvert à l'aide du pool d'applications spécifié. L'utilisateur final doit être autorisé à accéder au pool de postes de travail ou d'applications spécifié.

Vous pouvez ajouter ce modèle à des GPO pour l'agent et le client, mais si vous le faites, vérifiez que les règles ne sont pas en conflit ou que les conflits sont intentionnels.

## Détails du paramètre de modèle

Le tableau suivant décrit les paramètres de stratégie dans le fichier de modèle ADM de redirection de contenu URL Horizon. Le modèle ne contient que des paramètres Configuration d'ordinateur.

**Tableau 14-2.** Paramètres du modèle de redirection de contenu URL Horizon

| Paramètre | Propriétés |
|---|---|
| `IE Policy: Users can't disable URL Redirection plugin` | Détermine si les utilisateurs peuvent désactiver la redirection de contenu URL.<br>Ce paramètre est désactivé par défaut. |
| `IE Policy: Automatically activate newly installed plugins` | Détermine si les plug-ins Internet Explorer qui viennent d'être installés sont automatiquement activés.<br>Ce paramètre est désactivé par défaut. |
| `Url Redirection Enabled` | Détermine si cette fonctionnalité est activée.<br>Ce paramètre est activé par défaut. Vous pouvez utiliser ce paramètre pour désactiver la fonctionnalité même si le composant a été installé. |
| `Url Redirection Protocol 'http'` | Pour toutes les URL qui utilisent le protocole HTTP, spécifie les URL qui doivent être redirigées.<br>Par exemple, si vous définissez **agentRules** sur **`.*.mycompany.com`**, toutes les URL contenant « mycompany.com » sont redirigées vers une application ou un poste de travail distant. Vous pouvez en outre spécifier quel Serveur de connexion utiliser en définissant **brokerHostname**, et vous pouvez spécifier quel pool de postes de travail ou d'applications utiliser en définissant **remoteItem** sur le nom complet du pool, comme indiqué dans View Administrator.<br>Si vous définissez **clientRules** sur **`.*.mycompany.com`**, toutes les URL contenant « mycompany.com » sont redirigées vers le client Windows et ouvertes dans le navigateur par défaut sur le client.<br>**Remarque** Il est recommandé de définir les mêmes règles pour les protocoles HTTP et HTTPS. Ainsi, si un utilisateur saisit une URL partielle, telle que **`mycompany.com`** dans Internet Explorer, si ce site redirige automatiquement de HTTP vers HTTPS, la redirection de contenu URL fonctionnera comme prévu. Dans ce cas, si vous définissez une règle pour HTTPS, mais pas HTTP, l'URL partielle que l'utilisateur saisit n'est pas redirigée.<br>Ce paramètre est désactivé par défaut. |
| `Url Redirection Protocol 'https'` | Pour toutes les URL qui utilisent le protocole HTTPS, spécifie les URL qui doivent être redirigées.<br>Les options sont les mêmes que pour `Url Redirection Protocol 'http'`.<br>**Remarque** Il est recommandé de définir les mêmes règles pour les protocoles HTTPS et HTTP.<br>Ce paramètre est désactivé par défaut. |
| `Url Redirection Protocol 'callto'` | Pour toutes les URL qui utilisent le protocole callto, spécifie les URL qui doivent être redirigées.<br>Les options sont les mêmes que pour `Url Redirection Protocol 'http'`.<br>Ce paramètre est désactivé par défaut. |

**Tableau 14-2.** Paramètres du modèle de redirection de contenu URL Horizon (suite)

| Paramètre | Propriétés |
|---|---|
| `Url Redirection Protocol 'email'` | Pour toutes les URL qui utilisent le protocole email ou mailto, spécifie les URL qui doivent être redirigées.<br>Les options sont les mêmes que pour `Url Redirection Protocol 'http'`.<br>Ce paramètre est désactivé par défaut. |
| `Url Redirection Protocol '[...]'` | Il s'agit d'un modèle que vous pouvez modifier pour n'importe quel protocole supplémentaire. Si vous n'avez pas besoin de configurer des protocoles supplémentaires, vous pouvez supprimer ou commenter cette entrée avant d'ajouter le modèle d'administration à Active Directory. |

**Remarque** Pour la redirection client vers agent, si vous configurez un protocole sans gestionnaire par défaut, après avoir configuré un paramètre de GPO pour ce protocole, vous devez lancer Horizon Client une fois avant que les URL qui spécifient ce protocole soient redirigées.

# Configuration de l'Audio/Vidéo en temps réel

Audio/Vidéo en temps réel permet aux utilisateurs d'View d'exécuter Skype, Webex, Google Hangouts et d'autres applications de conférence en ligne sur leur poste de travail distant. Avec l'Audio/Vidéo en temps réel, les webcams et les périphériques audio qui sont connectés localement au système client sont redirigés vers le poste de travail distant. Cette fonctionnalité redirige les données vidéo et audio vers le poste de travail avec une bande passante beaucoup plus faible que celle utilisée par la redirection USB.

L'Audio/Vidéo en temps réel est compatible avec les applications de conférence standard et les applications vidéo basées sur navigateur, et prend en charge les webcams, les périphériques audio USB standard et l'entrée audio analogique.

Cette fonctionnalité installe une webcam virtuelle et un microphone virtuel VMware sur le système d'exploitation du poste de travail. La webcam virtuelle VMware utilise un pilote de webcam en mode noyau qui offre une compatibilité améliorée avec les applications vidéo basées sur un navigateur et avec d'autres logiciels de conférence tiers.

Lorsqu'une application de conférence ou vidéo est lancée, elle affiche et utilise ces périphériques virtuels VMware qui gèrent la redirection audio-vidéo à partir des périphériques connectés localement sur le client. La webcam et le microphone virtuels VMware s'affichent dans le Gestionnaire de périphériques sur le système d'exploitation du poste de travail.

Les pilotes des webcams et des périphériques audio doivent être installés sur vos systèmes Horizon Client pour permettre la redirection.

## Options de configuration de la fonctionnalité Audio-vidéo en temps réel

Lorsque vous installez Horizon Agent avec Audio/Vidéo en temps réel, la fonctionnalité s'utilise sur vos postes de travail View sans autre configuration. Il est recommandé d'utiliser les valeurs par défaut de la fréquence et de la résolution d'images pour la plupart des périphériques et applications courantes.

Vous pouvez configurer les paramètres de stratégie de groupe pour modifier ces valeurs par défaut et les adapter à des applications, webcams ou environnements particuliers. Vous pouvez également définir une stratégie pour désactiver ou activer la fonctionnalité. Un fichier de modèle d'administration ADM vous permet d'installer les paramètres de stratégie de groupe en matière d'audio-vidéo en temps réel sur Active Directory ou sur des postes de travail individuels. Reportez-vous à la section « Configuration des paramètres de stratégie de groupe de l'Audio/Vidéo en temps réel », page 225.

Si vous disposez de plusieurs webcams et périphériques d'entrée audio intégrés ou connectés à vos ordinateurs client, vous pouvez configurer des webcams et des périphériques d'entrée audio préférés qui seront redirigés vers vos postes de travail. Reportez-vous à la section « Sélection de webcams et microphones préférés », page 216.

**Remarque** Vous pouvez sélectionner un périphérique audio préféré, mais aucune autre option de configuration audio n'est disponible.

Lorsque les images de la webcam et l'entrée audio sont redirigées vers un poste de travail distant, vous ne pouvez pas accéder à la webcam et aux périphériques audio de l'ordinateur local. Inversement, lorsque ces périphériques sont utilisés sur l'ordinateur local, vous ne pouvez pas y accéder via le poste de travail distant.

Pour plus d'informations sur les applications prises en charge, consultez l'article de la base de connaissances VMware *Directives pour l'utilisation de l'Audio/Vidéo en temps réel avec des applications tierces sur les postes de travail Horizon View*, à l'adresse http://kb.vmware.com/kb/2053754.

## Configuration système requise pour l'Audio/Vidéo en temps réel

L'Audio/Vidéo en temps réel fonctionne avec des webcams standard, des périphériques audio USB et analogiques ainsi qu'avec les applications de conférence standard telles que Skype, WebEx et Google Hangouts. Pour prendre en charge l'Audio/Vidéo en temps réel, le déploiement de votre View doit satisfaire certaines exigences matérielles et logicielles.

**Poste de travail distant View**

Vous installez la fonctionnalité Audio/Vidéo en temps réel en installant View Agent 6.0 ou version ultérieure, ou Horizon Agent 7.0 ou version ultérieure. Cette fonctionnalité est prise en charge dans les pools de postes de travail qui sont déployés sur des machines virtuelles mono-utilisateur, mais pas dans les pools de postes de travail RDS. Reportez-vous à la section « Installer Horizon Agent sur une machine virtuelle », page 33.

**Logiciel Horizon Client**

Horizon Client 2.2 pour Windows ou versions ultérieures

Horizon Client 2.2 pour Linux ou version ultérieure. S'agissant de Horizon Client pour Linux 3.1 ou d'une version antérieure, cette fonctionnalité n'est disponible que pour la version de Horizon Client pour Linux fournie par des fournisseurs tiers. S'agissant de Horizon Client pour Linux 3.2 et versions ultérieures, cette fonction est également disponible pour les versions du client distribuées par VMware.

Horizon Client 2.3 pour Mac OS X ou version ultérieure

Horizon Client 4.0 pour iOS ou version ultérieure.

Horizon Client 4.0 pour Android ou version ultérieure.

**Ordinateur Horizon Client ou périphérique d'accès client**

- Tous les systèmes d'exploitation exécutant Horizon Client pour Windows.
- Tous les systèmes d'exploitation exécutant Horizon Client pour Linux sur des périphériques x86. Cette fonctionnalité n'est pas prise en charge par les processeurs ARM.
- Mac OS X Mountain Lion (10.8) et versions ultérieures. Elle est désactivée sur tous les systèmes d'exploitation Mac OS X antérieurs.
- Tous les systèmes d'exploitation exécutant Horizon Client pour iOS.
- Tous les systèmes d'exploitation exécutant Horizon Client pour Android.

- Pour plus d'informations sur les systèmes d'exploitation client pris en charge, reportez-vous au document *Utilisation de VMware Horizon Client* concernant le système ou périphérique approprié.
- Les pilotes des webcams et des périphériques audio doivent être installés, et la webcam ainsi que le périphérique audio doivent être opérationnels sur l'ordinateur client. Pour utiliser l'Audio/Vidéo en temps réel, vous n'avez pas à installer les pilotes des périphériques sur le système d'exploitation du poste de travail où l'agent est installé.

**Protocole d'affichage pour View**

- PCoIP
- VMware Blast (requiert Horizon Client 4.0 ou version ultérieure et Horizon Agent 7.0 ou version ultérieure)

L'Audio/Vidéo en temps réel n'est pas pris en charge par les sessions postes de travail RDP.

## Garantir que l'Audio/Vidéo en temps réel est utilisée plutôt que la redirection USB

Audio/Vidéo en temps réel prend en charge la redirection de webcam et d'entrée audio pour une utilisation dans des applications de conférence. La fonctionnalité Redirection USB qui peut être installée avec Horizon Agent ne prend pas en charge la redirection de webcam. Si vous redirigez des périphériques d'entrée audio au moyen de la redirection USB, le flux audio ne se synchronise pas correctement avec la vidéo pendant les sessions Audio/Vidéo en temps réel, et vous perdez l'avantage de la réduction de la demande sur la bande passante réseau. Vous pouvez prendre des mesures pour garantir que les webcams et les périphériques d'entrée audio sont redirigés vers vos postes de travail au moyen d'Audio/Vidéo en temps réel, et non avec Redirection USB.

Si vos postes de travail sont configurés avec la redirection USB, les utilisateurs finaux peuvent connecter et afficher leurs périphériques USB connectés localement en sélectionnant l'option **Connecter un périphérique USB** dans la barre de menus du client Windows ou dans le menu **Poste de travail > USB** du client Mac OS X. Les clients Linux bloquent la redirection USB des périphériques audio et vidéo par défaut et ne fournissent pas d'options de périphériques USB aux utilisateurs finaux.

Si l'utilisateur final sélectionne un périphérique USB dans le menu **Connecter un périphérique USB** ou la liste **Poste de travail > USB**, ce périphérique devient inutilisable pour la conférence vidéo ou audio. Par exemple, si un utilisateur passe un appel Skype, l'image de la vidéo peut ne pas s'afficher ou le flux audio peut être dégradé. Si un utilisateur final sélectionne un périphérique pendant une session de conférence, la redirection de webcam ou audio est interrompue.

Pour masquer ces périphériques aux utilisateurs finaux et éviter des perturbations potentielles, vous pouvez configurer les paramètres de la stratégie de groupe Redirection USB pour désactiver l'affichage des webcam et des périphériques d'entrée audio dans VMware Horizon Client.

Vous pouvez notamment créer des règles de filtrage de redirection USB pour Horizon Agent et spécifier les noms de famille de périphériques `audio-in` et `video` à désactiver. Pour plus d'informations sur la définition de stratégies de groupe et la spécification de règles de filtrage pour la redirection USB, reportez-vous à « Utilisation de règles pour contrôler la redirection USB », page 257.

**Avertissement** Si vous ne configurez pas de règles de filtrage de redirection USB pour désactiver des familles de périphériques USB, informez vos utilisateurs finaux qu'ils ne peuvent pas sélectionner des périphériques webcam ou audio dans le menu **Connecter un périphérique USB** ou la liste **Poste de travail > USB** dans la barre de menus de VMware Horizon Client.

## Sélection de webcams et microphones préférés

Si un ordinateur client dispose de plus d'une webcam et d'un microphone, vous pouvez configurer une webcam et un microphone par défaut que la fonctionnalité audio/vidéo en temps réel redirige vers le poste de travail. Ces périphériques peuvent être intégrés ou connectés à l'ordinateur client local.

Sur un ordinateur client Windows, vous sélectionnez une webcam préférée en définissant une clé de registre. Sur un ordinateur client Mac OS X, vous pouvez spécifier une webcam ou un microphone préféré à l'aide du système de valeurs par défaut de Mac OS X. Sur un ordinateur client Linux, vous pouvez spécifier une webcam ou un microphone préféré en modifiant un fichier de configuration. La fonctionnalité audio/vidéo en temps réel redirige la webcam préférée si elle est disponible. Autrement, la fonctionnalité audio/vidéo en temps réel utilise la première webcam énumérée par le système.

Pour sélectionner un microphone par défaut, vous pouvez configurer le contrôle Son dans le système d'exploitation Windows, Mac OS X ou Linux sur l'ordinateur client.

### Sélectionner un microphone par défaut sur un système client Windows

Si plusieurs microphones sont connectés à votre système client, un seul d'entre eux peut être utilisé sur votre poste de travail View. Pour spécifier le microphone par défaut, vous pouvez utiliser le contrôle du son de votre système client.

Avec la fonctionnalité Audio/Vidéo en temps réel, les périphériques d'entrée audio et les périphériques de sortie audio fonctionnent sans qu'il soit nécessaire d'utiliser la redirection USB, et la bande passante réseau nécessaire est considérablement réduite. Les périphériques d'entrée audio analogique sont également pris en charge.

---

**Important** Si vous utilisez un microphone USB, ne le connectez pas via le menu **Connecter un périphérique USB** d'Horizon Client. L'utilisation de redirection de périphériques USB dégrade les performances de la fonctionnalité Audio/Vidéo en temps réel.

---

#### Prérequis

- Assure-vous que vous disposez d'un microphone USB ou un autre type installé et opérationnel sur votre système client.
- Vérifiez que vous utilisez le protocole d'affichage VMware Blast ou PCoIP pour votre poste de travail distant.

#### Procédure

1. Si vous êtes en cours d'un appel, arrêtez l'appel.
2. Cliquez avec le bouton droit sur l'icône haut-parleur dans votre barre d'état système et sélectionnez **Périphériques d'enregistrement**.

   Vous pouvez également ouvrir le Contrôle du son à partir de du Panneau de configuration et cliquer sur l'onglet **Enregistrement**.
3. Dans l'onglet **Enregistrement** de la boîte de dialogue Son, cliquez avec le bouton droit sur le microphone que vous préférez utiliser.
4. Sélectionnez **Définir comme périphérique par défaut** et cliquez sur **OK**.
5. Démarrez un nouvel appel à partir de votre poste de travail View.

## Sélectionner une webcam préférée sur un système client Windows

Avec la fonctionnalité Audio-vidéo en temps réel, une seule des webcams de votre système client est utilisée sur votre poste de travail View. Vous pouvez définir une valeur de clé de registre pour spécifier la webcam préférée.

La webcam préférée est utilisée sur le poste de travail distant si elle est disponible. Sinon, une autre webcam est utilisée.

### Prérequis

- Assurez-vous qu'une webcam USB est installée et opérationnelle sur votre système client.
- Vérifiez que vous utilisez le protocole d'affichage VMware Blast ou PCoIP pour votre poste de travail distant.

### Procédure

1 Connectez la webcam que vous souhaitez utiliser.

2 Démarrez un appel, puis arrêtez l'appel.

Ce processus crée un fichier journal.

3 Ouvrez le fichier journal de débogage avec un éditeur de texte.

| Système d'exploitation | Emplacement du fichier journal |
|---|---|
| **Windows XP** | `C:\Documents and Settings\username\Local Settings\Application Data\VMware\VDM\Logs\debug-20`*`YY-MM-DD-XXXXXX`*`.txt` |
| **Windows 7 ou Windows 8** | `C:\Users\%username%\AppData\Local\VMware\VDM\Logs\debug-20`*`YY-MM-DD-XXXXXX`*`.txt` |

Le format du fichier journal est `debug-20`*`AA-MM-JJ-XXXXXX`*`.txt`, où 20 *AA* est l'année, *MM*le mois, *JJ* le jour et *XXXXXX* est un nombre.

4 Recherchez `[ViewMMDevRedir] VideoInputBase::LogDevEnum` dans le fichier journal pour trouver les entrées du fichier journal qui fait référence aux webcams connectées.

Voici un extrait du fichier journal identifiant la webcam Microsoft LifeCam HD-5000 :

```
[ViewMMDevRedir] VideoInputBase::LogDevEnum - 2 Device(s) found

[ViewMMDevRedir] VideoInputBase::LogDevEnum - Index=0 Name=Integrated Webcam
UserId=vid_1bcf&pid_2b83&mi_00#7&1b2e878b&0&0000   SystemId=\\?\usb#vid_1bcf&pid_2b83&mi_00#

[ViewMMDevRedir] VideoInputBase::LogDevEnum - Index=1 Name=Microsoft LifeCam HD-5000
UserId=vid_045e&pid_076d&mi_00#8&11811f49&0&0000  SystemId=\\?\usb#vid_045e&pid_076d&mi_00#
```

5 Copiez l'identificateur utilisateur de la webcam préférée.

Par exemple, copiez `vid_045e&pid_076d&mi_00#8&11811f49&0&0000` pour définir Microsoft LifeCam HD-5000 comme webcam par défaut.

6 Lancez l'éditeur du registre (`regedit.exe`) et accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\RTAV`.

7 Collez la partie de l'identificateur de la chaîne de caractères dans la valeur **srcWCamId**.

Par exemple, collez `vid_045e&pid_076d&mi_00#8&11811f49&0&0000` dans **srcWCamId**.

8 Enregistrez vos modifications et quittez le registre.

9 Démarrez un nouvel appel.

## Sélectionner un microphone par défaut sur un système client Mac OS X

Si plusieurs microphones sont connectés à votre système client, un seul d'entre eux peut être utilisé sur votre poste de travail distant. Vous pouvez spécifier le microphone par défaut à utiliser sur le poste de travail distant dans les Préférences système du système client.

Avec la fonctionnalité Audio/Vidéo en temps réel, les périphériques d'entrée audio et les périphériques de sortie audio fonctionnent sans qu'il soit nécessaire d'utiliser la redirection USB, et la bande passante réseau nécessaire est considérablement réduite. Les périphériques d'entrée audio analogique sont également pris en charge.

Cette procédure explique comment choisir un microphone par défaut dans l'interface utilisateur du système client. Les administrateurs peuvent également configurer un microphone préféré en utilisant le système de valeurs par défaut de Mac OS X. Reportez-vous à la section « Configurer une webcam ou un microphone préféré sur un système client Mac OS X », page 219.

---

**Important** Si vous utilisez un microphone USB, ne le connectez pas via le menu **Connexion > USB** d'Horizon Client. En effet, cette opération achemine le périphérique via la redirection USB, si bien qu'il ne pourra pas utiliser la fonctionnalité Audio/Vidéo en temps réel.

---

### Prérequis

- Assure-vous que vous disposez d'un microphone USB ou un autre type installé et opérationnel sur votre système client.
- Vérifiez que vous utilisez le protocole d'affichage VMware Blast ou PCoIP pour votre poste de travail distant.

### Procédure

1 Sur votre système client, sélectionnez **Menu Apple > Préférences système**, puis cliquez sur **Son**.

2 Ouvrez le volet Entrée des préférences de son.

3 Sélectionnez le microphone de votre choix.

Ainsi, dès que vous vous connecterez à un poste de travail distant et effectuerez un appel, le poste de travail utilisera le microphone que vous avez sélectionné sur le système client.

## Configuration de la fonctionnalité Audio/Vidéo en temps réel sur un client Mac OS X

Vous pouvez configurer les paramètres Audio/Vidéo en temps réel sur la ligne de commande en utilisant le système de valeurs par défaut de Mac OS X. Le système de valeurs par défaut vous permet de lire, d'écrire et de supprimer des valeurs d'utilisateur par défaut Mac OS X à l'aide de l'application Terminal (`/Applications/Utilities/Terminal.app`).

Les valeurs par défaut de Mac OS X appartiennent à des domaines. Les domaines correspondent généralement à des applications individuelles. Le domaine de la fonctionnalité Audio/Vidéo en temps réel est com.vmware.rtav.

### Syntaxe de configuration de la fonctionnalité Audio/Vidéo en temps réel

Pour configurer la fonctionnalité Audio/Vidéo en temps réel, vous pouvez utiliser les commandes suivantes.

**Tableau 14-3.** Syntaxe des commandes de configuration de la fonctionnalité Audio/Vidéo en temps réel

| vdmadmin | Description |
|---|---|
| `defaults write com.vmware.rtav scrWCamId "`*webcam-userid*`"` | Définit la webcam préférée à utiliser sur des postes de travail distants. Si cette valeur n'est pas définie, la webcam est automatiquement sélectionnée par l'énumération système. Vous pouvez spécifier n'importe quelle webcam connectée (ou intégrée) au système client. |
| `defaults write com.vmware.rtav srcAudioInId "`*audio-device-userid*`"` | Définit le microphone (périphérique d'entrée audio) préféré à utiliser sur des postes de travail distants. Si cette valeur n'est pas définie, les postes de travail distants utilisent le périphérique d'enregistrement par défaut du système client. Vous pouvez spécifier n'importe quel microphone connecté (ou intégré) au système client. |
| `defaults write com.vmware.rtav srcWCamFrameWidth`*pixels* | Définit la largeur de l'image. La valeur par défaut est une valeur codée en dur de 320 pixels. Vous pouvez modifier la largeur de l'image par n'importe quelle valeur de pixel. |
| `defaults write com.vmware.rtav srcWCamFrameHeight`*pixels* | Définit la hauteur de l'image. La valeur par défaut est une valeur codée en dur de 240 pixels. Vous pouvez modifier la hauteur de l'image par n'importe quelle valeur de pixel. |
| `defaults write com.vmware.rtav srcWCamFrameRate`*fps* | Définit la fréquence d'images. La valeur par défaut est de 15 ips. Vous pouvez modifier la fréquence d'images par n'importe quelle valeur. |
| `defaults write com.vmware.rtav LogLevel "`*level*`"` | Définit le niveau de journalisation du fichier journal de la fonctionnalité Audio/Vidéo en temps réel (`~/Library/Logs/VMware/vmware-RTAV-`*`pid`*`.log`). Vous pouvez définir le niveau de journalisation sur le suivi ou le débogage. |
| `defaults write com.vmware.rtav IsDisabled`*value* | Détermine si la fonctionnalité Audio/Vidéo en temps réel est activée ou désactivée. La fonctionnalité Audio/Vidéo en temps réel est activée par défaut. (Cette valeur n'est pas appliquée.) Pour désactiver la fonctionnalité Audio/Vidéo en temps réel sur le client, définissez la valeur sur True. |
| `defaults read com.vmware.rtav` | Affiche les paramètres de configuration de la fonctionnalité Audio/Vidéo en temps réel. |
| `defaults delete com.vmware.rtav`*setting* | Supprime un paramètre de configuration de la fonctionnalité Audio/Vidéo en temps réel. Par exemple : `defaults delete com.vmware.rtav srcWCamFrameWidth` |

**Remarque** Vous pouvez définir une fréquence d'images comprise entre 1 et 25 ips et une résolution maximale de 1 920 x 1 080. Une résolution élevée à une fréquence d'images rapide peut ne pas être prise en charge par tous les périphériques de vos environnements.

## Configurer une webcam ou un microphone préféré sur un système client Mac OS X

Avec la fonctionnalité Audio/Vidéo en temps réel, si vous disposez de plusieurs webcams et microphones sur votre système client, vous ne pouvez en utiliser qu'un seul sur votre poste de travail distant. Vous pouvez spécifier vos webcam et microphone préférés sur la ligne de commande en utilisant le système de valeurs par défauts de Mac OS X.

Avec la fonctionnalité Audio/Vidéo en temps réel, les webcams, les périphériques d'entrée audio et les périphériques de sortie audio fonctionnent sans nécessiter l'utilisation de la redirection USB, et la bande passante du réseau nécessaire est considérablement réduite. Les périphériques d'entrée audio analogique sont également pris en charge.

Dans la plupart des environnements, il n'est pas nécessaire de configurer une webcam ou un microphone préféré. Si vous ne définissez pas de microphone préféré, les postes de travail distants utilisent le périphérique audio par défaut défini dans les Préférences systèmes du système client. Reportez-vous à

« Sélectionner un microphone par défaut sur un système client Mac OS X », page 218. Si vous ne configurez pas de webcam préférée, les postes de travail distants sélectionnent la webcam par énumération.

### Prérequis

- Si vous configurez une webcam USB préférée, vérifiez que cette dernière est installée et opérationnelle sur le système client.
- Si vous configurez un microphone USB (ou un autre type) préféré, vérifiez que ce dernier est installé et opérationnel sur le système client.
- Vérifiez que vous utilisez le protocole d'affichage VMware Blast ou PCoIP pour votre poste de travail distant.

### Procédure

1 Sur votre système client Mac OS X, démarrez une application de webcam ou de microphone pour déclencher une énumération des périphériques de caméra ou audio dans le fichier journal de la fonctionnalité Audio/Vidéo en temps réel.

   a Connectez la webcam ou le périphérique audio.

   b Dans le dossier **Applications**, double-cliquez sur **VMware Horizon View Client** ( Horizon Client 3.0) ou **VMware Horizon Client** (Horizon Client 3.1 et version ultérieure) pour démarrer Horizon Client.

   c Démarrez un appel, puis arrêtez-le.

2 Recherchez les entrées de journal correspondant à la webcam ou au microphone dans le fichier journal de la fonctionnalité Audio/Vidéo en temps réel.

   a Dans un éditeur de texte, ouvrez le fichier journal de la fonctionnalité Audio/Vidéo en temps réel.

      Le fichier journal de la fonctionnalité Audio/Vidéo en temps réel se nomme `~/Library/Logs/VMware/vmware-RTAV-`*`pid`*`.log`, où *pid* est l'ID de processus de la session actuelle.

   b Recherchez dans le fichier journal de la fonctionnalité Audio/Vidéo en temps réel les entrées qui identifient les webcams ou microphones connectés.

   L'exemple suivant montre comment les entrées de webcam peuvent s'afficher dans le fichier journal de la fonctionnalité Audio/Vidéo en temps réel :

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() -
1 Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() -
Name=FaceTime HD Camera (Built-in)   UserId=FaceTime HD Camera (Built-
in)#0xfa20000005ac8509   SystemId=0xfa20000005ac8509
```

   L'exemple suivant montre comment les entrées de microphone peuvent s'afficher dans le fichier journal de la fonctionnalité Audio/Vidéo en temps réel :

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: int
AVCaptureEnumerateAudioDevices(MMDev::DeviceList&) -
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum()
- 2 Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum()
- Index=255   Name=Built-in Microphone   UserId=Built-in Microphone#AppleHDAEngineInput:1B,
```

```
0,1,0:1   SystemId=AppleHDAEngineInput:1B,0,1,0:1
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum()
- Index=255   Name=Built-in Input   UserId=Built-in Input#AppleHDAEngineInput:1B,0,1,1:2
SystemId=AppleHDAEngineInput:1B,0,1,1:2
```

3 Recherchez dans le fichier journal de la fonctionnalité Audio/Vidéo en temps réel la webcam ou le microphone que vous préférez et notez son ID d'utilisateur.

   L'ID d'utilisateur est affiché dans le fichier journal après la chaîne UserId=. Par exemple, l'ID d'utilisateur de la caméra FaceTime interne est « FaceTime HD Camera (Built-in) » et celui du microphone interne est « Built-in Microphone ».

4 Dans Terminal (`/Applications/Utilities/Terminal.app`), utilisez la commande `defaults write` pour définir la webcam ou le microphone préféré.

| Option | Action |
|---|---|
| **Définir la webcam préférée** | Tapez **`defaults write com.vmware.rtav srcWCamId "webcam-userid"`**, où *webcam-userid* correspond à l'ID d'utilisateur de la webcam préférée que vous pouvez trouver dans le fichier journal de la fonctionnalité Audio/Vidéo en temps réel. Par exemple : `defaults write com.vmware.rtav srcWCamId "HD Webcam C525”` |
| **Définir le microphone préféré** | Tapez **`defaults write com.vmware.rtav srcAudioInId "audio-device-userid"`**, où *audio-device-userid* correspond à l'ID d'utilisateur du microphone préféré que vous pouvez trouver dans le fichier journal de la fonctionnalité Audio/Vidéo en temps réel. Par exemple : `defaults write com.vmware.rtav srcAudioInId "Built-in Microphone"` |

5 (Facultatif) Utilisez la commande `defaults read` pour vérifier les modifications que vous avez apportées à la fonctionnalité Audio/Vidéo en temps réel.

   Par exemple : **`defaults read com.vmware.rtav`**

   Cette commande répertorie l'ensemble des paramètres de la fonctionnalité Audio/Vidéo en temps réel.

Désormais, lors de la connexion à un poste de travail distant ou du démarrage d'un appel, le poste de travail utilisera la webcam ou le microphone préféré que vous avez configurés, s'ils sont disponibles. S'ils ne sont pas disponibles, le poste de travail distant pourra utiliser une autre webcam ou un autre microphone disponible.

## Sélectionner un microphone par défaut sur un système client Linux

Si plusieurs microphones sont connectés à votre système client, un seul d'entre eux peut être utilisé sur votre poste de travail View. Pour spécifier le microphone par défaut, vous pouvez utiliser le contrôle du son de votre système client.

Avec la fonctionnalité Audio/Vidéo en temps réel, les périphériques d'entrée audio et les périphériques de sortie audio fonctionnent sans qu'il soit nécessaire d'utiliser la redirection USB, et la bande passante réseau nécessaire est considérablement réduite. Les périphériques d'entrée audio analogique sont également pris en charge.

Cette procédure explique comment sélectionner un microphone par défaut depuis l'interface utilisateur du système client. Les administrateurs peuvent également configurer un microphone préféré en modifiant un fichier de configuration. Reportez-vous à la section « Sélectionner une webcam ou un microphone préféré sur un système client Linux », page 222.

### Prérequis

- Assure-vous que vous disposez d'un microphone USB ou un autre type installé et opérationnel sur votre système client.
- Vérifiez que vous utilisez le protocole d'affichage VMware Blast ou PCoIP pour votre poste de travail distant.

### Procédure

1 Dans l'interface graphique Ubuntu, sélectionnez **Système > Préférences > Son**.

   Vous pouvez également cliquer sur l'icône **Son** à droite de la barre d'outils en haut de l'écran.

2 Cliquez sur l'onglet **Entrée** dans la boîte de dialogue Préférences de son.

3 Sélectionnez le périphérique préféré et cliquez sur **Fermer**.

## Sélectionner une webcam ou un microphone préféré sur un système client Linux

Avec la fonctionnalité Audio/Vidéo en temps réel, si vous disposez de plusieurs webcams et microphones sur votre système client, vous ne pouvez en utiliser qu'un seul sur votre poste de travail View. Pour désigner la webcam et le microphone préférés, vous pouvez modifier un fichier de configuration.

Selon sa disponibilité, la webcam ou le microphone préféré est utilisé sur le poste de travail View ; sinon, une autre webcam ou un autre microphone sera utilisé.

Avec la fonctionnalité Audio/Vidéo en temps réel, les webcams, les périphériques d'entrée audio et les périphériques de sortie audio fonctionnent sans nécessiter l'utilisation de la redirection USB, et la bande passante du réseau nécessaire est considérablement réduite. Les périphériques d'entrée audio analogique sont également pris en charge.

Pour définir les propriétés dans le fichier `/etc/vmware/config` et indiquer un périphérique préféré, vous devez déterminer l'ID du périphérique.

- Pour les webcams, affectez à la propriété `rtav.srcWCamId` la valeur de la description de webcam figurant dans le fichier journal, comme indiqué dans la procédure suivante.
- Pour les périphériques audio, affectez à la propriété `rtav.srcAudioInId` la valeur du champ Pulse Audio `device.description`.

  Recherchez cette valeur dans le fichier journal, comme indiqué dans la procédure suivante.

### Prérequis

Selon que vous configurez une webcam préférée, un micro préféré ou les deux, exécutez les tâches préalables appropriées :

- Assurez-vous qu'une webcam USB est installée et opérationnelle sur votre système client.
- Assure-vous que vous disposez d'un microphone USB ou un autre type installé et opérationnel sur votre système client.
- Vérifiez que vous utilisez le protocole d'affichage VMware Blast ou PCoIP pour votre poste de travail distant.

### Procédure

1 Lancez le client et démarrez une application de webcam ou de microphone pour déclencher une énumération de périphériques vidéo ou audio dans le journal client.

   a Connectez la webcam ou le périphérique audio que vous souhaitez utiliser.

   b Utilisez la commande `vmware-view` pour démarrer Horizon Client.

   c Démarrez un appel, puis arrêtez-le.

   Ce processus crée un fichier journal.

2 Recherchez les entrées relatives à la webcam ou au microphone.

a Ouvrez le fichier journal de débogage avec un éditeur de texte.

Le fichier journal contenant les messages audio-vidéo en temps réel se trouve dans `/tmp/vmware-<username>/vmware-RTAV-<pid>.log`. Le journal client se trouve dans `/tmp/vmware-<username>/vmware-view-<pid>.log`.

b Recherchez dans le fichier journal les entrées qui renvoient aux webcams et aux microphones raccordés.

L'exemple suivant montre un extrait de la sélection de webcams :

```
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - 3 Device(s) found
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=UVC Camera (046d:
0819)   UserId=UVC Camera (046d:0819)#/sys/devices/pci0000:00/0000:00:1a.
7/usb1/1-3/1-3.4/1-3.4.5   SystemId=/dev/video1
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=gspca main driver
UserId=gspca main driver#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.4/1-3.4.7
SystemId=/dev/video2
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=Microsoft®
LifeCam HD-6000 for Notebooks   UserId=Microsoft® LifeCam HD-6000 for
Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6   SystemId=/dev/video0
main| W110: RTAV: static bool AudioCaptureLin::EnumCaptureDevices(MMDev::DeviceList&) -
enumeration data unavailable
```

L'exemple suivant montre un extrait de la sélection de périphériques audio et le niveau sonore actuel de chacun d'entre eux :

```
vthread-18| I120: RTAV: bool AudioCaptureLin::TriggerEnumDevices() - Triggering
enumeration
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - PulseAudio Get Source (idx=1 'alsa_output.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-stereo.monitor' 'Monitor of Logitech USB
Headset Analog Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - channel:0 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - channel:1 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - PulseAudio Get Source (idx=2 'alsa_input.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-mono' 'Logitech USB Headset Analog Mono')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - channel:0 vol:98304
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - PulseAudio Get Source (idx=3 'alsa_output.usb-
Microsoft_Microsoft_LifeChat_LX-6000-00-LX6000.analog-stereo.monitor' 'Monitor of
Microsoft LifeChat LX-6000 Analog Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*,
const pa_source_info*, int, void*) - channel:0 vol:65536
```

Des avertissements s'affichent si l'un des niveaux sonores source du périphérique sélectionné ne respecte pas les critères PulseAudio lorsque la source n'est pas définie à 100 % (0 dB) ou si le périphérique source sélectionné est muet :

```
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel volume: 0:  67%
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel is muted
```

3 Copiez la description du périphérique et utilisez-la pour définir la propriété appropriée dans le fichier `/etc/vmware/config`.

Pour un exemple de webcam, copiez `Microsoft® LifeCam HD-6000 for Notebooks` afin de désigner la webcam Microsoft comme webcam préférée et définissez la propriété comme suit :

```
rtav.srcWCamId="Microsoft® LifeCam HD-6000 for Notebooks"
```

Dans cet exemple, vous pourriez aussi définir la propriété sur `rtav.srcWCamId="Microsoft"`.

Pour un exemple de périphérique audio, copiez `Logitech USB Headset Analog Mono` pour désigner le casque Logitech comme périphérique audio préféré et définissez la propriété comme suit :

```
rtav.srcAudioInId="Logitech USB Headset Analog Mono"
```

4 Enregistrez les modifications et fermez le fichier de configuration `/etc/vmware/config`.

5 Fermez la session du poste de travail et démarrez une nouvelle session.

## Configuration des paramètres de stratégie de groupe de l'Audio/Vidéo en temps réel

Vous pouvez configurer les paramètres de stratégie de groupe qui permettent de contrôler le comportement de l'Audio/Vidéo en temps réel (RTAV) sur vos postes de travail View. Ces paramètres définissent la fréquence et la résolution d'images maximales d'une webcam virtuelle. Ces paramètres vous permettent de définir la bande passante maximale qu'un utilisateur peut utiliser. Un paramètre supplémentaire permet de désactiver/activer la fonctionnalité Audio/Vidéo en temps réel (RTAV).

Vous n'avez pas à configurer ces paramètres de stratégie. L'Audio/Vidéo en temps réel utilise la fréquence et la résolution d'images qui sont fixées pour la webcam des systèmes client. Les paramètres par défaut sont recommandés pour la plupart des applications webcam et audio.

Pour voir des exemples d'utilisation de bande passante pour l'Audio/Vidéo en temps réel, reportez-vous à « Bande passante de l'Audio/Vidéo en temps réel », page 228.

Ces paramètres de stratégie affectent vos postes de travail View et non les systèmes client auxquels les périphériques physiques sont connectés. Pour configurer ces paramètres sur vos postes de travail, ajoutez le fichier de modèle d'administration (ADM) de stratégie de groupe pour l'Audio/Vidéo en temps réel (RTAV) dans Active Directory.

Pour plus d'informations sur la configuration des paramètres sur les systèmes clients, consultez l'article de la base de connaissances VMware *Configuration de la fréquence et de la résolution d'images pour l'Audio/Vidéo en temps réel sur les clients Horizon View*, à l'adresse http://kb.vmware.com/kb/2053644.

## Ajouter le modèle d'administration (ADM) pour l'Audio/Vidéo en temps réel (RTAV) dans Active Directory et configurer les paramètres

Vous pouvez ajouter les paramètres de stratégie au fichier RTAV ADM, `vdm_agent_rtav.adm`, aux objets de stratégie de groupe (GPO) dans Active Directory, et configurer les paramètres dans l'Éditeur d'objets de stratégie de groupe.

### Prérequis

- Vérifiez que l'option de configuration RTAV est installée sur vos postes de travail. Cette option de configuration est installée par défaut mais peut être désélectionnée pendant l'installation. Les paramètres n'ont aucun effet si RTAV n'est pas installé. Reportez-vous à la section « Installer Horizon Agent sur une machine virtuelle », page 33.
- Vérifiez que les objets de stratégie de groupe (GPO) dans Active Directory sont créés pour les paramètres de stratégie de groupe RTAV. Les objets de stratégie de groupe (GPO) doivent être liés à l'unité d'organisation (UO) qui contient vos postes de travail. Reportez-vous à la section « Exemple de stratégie de groupe Active Directory », page 347.
- Vérifiez que les composants logiciels enfichables Microsoft MMC (Microsoft Management Console) et l'Éditeur d'objets de stratégie de groupe sont disponibles sur votre serveur Active Directory.
- Familiarisez-vous avec les paramètres de stratégie de groupe RTAV. Reportez-vous à la section « Paramètres de stratégie de groupe de l'Audio/Vidéo en temps réel », page 227.

### Procédure

1. Téléchargez le fichier View GPO Bundle `.zip` sur le site de téléchargement de VMware à l'adresse https://my.vmware.com/web/vmware/downloads.

   Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut GPO Bundle.

   Le fichier se nomme `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip`, où *x.x.x* est la version et *yyyyyyy* le numéro de build. Tous les fichiers ADM et ADMX qui fournissent des paramètres de stratégie de groupe pour View sont disponibles dans ce fichier.
2. Décompressez le fichier `VMware-Horizon-View-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip` et copiez le fichier RTAV ADM, `vdm_agent_rtav.adm`, dans votre serveur Active Directory.
3. Sur le serveur Active Directory, modifiez les objets de stratégie de groupe (GPO) en sélectionnant **Démarrer > Outils d'administration > Gestion de stratégie de groupe**, puis en cliquant avec le bouton droit sur GPO et en sélectionnant **Édition**.
4. Dans l'Éditeur d'objets de stratégie de groupe, cliquez avec le bouton droit sur le dossier **Configuration de l'ordinateur > Modèles d'administration**, puis sélectionnez **Ajout/Suppression de modèles**.
5. Cliquez sur **Ajouter**, localisez le fichier `vdm_agent_rtav.adm` et cliquez sur **Ouvrir**.
6. Cliquez sur **Fermer** pour appliquer les paramètres de stratégie dans le fichier de modèle d'administration pour les objets de stratégie de groupe (GPO).

   Les paramètres se trouvent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Modèles d'administration classiques > Configuration de VMware Horizon Agent > Configuration de VMware View Agent**.
7. Configurer les paramètres de stratégie de groupe RTAV.

## Paramètres de stratégie de groupe de l'Audio/Vidéo en temps réel

Les paramètres de la stratégie de groupe Audio/Vidéo en temps réel (RTAV) contrôlent la fréquence et la résolution maximales des images d'une webcam virtuelle. Un paramètre supplémentaire permet de désactiver ou d'activer la fonctionnalité RTAV. Ces paramètres de stratégie affectent les postes de travail View, et non les systèmes clients sur lesquels les périphériques physiques sont connectés.

Si vous ne configurez pas les paramètres de la stratégie de groupe RTAV, RTAV utilise les valeurs qui sont définies sur les systèmes clients. Sur les systèmes clients, la fréquence d'images par défaut de la webcam est de 15 images par seconde. La résolution d'image par défaut de la webcam est de 320 x 240 pixels.

Les paramètres de stratégie de groupe **Résolution - ... d'image max...** déterminent les valeurs maximales pouvant être utilisées. La fréquence d'images et la résolution d'image qui sont définies sur les systèmes clients sont des valeurs absolues. Par exemple, si vous configurez les paramètres RTAV pour une résolution d'image maximale de 640 x 480 pixels, la webcam affiche n'importe quelle résolution qui est définie sur le client jusqu'à 640 x 480 pixels. Si vous définissez la résolution d'image sur le client sur une valeur supérieure à 640 x 480 pixels, la résolution du client est limitée à 640 x 480 pixels.

Toutes les configurations ne peuvent pas atteindre les valeurs maximales de la stratégie de groupe, à savoir une résolution de 1920 x 1080 à 25 images par seconde. La fréquence d'images maximale que votre configuration peut atteindre pour une résolution donnée dépend de la webcam utilisée, du matériel du système client, du matériel virtuel d'Horizon Agent et de la bande passante disponible.

Les paramètres de la stratégie du groupe **Résolution - ... d'image par défaut...** déterminent les valeurs par défaut qui sont utilisées lorsque les valeurs de résolution ne sont pas définies par l'utilisateur.

| Paramètre de stratégie de groupe | Description |
|---|---|
| Désactiver RTAV | Lorsque vous activez ce paramètre, la fonctionnalité Audio/Vidéo en temps réel est désactivée.<br>Lorsque ce paramètre n'est pas configuré ou est désactivé, Audio/Vidéo en temps réel est activé.<br>Ce paramètre se trouve dans le dossier **Configuration RTAV de View**. |
| Nombre maximal d'images par seconde | Détermine le nombre maximal d'images par seconde auquel la webcam peut capturer des images. Vous pouvez utiliser ce paramètre pour limiter la fréquence d'images de la webcam dans des environnements à faible bande passante réseau.<br>La valeur minimale est d'une image par seconde. La valeur maximale est de 25 images par seconde.<br>Lorsque ce paramètre n'est pas configuré ou est désactivé, aucune fréquence d'images maximale n'est définie. Audio/Vidéo en temps réel utilise la fréquence d'images qui est sélectionnée pour la webcam sur le système client.<br>Par défaut, les webcams clientes ont une fréquence d'images de 15 images par seconde. Si aucun paramètre n'est configuré sur le système client et si le paramètre **Nombre maximal d'images par seconde** n'est pas configuré ou est désactivé, la webcam capture 15 images par seconde.<br>Ce paramètre se trouve dans le dossier **Configuration RTAV de View > Paramètres RATV de la webcam View**. |
| Résolution - Largeur d'image maximale en pixels | Détermine la largeur maximale, en pixels, des images capturées par la webcam. En définissant une faible largeur maximale d'image, vous pouvez diminuer la résolution des images capturées et ainsi améliorer l'expérience de visualisation dans les environnements réseau à faible bande passante.<br>Lorsque ce paramètre n'est pas configuré ou est désactivé, la largeur maximale d'image n'est pas définie. RTAV utilise la largeur d'image définie sur le système client. La largeur par défaut d'une image de webcam sur un système client est de 320 pixels.<br>La limite maximale d'une image de webcam est de 1 920 x 1 080 pixels. Si vous configurez ce paramètre avec une valeur supérieure à 1 920 pixels, la largeur d'image maximale effective est de 1 920 pixels.<br>Ce paramètre se trouve dans le dossier **Configuration RTAV de View > Paramètres RATV de la webcam View**. |

| Paramètre de stratégie de groupe | Description |
|---|---|
| Résolution - Hauteur maximale d'image en pixels | Détermine la hauteur maximale, en pixels, des images capturées par la webcam. En définissant une faible hauteur maximale d'image, vous pouvez diminuer la résolution des images capturées et ainsi améliorer l'expérience de visualisation dans des environnements réseau à faible bande passante.<br>Lorsque ce paramètre n'est pas configuré ou est désactivé, la hauteur maximale d'image n'est pas définie. RTAV utilise la hauteur d'image définie sur le système client. La hauteur par défaut d'une image de webcam sur un système client est de 240 pixels.<br>La limite maximale d'une image de webcam est de 1 920 x 1 080 pixels. Si vous configurez ce paramètre avec une valeur supérieure à 1 080 pixels, la hauteur d'image maximale effective est de 1 080 pixels.<br>Ce paramètre se trouve dans le dossier **Configuration RTAV de View > Paramètres RATV de la webcam View**. |
| Résolution - Largeur de résolution d'image par défaut en pixels | Détermine la largeur de la résolution par défaut, en pixels, des images capturées par la webcam. Ce paramètre est utilisé lorsqu'aucune valeur de résolution n'est définie par l'utilisateur.<br>Lorsque ce paramètre n'est pas configuré ou est désactivé, la largeur d'image par défaut est de 320 pixels.<br>La valeur qui est configurée par ce paramètre de stratégie s'applique uniquement si View Agent 6.0 ou version ultérieure et Horizon Client 3.0 ou version ultérieure sont utilisés. Pour des versions plus anciennes de View Agent et d'Horizon Client, ce paramètre de stratégie n'a aucun effet et la largeur d'image par défaut est de 320 pixels.<br>Ce paramètre se trouve dans le dossier **Configuration RTAV de View > Paramètres RATV de la webcam View**. |
| Résolution - Hauteur de la résolution d'image par défaut en pixels | Détermine la hauteur de la résolution par défaut, en pixels, des images capturées par la webcam. Ce paramètre est utilisé lorsqu'aucune valeur de résolution n'est définie par l'utilisateur.<br>Lorsque ce paramètre n'est pas configuré ou est désactivé, la hauteur d'image par défaut est de 240 pixels.<br>La valeur qui est configurée par ce paramètre de stratégie s'applique uniquement si View Agent 6.0 ou version ultérieure et Horizon Client 3.0 ou version ultérieure sont utilisés. Pour les versions plus anciennes de View Agent et d'Horizon Client, ce paramètre de stratégie n'a aucun effet et la hauteur d'image par défaut est de 240 pixels.<br>Ce paramètre se trouve dans le dossier **Configuration RTAV de View > Paramètres RATV de la webcam View**. |

## Bande passante de l'Audio/Vidéo en temps réel

La bande passante de la fonctionnalité Audio/Vidéo en temps réel varie selon la résolution et la fréquence d'image de la webcam, ainsi que des données images et audio en cours de capture.

Les exemples de tests présentés dans Tableau 14-4 mesurent la bande passante que la fonctionnalité Audio/Vidéo en temps réel utilise dans un environnement View avec une webcam et des périphériques d'entrée vidéo standard. Les tests mesurent la bande passante permettant d'envoyer des données vidéo et audio d'Horizon Client à Horizon Agent. La bande passante totale requise pour exécuter une session de poste de travail à partir d'Horizon Client peut être supérieure à ces chiffres. Au cours de ces tests, la webcam capture des images à 15 images/seconde pour la résolution de chaque image.

**Tableau 14-4.** Résultats de l'exemple de bande passante pour envoyer des données Audio/Vidéo en temps réel d' Horizon Client à Horizon Agent

| Résolution de l'image (largeur x hauteur) | Bande passante utilisée (Kbits/s) |
|---|---|
| 160 x 120 | 225 |
| 320 x 240 | 320 |
| 640 x 480 | 600 |

# Configuration de la redirection de scanner

La redirection de scanner permet aux utilisateurs de View d'analyser les informations qui se trouvent sur leurs applications et postes de travail distants à l'aide de périphériques d'analyse et d'acquisition d'images connectés localement à leurs ordinateurs clients. La redirection de scanner est disponible dans Horizon 6.0.2 et versions ultérieures.

La redirection de scanner prend en charge les périphériques d'analyse et d'acquisition d'images standard compatibles avec les formats TWAIN et WIA.

Une fois que vous avez installé Horizon Agent avec l'option de configuration Redirection de scanner, la fonctionnalité est opérationnelle sur vos applications et postes de travail distants, sans configuration supplémentaire. Vous n'avez besoin de configurer aucun pilote spécifique au scanner sur les applications ou postes de travail distants.

Vous pouvez configurer les paramètres de stratégie de groupe et modifier les valeurs par défaut pour les adapter à des environnements ou applications d'acquisition d'images spécifiques. Vous pouvez également définir une stratégie pour désactiver ou activer la fonctionnalité. Un fichier de modèle d'administration vous permet d'installer des paramètres de stratégie de groupe de redirection de scanner dans Active Directory ou sur des postes de travail individuels. Reportez-vous à la section « Configuration des paramètres de stratégie de groupe de redirection de scanner », page 231.

Lorsque les données d'analyse sont redirigées vers une application ou un poste de travail distant, vous ne pouvez pas accéder au périphérique d'analyse ou d'acquisition d'images sur l'ordinateur local. Inversement, lorsqu'un périphérique est utilisé sur l'ordinateur local, vous ne pouvez pas y accéder via l'application ou le poste de travail distant.

## Configuration système requise pour la redirection de scanner

Pour prendre en charge la redirection de scanner, le déploiement de votre View doit répondre à certaines exigences matérielles et logicielles.

**Application ou poste de travail distant View**

Cette fonctionnalité est prise en charge sur les postes de travail RDS, les applications RDS et les postes de travail VDI déployés sur des machines virtuelles mono-utilisateur.

Vous devez installer View Agent 6.0.2 ou une version ultérieure sur les machines virtuelles parentes ou modèles, ou sur les hôtes RDS, et sélectionner l'option de configuration de redirection de scanner.

Sur les systèmes d'exploitation de poste de travail Windows et invités Windows Server, l'option de configuration de redirection de scanner d'Horizon Agent est désélectionnée par défaut.

Les systèmes d'exploitation invités suivants sont pris en charge sur les machines virtuelles mono-utilisateur et, si indiqué, sur les hôtes RDS :

- Windows 7 32 ou 64 bits
- Windows 8 32 ou 64 bits.*x*
- Windows 10 32 ou 64 bits
- Windows Server 2008 R2 configuré en tant que poste de travail ou hôte RDS

| | |
|---|---|
| | ■ Windows Server 2012 R2 configuré en tant que poste de travail ou hôte RDS<br><br>**IMPORTANT** La fonctionnalité Expérience de poste de travail doit être installée sur les systèmes d'exploitation invités Windows Server, qu'ils soient configurés en tant que postes de travail ou hôtes RDS.<br><br>Les pilotes du scanner n'ont pas à être installés sur le système d'exploitation du poste de travail où Horizon Agent est installé. |
| **Logiciel Horizon Client** | Horizon Client 3.2 pour Windows ou version ultérieure |
| **Ordinateur Horizon Client ou périphérique d'accès client** | Systèmes d'exploitation pris en charge :<br>■ Windows 7 32 ou 64 bits<br>■ Windows 8 32 ou 64 bits.*x*<br>■ Windows 10 32 ou 64 bits<br><br>Les pilotes du scanner doivent être installés, et ce dernier doit être opérationnel sur l'ordinateur client. |
| **Norme de scanner** | TWAIN ou WIA |
| **Protocole d'affichage pour View** | PCoIP<br><br>La redirection de scanner n'est pas prise en charge dans les sessions de poste de travail RDP. |

## Opération utilisateur de la redirection de scanner

Grâce à la fonction de redirection de scanner, les utilisateurs peuvent connecter des scanners physiques et des périphériques d'imagerie à leurs ordinateurs client comme périphériques virtuels capables de réaliser des opérations d'analyse dans leurs applications et leurs postes de travail distants.

Les utilisateurs peuvent se servir des scanners virtuels presque comme ils se servent des scanners sur les ordinateurs client connectés localement.

- Une fois l'option Redirection de scanner installée avec Horizon Agent, une icône de barre d'état système de scanner ( ) est ajoutée au poste de travail. Sur les applications RDS, l'icône de barre d'état système de scanner est redirigée vers l'ordinateur client local.

  Vous n'avez pas à utiliser l'icône de barre d'état système de scanner. La redirection de scanner fonctionne sans autre configuration. Vous pouvez utiliser l'icône pour configurer des options telles que le périphérique à utiliser, lorsque plusieurs périphériques sont connectés à l'ordinateur client.
- Lorsque vous cliquez sur l'icône du scanner, le menu Redirection de scanner pour VMware Horizon s'affiche. Aucun scanner n'apparaît dans la liste de ce menu si des scanners incompatibles sont connectés à l'ordinateur client.
- Par défaut, les périphériques d'analyse sont sélectionnés automatiquement. Les scanners TWAIN et WIA sont sélectionnés séparément. Il se peut qu'un scanner TWAIN et un scanner WIA soient sélectionnés simultanément.
- Si plusieurs scanners connectés localement sont configurés, vous pouvez sélectionner un scanner différent de celui qui est sélectionné par défaut.
- Les scanners WIA s'affichent dans le menu du gestionnaire des périphériques du poste de travail distant, sous **Périphériques d'imagerie**. Le scanner WIA est appelé **VMware Virtual Scanner WIA**.

- Dans le menu Redirection de scanner pour VMware Horizon, vous pouvez cliquer sur l'option **Préférences** et sélectionner des options telles que masquer les webcams dans le menu de redirection de scanner et définir la sélection du scanner par défaut.

  Vous pouvez également contrôler ces fonctionnalités en configurant les paramètres de stratégie de groupe de la redirection de scanner dans Active Directory. Reportez-vous à la section « Paramètres de stratégie de groupe de redirection de scanner », page 232.

- Lorsque vous utilisez un scanner TWAIN, le menu Redirection de scanner TWAIN pour VMware Horizon offre des options supplémentaires pour la sélection des régions d'une image, l'analyse en couleur, en noir et blanc ou en nuances de gris, et le choix d'autres fonctions courantes.

- Pour afficher la fenêtre de l'interface utilisateur TWAIN si un logiciel d'analyse TWAIN ne l'affiche pas par défaut, sélectionnez l'option **Toujours afficher la boîte de dialogue des paramètres du scanner** dans la boîte de dialogue Préférences de redirection de VMware Horizon Scanner.

  Notez toutefois que la plupart des logiciels d'analyse TWAIN affichent cette fenêtre par défaut. Pour ce logiciel, la fenêtre est toujours affichée, que l'option **Toujours afficher la boîte de dialogue des paramètres du scanner** soit sélectionnée ou non.

---

**Remarque** Si vous exécutez deux applications RDS hébergées sur différentes batteries de serveurs, deux icônes de redirection de scanner apparaissent dans la barre d'état système de l'ordinateur client. Généralement, un seul scanner est connecté à un ordinateur client. Dans ce cas, les deux icônes utilisent le même périphérique, ce qui signifie que l'une comme l'autre sont valides. Dans certaines situations, vous pouvez disposer de deux scanners connectés localement et exécuter deux applications RDS qui s'exécutent à leur tour sur des batteries de serveurs différentes. Dans ce cas, vous devez ouvrir chaque icône pour savoir quel menu de redirection de scanner contrôle quelle application RDS.

---

Pour obtenir des instructions d'utilisateur final relatives à l'utilisation des scanners redirigés, consultez le document *Utilisation de VMware Horizon Client pour Windows*.

## Configuration des paramètres de stratégie de groupe de redirection de scanner

Vous pouvez configurer les paramètres de stratégie de groupe qui contrôlent le comportement de la redirection de scanner sur vos applications et postes de travail View. Avec ces paramètres de stratégie, vous pouvez contrôler de façon centralisée, depuis Active Directory, les options qui sont disponibles dans la boîte de dialogue Préférences de redirection de VMware Horizon Scanner, dans les applications et sur les postes de travail des utilisateurs.

Vous n'avez pas à configurer ces paramètres de stratégie. La redirection de scanner fonctionne avec les paramètres par défaut qui sont configurés pour analyser les périphériques sur les postes de travail distants et les systèmes clients.

Ces paramètres de stratégie ont un impact sur vos applications et postes de travail distants (pas sur les systèmes clients auxquels les scanners physiques sont connectés). Pour configurer ces paramètres sur vos postes de travail et applications, ajoutez le fichier de modèle d'administration (ADM) de stratégie de groupe de redirection de scanner dans Active Directory.

### Ajouter le modèle d'administration de redirection de scanner à Active Directory

Vous pouvez ajouter les paramètres de stratégie du fichier ADM de redirection de scanner `vdm_agent_scanner.adm` aux objets de stratégie de groupe (GPO) dans Active Directory et configurer les paramètres dans l'Éditeur d'objets de stratégie de groupe.

#### Prérequis

- Vérifiez que l'option de configuration Redirection de scanner est installée sur vos hôtes RDS et vos postes de travail. Les paramètres de stratégie de groupe n'ont aucun effet si la redirection de scanner n'est pas installée. Reportez-vous à la section « Installer Horizon Agent sur une machine virtuelle », page 33.

- Vérifiez que les objets de stratégie de groupe (GPO) Active Directory sont créés pour les paramètres de stratégie de groupe de redirection de scanner. Les objets de stratégie de groupe (GPO) doivent être liés à l'unité d'organisation (UO) qui contient vos hôtes RDS et vos postes de travail. Reportez-vous à la section « Exemple de stratégie de groupe Active Directory », page 347.
- Vérifiez que les composants logiciels enfichables MMC (Microsoft Management Console) et l'Éditeur d'objets de stratégie de groupe sont disponibles sur votre serveur Active Directory.
- Familiarisez-vous avec les paramètres de stratégie de groupe de redirection de scanner. Reportez-vous à la section « Paramètres de stratégie de groupe de redirection de scanner », page 232.

### Procédure

1. Téléchargez le fichier View GPO Bundle `.zip` sur le site de téléchargement de VMware à l'adresse https://my.vmware.com/web/vmware/downloads.

   Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut GPO Bundle.

   Le fichier se nomme `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip`, où *x.x.x* est la version et *yyyyyyy* le numéro de build. Tous les fichiers ADM et ADMX qui fournissent des paramètres de stratégie de groupe pour View sont disponibles dans ce fichier.

2. Décompressez le fichier `VMware-Horizon-View-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip` et copiez le fichier ADM de redirection de scanner `vdm_agent_scanner.adm` sur votre serveur Active Directory.

3. Sur le serveur Active Directory, modifiez les objets de stratégie de groupe (GPO) en sélectionnant **Démarrer > Outils d'administration > Gestion de stratégie de groupe**, puis en cliquant avec le bouton droit sur GPO et en sélectionnant **Édition**.

4. Dans l'Éditeur d'objets de stratégie de groupe, cliquez avec le bouton droit sur le dossier **Configuration de l'ordinateur > Modèles d'administration**, puis sélectionnez **Ajout/Suppression de modèles**.

5. Cliquez sur **Ajouter**, accédez au fichier `vdm_agent_scanner.adm` et cliquez sur **Ouvrir**.

6. Cliquez sur **Fermer** pour appliquer les paramètres de stratégie dans le fichier de modèle d'administration pour les objets de stratégie de groupe (GPO).

   Les paramètres se trouvent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Modèles d'administration classiques > Configuration de VMware View Agent > Redirection de scanner**.

   La plupart des paramètres sont également ajoutés au dossier **Configuration utilisateur**, situé dans **Configuration utilisateur > Stratégies > Modèles d'administration > Modèles d'administration classiques > Configuration de VMware View Agent > Redirection de scanner**.

7. Configurez les paramètres de stratégie de groupe de redirection de scanner.

## Paramètres de stratégie de groupe de redirection de scanner

Les paramètres de stratégie de groupe de redirection de scanner contrôlent les options qui sont disponibles dans la boîte de dialogue Préférences de redirection de VMware Horizon Scanner des postes de travail et applications des utilisateurs.

Le fichier ADM de redirection de scanner contient les stratégies Configuration d'ordinateur et Configuration d'utilisateur. Les stratégies de configuration d'utilisateur vous permettent de définir des configurations différentes pour les utilisateurs de postes de travail VDI, de postes de travail RDS et d'applications RDS. Plusieurs stratégies de configuration d'utilisateur peuvent prendre effet, même lorsque les sessions de poste de travail et les applications des utilisateurs s'exécutent sur les mêmes hôtes RDS.

| Paramètre de stratégie de groupe | Description |
|---|---|
| Désactiver la fonctionnalité | Désactive la fonctionnalité de redirection de scanner.<br>Ce paramètre est disponible uniquement en tant que stratégie Configuration d'ordinateur.<br>Lorsque vous activez ce paramètre, les scanners ne peuvent pas être redirigés et n'apparaissent pas dans le menu du scanner des postes de travail et des applications des utilisateurs.<br>Lorsque vous désactivez ce paramètre ou ne le configurez pas, la redirection de scanner fonctionne et les scanners apparaissent dans le menu correspondant. |
| Configuration de verrouillage | Verrouille l'interface utilisateur de redirection de scanner et empêche les utilisateurs de modifier les options de configuration sur leurs postes de travail et dans leurs applications.<br>Ce paramètre est disponible uniquement en tant que stratégie Configuration d'ordinateur.<br>Lorsque vous activez ce paramètre, les utilisateurs ne peuvent pas configurer les options disponibles dans le menu de la barre d'état de leurs postes de travail et de leurs applications. Les utilisateurs peuvent afficher la boîte de dialogue Préférences de redirection de VMware Horizon Scanner, mais les options sont désactivées et ne peuvent pas être modifiées.<br>Lorsque vous désactivez ce paramètre ou ne le configurez pas, les utilisateurs peuvent configurer les options de la boîte de dialogue Préférences de redirection de VMware Horizon Scanner. |
| Compression | Définit le taux de compression d'image au cours du transfert d'image vers le poste de travail à distance ou l'application distante.<br>Vous avez le choix parmi les modes de compression suivants :<br>■ **Désactiver**. La compression d'image est désactivée.<br>■ **Sans perte**. La compression sans perte (`zlib`) conserve la qualité de l'image d'origine.<br>■ **JPEG**. La compression JPEG est source de perte de qualité. Spécifiez le niveau de qualité d'image dans le champ **Qualité de compression JPEG**. La qualité de compression JPEG doit être une valeur comprise entre 0 et 100.<br>Lorsque vous activez ce paramètre, le mode de compression sélectionné est défini pour tous les utilisateurs affectés par cette stratégie. Cependant, les utilisateurs peuvent modifier l'option **Compression** dans la boîte de dialogue Préférences de redirection de VMware Horizon Scanner et remplacer le paramètre de stratégie.<br>Lorsque vous désactivez le paramètre de cette stratégie ou ne le configurez pas, le mode de compression **JPEG** est utilisé. |
| Masquer la webcam | Empêche les webcams d'apparaître dans le menu de sélection de scanner de la boîte de dialogue Préférences de redirection de VMware Horizon Scanner.<br>Ce paramètre est disponible en tant que stratégie Configuration d'ordinateur et Configuration d'utilisateur.<br>Par défaut, les webcams peuvent être redirigées vers les postes de travail et les applications. Les utilisateurs peuvent sélectionner des webcams et les utiliser comme scanners virtuels pour capturer des images.<br>Lorsque vous activez ce paramètre en tant que stratégie Configuration d'ordinateur, les webcams sont masquées pour tous les utilisateurs des ordinateurs affectés. Les utilisateurs ne peuvent pas modifier l'option **Masquer la webcam** dans la boîte de dialogue Préférences de redirection de VMware Horizon Scanner.<br>Lorsque vous activez ce paramètre en tant que stratégie Configuration d'utilisateur, les webcams sont masquées pour tous les utilisateurs affectés. Cependant, les utilisateurs peuvent modifier l'option **Masquer la webcam** dans la boîte de dialogue Préférences de redirection de VMware Horizon Scanner.<br>Lorsque vous activez ce paramètre à la fois dans la configuration d'ordinateur et dans la configuration d'utilisateur, le paramètre **Masquer la webcam** de la configuration d'ordinateur remplace le paramètre de stratégie correspondant de la configuration d'utilisateur pour tous les utilisateurs des ordinateurs affectés.<br>Lorsque vous désactivez ce paramètre ou ne le configurez pas dans l'une des configurations de stratégie, le paramètre **Masquer la webcam** est déterminé par le paramètre de stratégie correspondant (soit Configuration d'ordinateur, soit Configuration d'utilisateur) ou par la sélection de l'utilisateur dans la boîte de dialogue Préférences de redirection de VMware Horizon Scanner. |

| Paramètre de stratégie de groupe | Description |
|---|---|
| Scanner par défaut | Permet la gestion centralisée de sélection automatique de scanner.<br>Ce paramètre est disponible en tant que stratégie Configuration d'ordinateur et Configuration d'utilisateur.<br>Les options de sélection automatique de scanner sont sélectionnées séparément pour les scanners TWAIN et WIA. Vous avez le choix parmi les options de sélection automatique suivantes :<br>■ **Aucune**. Ne pas sélectionner de scanner automatiquement.<br>■ **Sélection automatique**. Sélectionne automatiquement le scanner connecté localement.<br>■ **Dernier scanner utilisé**. Sélectionne automatiquement le dernier scanner utilisé.<br>■ **Spécifié**. Sélectionne le scanner dont vous avez entré le nom dans la zone de texte **Scanner spécifié**.<br>Lorsque vous activez ce paramètre en tant que stratégie Configuration d'ordinateur, le paramètre détermine le mode de sélection automatique de scanner pour tous les utilisateurs des ordinateurs affectés. Les utilisateurs ne peuvent pas modifier l'option **Scanner par défaut** dans la boîte de dialogue Préférences de redirection de VMware Horizon Scanner.<br>Lorsque vous activez ce paramètre en tant que stratégie Configuration d'utilisateur, le paramètre détermine le mode de sélection automatique de scanner pour tous les utilisateurs affectés. Cependant, les utilisateurs peuvent modifier l'option **Scanner par défaut** dans la boîte de dialogue Préférences de redirection de VMware Horizon Scanner.<br>Lorsque vous activez ce paramètre à la fois dans la configuration d'ordinateur et dans la configuration d'utilisateur, le mode de sélection automatique de scanner de la configuration d'ordinateur remplace le paramètre de stratégie correspondant de la configuration d'utilisateur pour tous les utilisateurs des ordinateurs affectés.<br>Lorsque vous désactivez ce paramètre ou ne le configurez pas dans l'une des configurations de stratégie, le mode de sélection automatique de scanner est déterminé par le paramètre de stratégie correspondant (soit Configuration d'ordinateur, soit Configuration d'utilisateur) ou par la sélection de l'utilisateur dans la boîte de dialogue Préférences de redirection de VMware Horizon Scanner. |

## Configuration de la redirection de port série

Avec la redirection de port série, les utilisateurs peuvent rediriger des ports série (COM) connectés en local, tels que les ports RS232 intégrés ou les adaptateurs USB-série. Les périphériques, comme les imprimantes, les lecteurs de code-barres et autres périphériques série, peuvent être connectés à ces ports et utilisés sur les postes de travail distants.

La redirection de port série est disponible dans Horizon 6 version 6.1.1 et versions ultérieures avec Horizon Client pour Windows 3.4 et versions ultérieures.

Après avoir installé Horizon Agent et configuré la fonctionnalité de redirection de port série, cette dernière peut fonctionner sur vos postes de travail distants sans configuration supplémentaire. Par exemple, COM1 sur le système client local est redirigé en tant que COM1 sur le poste de travail distant, et COM2 est redirigé en tant que COM2, sauf si un port COM existe déjà sur le poste de travail distant. Si c'est le cas, le port COM est mappé pour éviter les conflits. Par exemple, si COM1 et COM2 existent déjà sur le poste de travail distant, COM1 sur le client est mappé vers COM3 par défaut. Vous n'avez pas à configurer les ports COM ou à installer des pilotes de périphérique sur les postes de travail distants.

Pour activer un port COM redirigé, l'utilisateur sélectionne l'option **Se connecter** dans le menu sur l'icône de barre d'état système du port série lors d'une session de poste de travail. Un utilisateur peut également régler un périphérique de port COM pour qu'il se connecte automatiquement dès que l'utilisateur ouvre une session sur le poste de travail distant. Reportez-vous à la section « Opération utilisateur de la redirection de port série », page 236.

Vous pouvez configurer des paramètres de stratégie de groupe pour modifier la configuration par défaut. Par exemple, vous pouvez verrouiller les paramètres pour que les utilisateurs ne puissent pas modifier les mappages ou les propriétés du port COM. Vous pouvez également définir une stratégie pour désactiver ou activer la fonctionnalité. Un fichier de modèle d'administration vous permet d'installer des paramètres de stratégie de groupe de redirection de port série dans Active Directory ou sur des postes de travail individuels. Reportez-vous à la section « Configuration des paramètres de stratégie de groupe de redirection de port série », page 237.

Lorsqu'un port COM redirigé est ouvert et utilisé sur un poste de travail distant, vous ne pouvez pas accéder au port sur l'ordinateur local. À l'inverse, lorsqu'un port COM est utilisé sur l'ordinateur local, vous ne pouvez pas accéder au port sur le poste de travail distant.

## Exigences de la redirection de port série

Avec cette fonction, les utilisateurs peuvent rediriger des ports série (COM) connectés en local, tels que les ports RS232 intégrés ou les adaptateurs USB-série, vers leurs postes de travail distants. Pour prendre en charge la redirection de port série, votre déploiement de View doit répondre à certaines exigences matérielles et logicielles.

**Poste de travail distant View**

Les postes de travail distants requièrent l'installation de View Agent 6.1.1 ou version ultérieure, ou d'Horizon Agent 7.0 ou version ultérieure, avec l'option d'installation de redirection de port série, sur les machines virtuelles parentes ou modèles. Cette option d'installation n'est pas sélectionnée par défaut.

Les systèmes d'exploitation invités suivants sont pris en charge sur les machines virtuelles mono-utilisateur :

- Windows 7 32 ou 64 bits
- Windows 8.x 32 ou 64 bits
- Windows 10 32 ou 64 bits
- Windows Server 2008 R2 configuré en tant que poste de travail
- Windows Server 2012 R2 configuré en tant que poste de travail

Cette fonction n'est pas actuellement prise en charge pour les hôtes RDS Windows Server.

Les pilotes du périphérique de port série n'ont pas à être installés sur le système d'exploitation du poste de travail sur lequel l'agent est installé.

**Ordinateur Horizon Client ou périphérique d'accès client**

- Horizon Clientpour Windows 3.4 ou version ultérieure doit être installé sur le système client.
- La redirection de port série est prise en charge sur les systèmes clients Windows 7 32 ou 64 bits, Windows 8.x 32 ou 64 bits et Windows 10 32 et 64 bits.
- Tous les pilotes du périphérique de port série nécessaires doivent être installés, et le port série doit être opérationnel sur l'ordinateur client. Vous n'avez pas besoin d'installer les pilotes de périphérique sur le système d'exploitation du poste de travail à distance sur lequel l'agent est installé.

**Protocole d'affichage pour View**

- PCoIP

- VMware Blast Extreme (requiert Horizon Client 4.0 ou version ultérieure et Horizon Agent 7.0 ou version ultérieure)

La redirection de port série VMware Horizon n'est pas prise en charge dans les sessions de poste de travail RDP.

## Opération utilisateur de la redirection de port série

Les utilisateurs peuvent faire fonctionner des périphériques de port COM physiques qui sont connectés à leurs ordinateurs clients et utiliser la virtualisation de port série pour connecter les périphériques à leurs postes de travail distants, lorsque les périphériques sont accessibles à des applications tierces.

- Une fois l'option Redirection de port série installée avec Horizon Agent, une icône de barre d'état système de port série ( ) est ajoutée au poste de travail distant.

  L'icône apparaît uniquement si vous utilisez les versions requises d'Horizon Agent et d'Horizon Client pour Windows, et si vous vous connectez sur PCoIP. L'icône n'apparaît pas si vous vous connectez à un poste de travail distant depuis un Mac, Linux ou un client mobile.

  Vous pouvez utiliser l'icône afin de configurer des options pour connecter, déconnecter et personnaliser les ports COM mappés.

- Lorsque vous cliquez sur l'icône de port série, le menu **Redirection série COM pour VMware Horizon** s'affiche.

- Par défaut, les ports COM connectés en local sont mappés vers les ports COM correspondants sur le poste de travail distant. Par exemple : **COM1 mappé vers COM3**. Les ports mappés ne sont pas connectés par défaut.

- Pour utiliser un port COM mappé, vous devez sélectionner manuellement l'option **Se connecter** dans le menu **Redirection série COM pour VMware Horizon** ou l'option **Se connecter automatiquement** doit être définie lors d'une session de poste de travail précédente ou en configurant un paramètre de stratégie de groupe. **Se connecter automatiquement** configure un port mappé pour qu'il se connecte automatiquement lorsqu'une session de poste de travail distant est démarrée.

- Lorsque vous sélectionnez l'option **Se connecter**, le port redirigé est actif. Dans le gestionnaire des périphériques du système d'exploitation invité sur le poste de travail distant, le port redirigé est indiqué par **Redirecteur de port série pour VMware Horizon (COM*n*)**.

  Lorsque le port COM est connecté, vous pouvez ouvrir le port dans une application tierce, qui peut échanger des données avec le périphérique de port COM connecté à la machine cliente. Lorsqu'un port est ouvert dans une application, vous ne pouvez pas le déconnecter dans le menu **Redirection série COM pour VMware Horizon**.

  Avant de pouvoir déconnecter le port COM, vous devez le fermer dans l'application ou fermer l'application. Vous pouvez ensuite sélectionner l'option **Déconnecter** pour déconnecter le port et rendre le port COM physique disponible pour utilisation sur la machine cliente.

- Dans le menu **Redirection série COM pour VMware Horizon**, vous pouvez cliquer avec le bouton droit sur un port redirigé pour sélectionner la commande **Propriétés du port**.

  Dans la boîte de dialogue Propriétés COM, vous pouvez configurer un port pour qu'il se connecte automatiquement lorsqu'une session de poste de travail distant est démarrée, ignorer le signal DSR (Data Set Ready) et mapper le port local sur le client vers un port COM différent sur le poste de travail distant en sélectionnant un port dans la liste déroulante **Personnaliser le nom de port**.

  Un port de poste de travail distant peut apparaître comme étant chevauché. Par exemple, vous pouvez voir **COM1 (chevauché)**. Dans ce cas, la machine virtuelle est configurée avec un port COM dans le matériel virtuel sur l'hôte ESXi. Vous pouvez utiliser un port redirigé même lorsqu'il est mappé vers un port chevauché sur la machine virtuelle. La machine virtuelle reçoit des données de série via le port depuis l'hôte ESXi ou le système client.

- Dans le gestionnaire des périphériques du système d'exploitation invité, vous pouvez utiliser l'onglet **Propriétés > Paramètres du port** pour configurer des paramètres d'un port COM redirigé. Par exemple, vous pouvez régler le débit en bauds et les bits de données par défaut. Toutefois, les paramètres que vous configurez dans le gestionnaire des périphériques sont ignorés si l'application spécifie les paramètres du port.

Pour obtenir des instructions d'utilisateur final relatives à l'utilisation des ports COM série redirigés, consultez le document *Utilisation de VMware Horizon Client pour Windows*.

## Instructions relatives à configuration de la redirection de port série

Grâce aux paramètres de stratégie de groupe, vous pouvez configurer la redirection de port série et limiter la capacité des utilisateurs à personnaliser les ports COM redirigés. Vos choix dépendent des rôles d'utilisateur et des applications tierces de votre organisation.

Pour plus d'informations sur les paramètres de stratégie de groupe, reportez-vous à « Paramètres de stratégie de groupe de redirection de port série », page 239.

- Si vos utilisateurs exécutent les mêmes applications tierces et périphériques de port COM, assurez-vous que les ports redirigés sont configurés de la même façon. Par exemple, dans une banque ou une boutique qui utilise des périphériques de point de vente, assurez-vous que tous les périphériques de port COM sont connectés aux mêmes ports sur les points de terminaison clients, et que tous les ports sont mappés vers les mêmes ports COM redirigés sur les postes de travail distants.

  Réglez le paramètre de stratégie **PortSettings** pour mapper les ports clients vers les ports redirigés. Sélectionnez l'élément **Autoconnect** dans **PortSettings** pour vous assurer que les ports redirigés sont connectés au début de chaque session de poste de travail. Activez le paramètre de stratégie **Lock Configuration** pour empêcher les utilisateurs de modifier les mappages de port ou de personnaliser les configurations de port. Dans ce scénario, les utilisateurs n'ont jamais à se connecter ou à se déconnecter manuellement et ils ne peuvent pas accidentellement rendre un port COM redirigé inaccessible à une application tierce.

- Si vos utilisateurs sont des travailleurs du savoir qui utilisent diverses applications tierces et qui peuvent également utiliser leurs ports COM localement sur leurs machines clientes, assurez-vous que les utilisateurs peuvent se connecter et se déconnecter des ports COM redirigés.

  Vous pouvez régler le paramètre de stratégie **PortSettings** si les mappages de port par défaut sont incorrects. En fonction des exigences de vos utilisateurs, vous pouvez ou non régler l'élément **Autoconnect**. N'activez pas le paramètre de stratégie **Lock Configuration**.

- Assurez-vous que vos applications tierces ouvrent le port COM mappé vers le poste de travail distant.
- Assurez-vous que le débit en bauds utilisé pour un périphérique correspond au débit en bauds que l'application tierce tente d'utiliser.
- Vous pouvez rediriger jusqu'à cinq ports COM entre un système client et un poste de travail distant.

## Configuration des paramètres de stratégie de groupe de redirection de port série

Vous pouvez configurer les paramètres de stratégie de groupe qui contrôlent le comportement de la redirection de port série sur vos postes de travail distants. Avec ces paramètres de stratégie, vous pouvez contrôler de façon centralisée, depuis Active Directory, les options disponibles dans le menu **Redirection série COM pour VMware Horizon** sur les postes de travail des utilisateurs.

Vous n'avez pas à configurer ces paramètres de stratégie. La redirection de port série fonctionne avec les paramètres par défaut qui sont configurés pour les ports COM redirigés sur les postes de travail distants et les systèmes clients.

Ces paramètres de stratégie affectent vos postes de travail, et non les systèmes clients sur lesquels les périphériques de port COM physiques sont connectés. Pour configurer ces paramètres sur vos postes de travail, ajoutez le fichier de modèle d'administration (ADM) de stratégie de groupe pour la redirection de port série dans Active Directory.

## Ajouter le modèle d'administration de redirection de port série à Active Directory

Vous pouvez ajouter les paramètres de stratégie du fichier ADM de redirection de port série `vdm_agent_serialport.adm` aux objets de stratégie de groupe (GPO) dans Active Directory et configurer les paramètres dans l'Éditeur d'objets de stratégie de groupe.

### Prérequis

- Vérifiez que l'option d'installation Redirection de port série est installée sur vos postes de travail. Les paramètres de stratégie de groupe n'ont aucun effet si la redirection de port série n'est pas installée. Reportez-vous à la section « Installer Horizon Agent sur une machine virtuelle », page 33.
- Vérifiez que les objets de stratégie de groupe (GPO) Active Directory sont créés pour les paramètres de stratégie de groupe de redirection de port série. Les objets de stratégie de groupe (GPO) doivent être liés à l'unité d'organisation (UO) qui contient vos postes de travail. Reportez-vous à la section « Exemple de stratégie de groupe Active Directory », page 347.
- Vérifiez que les composants logiciels enfichables MMC (Microsoft Management Console) et l'Éditeur d'objets de stratégie de groupe sont disponibles sur votre serveur Active Directory.
- Familiarisez-vous avec les paramètres de stratégie de groupe de redirection de port série. Reportez-vous à la section « Paramètres de stratégie de groupe de redirection de port série », page 239.

### Procédure

1. Téléchargez le fichier View GPO Bundle `.zip` sur le site de téléchargement de VMware à l'adresse https://my.vmware.com/web/vmware/downloads.

   Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut GPO Bundle.

   Le fichier se nomme `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`, où *x.x.x* est la version et *yyyyyyy* le numéro de build. Tous les fichiers ADM et ADMX qui fournissent des paramètres de stratégie de groupe pour View sont disponibles dans ce fichier.

2. Décompressez le fichier `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` et copiez le fichier ADM de redirection de port série `vdm_agent_serialport.adm` sur votre serveur Active Directory.

3. Sur le serveur Active Directory, modifiez les objets de stratégie de groupe (GPO) en sélectionnant **Démarrer > Outils d'administration > Gestion de stratégie de groupe**, puis en cliquant avec le bouton droit sur GPO et en sélectionnant **Édition**.

4. Dans l'Éditeur d'objets de stratégie de groupe, cliquez avec le bouton droit sur le dossier **Configuration de l'ordinateur > Modèles d'administration**, puis sélectionnez **Ajout/Suppression de modèles**.

5. Cliquez sur **Ajouter**, accédez au fichier `vdm_agent_serialport.adm` et cliquez sur **Ouvrir**.

6. Cliquez sur **Fermer** pour appliquer les paramètres de stratégie dans le fichier de modèle d'administration pour les objets de stratégie de groupe (GPO).

   Les paramètres se trouvent dans le dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Modèles d'administration classiques > Configuration de VMware View Agent > Série COM**.

   La plupart des paramètres sont également ajoutés au dossier **Configuration utilisateur**, situé dans **Configuration utilisateur > Stratégies > Modèles d'administration > Modèles d'administration classiques > Configuration de VMware View Agent > Série COM**.

7 Configurez les paramètres de stratégie de groupe de redirection de port série.

## Paramètres de stratégie de groupe de redirection de port série

Les paramètres de stratégie de groupe de redirection de port série contrôlent la configuration du port COM redirigé, y compris les options qui sont disponibles dans le menu **Redirection série COM pour VMware Horizon** sur les postes de travail distants.

Le fichier ADM de redirection de port série contient les stratégies Configuration d'ordinateur et Configuration d'utilisateur. Les stratégies Configuration d'utilisateur vous permettent de régler différentes configurations pour des utilisateurs spécifiés de postes de travail VDI. Les paramètres de stratégie configurés dans Configuration d'ordinateur sont prioritaires sur les paramètres correspondants configurés dans Configuration d'utilisateur.

| Paramètre de stratégie de groupe | Description |
|---|---|
| PortSettings | Détermine le mappage entre le port COM sur le système client et le port COM redirigé sur le poste de travail distant et détermine d'autres paramètres qui affectent le port COM redirigé.<br>Vous configurez chaque port COM redirigé individuellement. Cinq paramètres de stratégie **PortSettings** sont disponibles, **PortSettings1** à **PortSettings5**, ce qui permet de mapper jusqu'à cinq ports COM entre le client et le poste de travail distant. Sélectionnez un paramètre de stratégie **PortSettings** pour chaque port COM que vous voulez configurer.<br>Lorsque vous activez le paramètre de stratégie **PortSettings**, vous pouvez configurer les éléments suivants qui affectent le port COM redirigé :<br>■ Le paramètre **Source port number** spécifie le numéro du port COM physique connecté au système client.<br>■ Le paramètre **Destination virtual port number** spécifie le numéro du port COM virtuel redirigé sur le poste de travail distant.<br>■ Le paramètre **Autoconnect** connecte automatiquement le port COM au port COM redirigé au début de chaque session de poste de travail.<br>■ Avec le paramètre **IgnoreDSR**, le périphérique du port COM redirigé ignore le signal DSR (Data Set Ready).<br>■ Le paramètre **Pause before close port (in milliseconds)** spécifie le temps d'attente (en millisecondes) entre la fermeture du port redirigé par un utilisateur et la fermeture réelle du port. Certains adaptateurs USB-série requièrent ce délai pour garantir que les données transmises sont conservées. Ce paramètre est conçu à des fins de dépannage.<br>■ Le paramètre **Serial2USBModeChangeEnabled** résout les problèmes qui s'appliquent aux adaptateurs USB-série utilisant la puce Prolific, y compris l'adaptateur GlobalSat BU353 GPS. Si vous n'activez pas ce paramètre pour les adaptateurs de puce Prolific, les périphériques connectés peuvent transmettre des données mais pas en recevoir.<br>■ Le paramètre **Disable errors in wait mask** désactive la valeur d'erreur dans le masque de port COM. Ce paramètre de dépannage est requis pour certaines applications. Pour plus de détails, consultez la documentation Microsoft de la fonction `WaitCommEvent` à l'adresse http://msdn.microsoft.com/en-us/library/windows/desktop/aa363479(v=vs.85).aspx.<br>■ Le paramètre **HandleBtDisappear** prend en charge le comportement du port COM BlueTooth. Ce paramètre est conçu à des fins de dépannage.<br>■ Le paramètre **UsbToComTroubleShooting** résout certains problèmes qui s'appliquent aux adaptateurs de port USB-série. Ce paramètre est conçu à des fins de dépannage.<br>Lorsque vous activez le paramètre **PortSettings** pour un port COM particulier, les utilisateurs peuvent se connecter et se déconnecter du port redirigé, mais ils ne peuvent pas configurer les propriétés du port sur le poste de travail distant. Par exemple, les utilisateurs ne peuvent pas régler le port pour qu'il soit redirigé automatiquement lorsqu'ils se connectent au poste de travail, et ils ne peuvent pas ignorer le signal DSR. Ces propriétés sont contrôlées par le paramètre de stratégie de groupe.<br>**Remarque** Un port COM redirigé est connecté et actif uniquement si le port COM physique est connecté en local au système client. Si vous mappez un port COM qui n'existe pas sur le client, le port redirigé apparaît comme étant inactif et indisponible dans le menu de la barre d'état système sur le poste de travail distant.<br>Lorsque le paramètre **PortSettings** est désactivé ou non configuré, le port COM redirigé utilise les paramètres que les utilisateurs configurent sur le poste de travail distant. Les options du menu **Redirection série COM pour VMware Horizon** sont actives et disponibles pour les utilisateurs.<br>Ce paramètre est disponible en tant que stratégie Configuration d'ordinateur et Configuration d'utilisateur. |
| Local settings priority | Donne la priorité aux paramètres configurés sur le poste de travail distant.<br>Lorsque vous activez cette stratégie, les paramètres de redirection de port série qu'un utilisateur configure sur le poste de travail distant sont prioritaires sur les paramètres de stratégie de groupe. Un paramètre de stratégie de groupe prend effet uniquement si un paramètre n'est pas configuré sur le poste de travail distant.<br>Lorsque ce paramètre est désactivé ou non configuré, les paramètres de stratégie de groupe sont prioritaires sur les paramètres configurés sur le poste de travail distant.<br>Ce paramètre est disponible en tant que stratégie Configuration d'ordinateur et Configuration d'utilisateur. |

| Paramètre de stratégie de groupe | Description |
|---|---|
| Désactiver la fonctionnalité | Désactive la fonctionnalité de redirection de port série.<br>Lorsque vous activez ce paramètre, les ports COM ne sont pas redirigés vers le poste de travail distant. L'icône de barre d'état système du port série sur le poste de travail distant n'est pas affichée.<br>Lorsque ce paramètre est désactivé, la redirection de port série fonctionne, l'icône de barre d'état système du port série est affichée et les ports COM apparaissent dans le menu **Redirection série COM pour VMware Horizon**.<br>Lorsque ce paramètre n'est pas configuré, les paramètres locaux sur le poste de travail distant déterminent si la redirection de port série est désactivée ou activée.<br>Ce paramètre est disponible uniquement en tant que stratégie Configuration d'ordinateur. |
| Lock configuration | Verrouille l'interface utilisateur de la redirection de port série et empêche les utilisateurs de modifier les options de configuration sur le poste de travail distant.<br>Lorsque vous activez ce paramètre, les utilisateurs ne peuvent pas configurer les options disponibles dans le menu de la barre d'état système de leurs postes de travail. Les utilisateurs peuvent afficher le menu **Redirection série COM pour VMware Horizon**, mais les options sont inactives et ne peuvent pas être modifiées.<br>Lorsque ce paramètre est désactivé, les utilisateurs peuvent configurer les options dans le menu **Redirection série COM pour VMware Horizon**.<br>Lorsque ce paramètre n'est pas configuré, les paramètres de programme locaux sur le poste de travail distant déterminent si les utilisateurs peuvent configurer les paramètres de redirection de port COM. |
| Bandwidth limit | Définit une limite sur la vitesse de transmission des données, en kilo-octets par seconde, entre le port série redirigé et les systèmes clients.<br>Lorsque vous activez ce paramètre, vous pouvez définir une valeur dans la case **Bandwidth limit (in kilobytes per second)** qui détermine la vitesse de transmission des données maximale entre le port série redirigé et le client. La valeur de 0 désactive la limite de bande passante.<br>Lorsque ce paramètre est désactivé, aucune limite de bande passante n'est définie.<br>Lorsque ce paramètre n'est pas configuré, les paramètres de programme locaux sur le poste de travail distant déterminent si une limite de bande passante est définie.<br>Ce paramètre est disponible uniquement en tant que stratégie Configuration d'ordinateur. |

## Configurer des adaptateurs USB-série

Vous pouvez configurer des adaptateurs USB-série utilisant une puce Prolific de façon à ce qu'ils soient redirigés vers des postes de travail distants par la fonctionnalité de redirection de port série.

Pour vérifier que les données sont bien transmises sur les adaptateurs de puce Prolific, vous pouvez activer un paramètre de stratégie de groupe de redirection de port série dans Active Directory ou sur une machine virtuelle de poste de travail individuel.

Si vous ne configurez pas le paramètre de stratégie de groupe pour résoudre les problèmes des adaptateurs de puce Prolific, les périphériques connectés peuvent transmettre des données mais pas en recevoir.

Vous n'avez pas à configurer un paramètre de stratégie ou une clé de registre sur les systèmes clients.

### Prérequis

- Vérifiez que l'option d'installation Redirection de port série est installée sur vos postes de travail. Les paramètres de stratégie de groupe n'ont aucun effet si la redirection de port série n'est pas installée. Reportez-vous à la section « Installer Horizon Agent sur une machine virtuelle », page 33.
- Vérifiez que le fichier ADM de redirection de port série est ajouté dans Active Directory ou sur la machine virtuelle de poste de travail. Reportez-vous à la section « Ajouter le modèle d'administration de redirection de port série à Active Directory », page 238.
- Familiarisez-vous avec l'élément **Serial2USBModeChangeEnabled** dans le paramètre de stratégie de groupe **PortSettings**. Reportez-vous à la section « Paramètres de stratégie de groupe de redirection de port série », page 239.

**Procédure**

1 Dans Active Directory ou sur la machine virtuelle, ouvrez l'Éditeur d'objets de stratégie de groupe.

2 Accédez au dossier **Configuration ordinateur > Stratégies > Modèles d'administration > Modèles d'administration classiques > Configuration de VMware View Agent > Série COM**.

3 Sélectionnez le dossier **PortSettings**.

4 Sélectionnez et activez le paramètre de stratégie de groupe **PortSettings**.

5 Spécifiez les numéros des ports COM source et de destination pour mapper le port COM.

6 Cochez la case **Serial2USBModeChangeEnabled**.

7 Configurez d'autres éléments dans le paramètre de stratégie **PortSettings** si nécessaire.

8 Cliquez sur **OK** et fermez l'Éditeur d'objets de stratégie de groupe.

Les adaptateurs USB-série peuvent être redirigés vers des postes de travail distants. Ils peuvent recevoir des données lorsque les utilisateurs démarrent leurs prochaines sessions de poste de travail.

# Gestion de l'accès à la redirection multimédia (MMR) Windows Media

View fournit la fonction Windows Media MMR pour les postes de travail VDI exécutés sur des machines mono-utilisateur et pour les postes de travail RDS.

MMR délivre le flux multimédia directement aux ordinateurs client. Avec MMR, le flux multimédia est traité, c'est-à-dire décodé, sur le système client. Le système client effectue la lecture du contenu multimédia, déchargeant ainsi la demande sur l'hôte ESXi.

Les données MMR sont envoyées sur le réseau sans cryptage au niveau de l'application et peuvent contenir des éléments sensibles, selon le contenu redirigé. Pour garantir que les données ne puissent pas être surveillées sur le réseau, utilisez MMR uniquement sur un réseau sécurisé.

Si le tunnel sécurisé est activé, les connexions MMR entre Horizon Clients et View Secure Gateway sont sécurisées, mais les connexions entre View Secure Gateway et les machines de poste de travail ne sont pas cryptées. Si le tunnel sécurisé est désactivé, les connexions MMR entre Horizon Clients et les machines de poste de travail ne sont pas cryptées.

## Activation de la redirection multimédia dans View

Vous pouvez prendre des mesures pour vous assurer que la Redirection multimédia (MMR) est accessible uniquement aux systèmes Horizon Client qui disposent de ressources suffisantes pour gérer le décodage multimédia local et qui sont connectés à View sur un réseau sécurisé.

Par défaut, la stratégie globale de View Administrator, **Redirection multimédia (MMR)** est définie sur **Refuser**.

Pour utiliser la fonctionnalité MMR, vous devez définir cette valeur de manière explicite sur **Autoriser**.

Pour contrôler l'accès à MMR, vous pouvez activer ou désactiver la stratégie **Redirection multimédia (MMR)** globalement, pour des pools de postes de travail individuels ou pour des utilisateurs spécifiques.

Pour savoir comment définir des stratégies globales dans View Administrator, reportez-vous à « Règles de View », page 299.

## Configuration système requise pour la redirection multimédia (MMR) Windows Media

Pour prendre en charge la redirection multimédia (MMR) Windows Media, le déploiement de votre View doit répondre à certaines exigences matérielles et logicielles. La fonctionnalité MMR Windows Media est fournie dans Horizon 6.0.2 et versions ultérieures.

**Poste de travail distant View**

- Cette fonctionnalité est prise en charge sur les postes de travail VDI qui sont déployés sur des machines virtuelles mono-utilisateur et sur les postes de travail RDS.

  View Agent 6.1.1 ou version ultérieure est requis pour prendre en charge cette fonctionnalité sur les postes de travail RDS.

  View Agent 6.0.2 ou version ultérieure est requis pour prendre en charge cette fonctionnalité sur les machines mono-utilisateur.
- Les systèmes d'exploitation invités suivants sont pris en charge :
  - Windows 7 SP1 Entreprise ou Intégrale 32 ou 64 bits (machine mono-utilisateur). Windows 7 Professionnel n'est pas pris en charge.
  - Windows 8/8.1 Professionnel ou Entreprise 32 ou 64 bits (machine mono-utilisateur)
  - Windows Server 2008 R2 configuré en tant qu'hôte RDS
  - Windows Server 2012 et 2012 R2 configuré en tant qu'hôte RDS
- Le **rendu 3D** peut être activé ou désactivé sur le pool de postes de travail.
- Les utilisateurs doivent lire les vidéos sur Lecteur Windows Media 12 (ou version ultérieure) ou sur Internet Explorer 8 (ou version ultérieure).

  Si vous utilisez Internet Explorer, désactivez le mode protégé. Dans la boîte de dialogue Options Internet, cliquez sur l'onglet **Sécurité** et désélectionnez **Activer le mode protégé**.

**Logiciel Horizon Client**

Horizon Client 3.2 pour Windows ou une version ultérieure est requis pour prendre en charge Windows Media MMR sur les machines mono-utilisateur.

**Ordinateur Horizon Client ou périphérique d'accès client**

- Les clients doivent exécuter des systèmes d'exploitation Windows 7 ou Windows 8/8.1 à 64 ou 32 bits.

**Formats multimédias pris en charge**

Les formats multimédia pris en charge sont ceux que prend en charge Lecteur Windows Media. Par exemple : M4V ; MOV ; MP4 ; WMP ; MPEG-4 Part 2 ; WMV 7, 8 et 9 ; WMA ; AVI ; ACE ; MP3 ; WAV.

---

**Remarque** Le contenu protégé par DRM n'est pas redirigé via la Redirection multimédia du Lecteur Windows Media.

---

**Stratégies View** Dans View Administrator, définissez la stratégie **Redirection multimédia (MMR)** sur **Autoriser**. La valeur par défaut est **Refuser**.

**Pare-feu dorsal** Si le déploiement d'View inclut un pare-feu dorsal entre vos serveurs de sécurité de la zone DMZ et votre réseau interne, assurez-vous que le pare-feu dorsal autorise le trafic vers le port 9427 de vos postes de travail.

## Déterminer s'il convient d'utiliser Windows Media MMR en fonction de la latence réseau

Par défaut, Windows Media MMR s'adapte aux conditions du réseau sur les postes de travail mono-utilisateur qui s'exécutent sous Windows 8 ou versions ultérieures et les postes de travail RDS qui s'exécutent sous Windows Server 2012 ou 2012 R2 ou versions ultérieures. Si la latence réseau entre Horizon Client et le poste de travail distant est de 29 millisecondes ou moins, la vidéo est redirigée avec Windows Media MMR. Si la latence réseau est de 30 millisecondes ou plus, la vidéo n'est pas redirigée. Elle est rendue sur l'hôte ESXi et envoyée au client sur PCoIP.

Cette fonction s'applique aux postes de travail mono-utilisateur Windows 8 ou versions ultérieures et aux postes de travail RDS Windows Server 2012 ou 2012 R2 ou versions ultérieures. Les utilisateurs peuvent exécuter n'importe quel système client pris en charge, Windows 7 ou Windows 8/8.1.

Cette fonction ne s'applique pas aux postes de travail mono-utilisateur Windows 7 ni aux postes de travail RDS Windows Server 2008 R2. Sur ces systèmes d'exploitation invités, Windows Media MMR effectue toujours la redirection multimédia, quelle que soit la latence réseau.

Vous pouvez remplacer cette fonction pour obliger Windows Media MMR à effectuer une redirection multimédia quelle que soit la latence réseau, en configurant le paramètre de registre `RedirectionPolicy` sur le poste de travail.

### Procédure

1 Lancez l'éditeur du Registre Windows sur le poste de travail distant.

2 Accédez à la clé de registre Windows qui contrôle la stratégie de redirection.

| Option | Description |
|---|---|
| **Poste de travail 64 bits** | `HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware tsmmr` |
| **Poste de travail 32 bits** | `HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware tsmmr` |

3 Définissez la valeur de `RedirectionPolicy` sur `always`.

```
Value name = RedirectionPolicy
Value Type = REG_SZ
Value data = always
```

4 Redémarrez Windows Media Player sur le poste de travail pour que la valeur mise à jour entre en vigueur.

# Gestion de l'accès à la redirection de lecteur client

Lorsque vous déployez Horizon Client 3.5 ou version ultérieure, View Agent 6.2 ou version ultérieure et Horizon Agent 7.0 ou version ultérieure avec la redirection du lecteur client, les dossiers et les fichiers sont envoyés sur le réseau avec chiffrement. Les connexions de redirection du lecteur client entre les clients et View Secure Gateway et les connexions entre View Secure Gateway et les machines de poste de travail sont sécurisées.

Avec des versions de client ou d'agent antérieures, les dossiers et les fichiers de redirection de lecteur client sont envoyés sur le réseau sans chiffrement et peuvent contenir des données sensibles, selon le contenu redirigé.

Si le tunnel sécurisé est activé, les connexions de redirection du lecteur client entre Horizon Client et View Secure Gateway sont sécurisées, mais les connexions entre View Secure Gateway et les machines de poste de travail ne sont pas chiffrées. Si le tunnel sécurisé est désactivé, les connexions de redirection du lecteur client entre Horizon Client et les machines de poste de travail ne sont pas chiffrées.

Pour vous assurer que ces données ne peuvent pas être surveillées sur le réseau, utilisez la redirection du lecteur client uniquement sur un réseau sécurisé si Horizon Client est antérieur à la version 3.5 ou si l'agent est antérieur à la version 6.2.

L'option d'installation **Redirection du lecteur client** dans le programme d'installation de l'agent est sélectionnée par défaut. Il vous est conseillé d'activer l'option d'installation **Redirection du lecteur client** uniquement sur les pools de postes de travail où les utilisateurs requièrent cette fonctionnalité.

## Utiliser une stratégie de groupe pour désactiver la redirection du lecteur client

Vous pouvez désactiver la redirection du lecteur client en configurant un paramètre de stratégie de groupe Services Bureau à distance Microsoft pour des postes de travail distants et des hôtes RDS dans Active Directory.

Pour plus d'informations sur la redirection du lecteur client, consultez le document *Utilisation de VMware Horizon Client* pour le type spécifique de périphérique client de poste de travail. Allez sur https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

---

**Remarque** Ce paramètre remplace le registre local et les paramètres des Stratégies de carte à puce qui activent la fonctionnalité de redirection du lecteur client.

---

### Prérequis

Si le déploiement d'View inclut un pare-feu dorsal entre vos serveurs de sécurité de la zone DMZ et votre réseau interne, assurez-vous que le pare-feu dorsal autorise le trafic vers le port 9427 de vos postes de travail mono-utilisateur et RDS. Des connexions TCP sur le port 9427 sont requises pour prendre en charge la redirection du lecteur client.

### Procédure

1. Dans l'Éditeur de stratégie de groupe, accédez à **Configuration de l'ordinateur\Règles\Modèles d'administration\Composants Windows\Services Bureau à distance\Hôte de session de poste de travail distant\Redirection de périphériques et de ressources**.

   Ce chemin de navigation concerne Active Directory sur Windows Server 2012. Le chemin de navigation est différent sur d'autres systèmes d'exploitation Windows.

2. Activez le paramètre de stratégie de groupe **Ne pas autoriser la redirection de lecteur**.

## Utiliser des paramètres de registre pour configurer la redirection du lecteur client

Vous pouvez utiliser des paramètres de clé de registre Windows pour contrôler le comportement de la redirection du lecteur client sur un poste de travail distant. Cette fonctionnalité requiert Horizon Agent 7.0 ou version ultérieure et Horizon Client 4.0 ou version ultérieure.

Les paramètres de registre Windows qui contrôlent le comportement de la redirection du lecteur client sur un poste de travail distant se trouvent dans le chemin d'accès suivant :

```
HKLM\Software\VMware, Inc.\VMware TSDR
```

Vous pouvez utiliser l'Éditeur du Registre Windows sur le poste de travail distant pour modifier les paramètres de registre locaux.

---

**Remarque** Les stratégies de redirection du lecteur client définies avec Stratégies de carte à puce sont prioritaires sur les paramètres de registre locaux.

---

### Désactivation de la redirection du lecteur client

Pour désactiver la redirection du lecteur client, créez une valeur de chaîne `disabled` et définissez-la sur `true`.

```
HKLM\Software\VMware, Inc.\VMware TSDR\disabled=true
```

La valeur est `false` (activée) par défaut.

### Empêcher l'accès en écriture à des dossiers partagés

Pour empêcher l'accès en écriture à tous les dossiers partagés avec le poste de travail distant, créez une valeur de chaîne `permissions` et définissez-la sur une chaîne qui commence par `r`, sauf pour `rw`.

```
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
```

La valeur est `rw` (tous les dossiers partagés sont accessibles en lecture et en écriture) par défaut.

### Partage de dossiers spécifiques

Pour partager des dossiers spécifiques avec le poste de travail distant, créez une clé `default shares` et créez une sous-clé pour chaque dossier à partager avec le poste de travail distant. Pour chaque sous-clé, créez une valeur de chaîne `name` et définissez-la sur le chemin d'accès du dossier à partager. L'exemple suivant partage les dossiers `C:\ebooks` et `C:\spreadsheets`.

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f1\name=C:\ebooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f2\name=C:\spreadsheets
```

Si vous définissez `name` sur `*all`, tous les lecteurs clients sont partagés avec le poste de travail distant. Le paramètre `*all` n'est pris en charge que sur les systèmes clients Windows.

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\1st\name=*all
```

Pour empêcher le client de partager d'autres dossiers (c'est-à-dire des dossiers non spécifiés avec la clé `default shares`), créez une valeur de chaîne `ForcedByAdmin` et définissez-la sur `true`.

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
```

Lorsque la valeur est `true`, la boîte de dialogue Partage n'apparaît pas quand les utilisateurs se connectent au poste de travail distant dans Horizon Client. La valeur est `false` (les clients peuvent partager des dossiers supplémentaires) par défaut.

L'exemple suivant partage les dossiers `C:\ebooks` et `C:\spreadsheets`, met les deux dossiers en lecture seule et empêche le client de partager des dossiers supplémentaires.

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f1\name=C:\ebooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f2\name=C:\spreadsheets
```

# Utilisation de périphériques USB avec des applications et postes de travail distants

# 15

Les administrateurs peuvent configurer l'utilisation des périphériques USB, tels que des clés USB, des caméras, des périphériques VoIP (voice-over-IP) et des imprimantes, à partir d'un poste de travail distant. Cette fonctionnalité est appelée redirection USB, et elle prend en charge l'utilisation des protocoles d'affichage Blast Extreme, PCoIP et Microsoft RDP. Un poste de travail distant peut recevoir jusqu'à 128 périphériques USB.

Vous pouvez également rediriger des clés et des disques durs USB localement connectés pour une utilisation dans des postes de travail et des applications RDS. D'autres types de périphériques USB, notamment des périphériques de stockage, ne sont pas pris en charge dans des postes de travail et des applications RDS.

Lorsque vous utilisez cette fonctionnalité dans des pools de postes de travail qui sont déployés sur des machines mono-utilisateur, la plupart des périphériques USB raccordés au système client local deviennent disponibles à partir d'un poste de travail distant. Vous pouvez même vous connecter à un iPad et le gérer depuis un poste de travail distant. Par exemple, vous pouvez synchroniser votre iPad avec l'application iTunes installée sur votre poste de travail distant. Sur certains périphériques clients, comme les ordinateurs Windows et Mac OS X, les périphériques USB sont répertoriés dans un menu d'Horizon Client. Vous utilisez le menu pour connecter et déconnecter les périphériques.

Dans la plupart des cas, vous ne pouvez pas utiliser simultanément un périphérique USB sur votre système client et sur votre application ou poste de travail distant. Seuls quelques types de périphériques USB peuvent être partagés entre un poste de travail distant et l'ordinateur local. Ces périphériques sont notamment les lecteurs de carte à puce et les périphériques d'interface utilisateur tels que les claviers et les dispositifs de pointage.

Les administrateurs peuvent spécifier à quels types de périphériques USB les utilisateurs finaux sont autorisés à se connecter. Pour les périphériques composites qui contiennent plusieurs types de périphériques, tels qu'un périphérique d'entrée vidéo et un périphérique de stockage, sur certains systèmes clients, les administrateurs peuvent diviser le périphérique pour qu'un périphérique (par exemple, le périphérique d'entrée vidéo) soit autorisé mais pas l'autre (par exemple, le périphérique de stockage).

La fonction de redirection USB n'est disponible que sur certains types de clients. Pour savoir si cette fonctionnalité est prise en charge sur un type de client particulier, consultez la matrice de prise en charge des fonctionnalités incluse dans le document « Utilisation de VMware Horizon Client » pour le type spécifique de poste de travail ou d'appareil mobile client. Allez sur https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

**Important** Lorsque vous déployez la fonctionnalité de redirection USB, vous pouvez effectuer des opérations pour protéger votre organisation des vulnérabilités de sécurité pouvant affecter les périphériques USB. Reportez-vous à la section « Déploiement de périphériques USB dans un environnement View sécurisé », page 254.

Ce chapitre aborde les rubriques suivantes :



## Limitations concernant les types de périphérique USB

Bien qu'View n'empêche pas de manière explicite les périphériques de fonctionner sur un poste de travail distant, des facteurs tels que la latence et la bande passante réseau permettent à certains périphériques de fonctionner mieux que d'autres. Par défaut, l'utilisation de certains périphériques est automatiquement filtrée ou bloquée.

Dans Horizon 6.0.1, avec Horizon Client 3.1 ou version ultérieure, vous pouvez brancher des périphériques USB 3.0 sur les ports USB 3.0 sur la machine cliente, sur des clients Windows, Linux et Mac OS X. Les périphériques USB 3.0 sont uniquement pris en charge avec un flux unique. Dans la mesure où la prise en charge de flux multiples n'est pas mise en œuvre dans cette version, les performances des périphériques USB ne sont pas améliorées. Certains périphériques USB 3.0 qui nécessitent un haut débit constant pour fonctionner correctement risquent de ne pas fonctionner dans une session VDI en raison de la latence réseau.

Dans les versions antérieures de View, bien que les périphériques USB 3.0 super rapides ne soient pas pris en charge, ils fonctionnent lorsqu'ils sont connectés à un port USB 2.0 sur la machine cliente. Cependant, il peut y avoir des exceptions, selon le type de jeu de puces USB sur la carte mère du système client.

Les types de périphériques suivants ne conviennent pas à la redirection USB vers un poste de travail distant qui est déployé sur une machine mono-utilisateur :

- En raison des besoins en bande passante des webcams qui consomment généralement plus 60 Mbits/s de bande passante, les webcams ne sont pas prises en charge via la redirection USB. Pour les webcams, vous pouvez utiliser la fonctionnalité Audio-vidéo en temps réel.
- La redirection de périphériques audio USB dépend de l'état du réseau et n'est pas fiable. Certains périphériques requièrent un débit de données élevé même lorsqu'ils sont inactifs. Si vous disposez de la fonctionnalité Audio-vidéo en temps réel, les périphériques d'entrée et de sortie audio fonctionneront correctement à l'aide de cette fonctionnalité et vous n'avez pas besoin d'utiliser la redirection USB pour ces périphériques.
- La gravure de CD/DVD USB n'est pas prise en charge.
- Les performances de certains périphériques USB varient considérablement, en fonction de la latence et de la fiabilité du réseau, en particulier sur un réseau étendu. Par exemple, une demande de lecture d'un seul périphérique de stockage USB nécessite trois allers-retours entre le client et le poste de travail distant. La lecture d'un fichier complet peut nécessiter plusieurs opérations de lecture USB, et plus la latence est grande, plus l'aller-retour prendra du temps.

Selon le format utilisé, la structure du fichier peut être très volumineuse. Des lecteurs de disques USB de taille importante peuvent nécessiter plusieurs minutes avant d'apparaître sur le poste de travail. Le formatage d'un périphérique USB en NTFS plutôt qu'en FAT permet de diminuer le délai de connexion initial. Un lien réseau non fiable peut entraîner plusieurs tentatives, ce qui diminue davantage les performances.

De la même façon, les lecteurs de CD/DVD USB, ainsi que les scanners et les périphériques tactiles comme les tablettes de signature, ne fonctionnent pas correctement sur un réseau latent tel qu'un réseau étendu.

- La redirection de scanners USB dépend de l'état du réseau, et les numérisations peuvent être anormalement longues.

Vous pouvez rediriger les types de périphériques suivants vers un poste de travail ou une application RDS :

- clés USB
- disques durs USB

Vous ne pouvez pas rediriger d'autres types de périphériques USB (par exemple, d'autres types de périphériques de stockage USB tels que les lecteurs de stockage de sécurité et les CD-ROM USB) vers un poste de travail ou une application RDS.

## Présentation de la configuration de la redirection USB

Pour configurer votre déploiement afin que les utilisateurs finaux puissent connecter des périphériques amovibles, par exemple des clés USB, des appareils photo et des casques audio, vous devez installer certains composants sur le poste de travail distant ou l'hôte RDS et le périphérique client, et vérifier que le paramètre général des périphériques USB est activé dans View Administrator.

Cette liste de contrôle inclut des tâches obligatoires et facultatives pour la configuration de la redirection USB dans votre entreprise.

La fonctionnalité de redirection USB n'est disponible que sur certains types de clients, par exemple Windows, Mac OS X et des clients Linux fournis par des partenaires. Pour savoir si cette fonctionnalité est prise en charge sur un type de client particulier, reportez-vous à la matrice de prise en charge des fonctionnalités incluse dans le document « Utilisation de VMware Horizon Client » pour le type spécifique de périphérique client. Allez sur https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html.

---

**Important** Lorsque vous déployez la fonctionnalité de redirection USB, vous pouvez effectuer des opérations pour protéger votre organisation des vulnérabilités de sécurité pouvant affecter les périphériques USB. Par exemple, vous pouvez utiliser des paramètres de stratégie de groupe pour désactiver Redirection USB pour certains postes de travail distants et utilisateurs, ou pour limiter les types de périphériques USB pouvant être redirigés. Reportez-vous à la section « Déploiement de périphériques USB dans un environnement View sécurisé », page 254.

---

1. Lors de l'exécution de l'assistant d'installation d'Horizon Agent sur la source du poste de travail distant ou l'hôte RDS, veillez à inclure le composant Redirection USB.

   par défaut. Ce composant est désélectionné par défaut. Vous devez sélectionner le composant pour l'installer.

2. Lors de l'exécution de l'assistant d'installation de VMware Horizon Client sur le système client, veillez à inclure le composant Redirection USB.

   Ce composant est inclus par défaut.

3. Vérifiez que l'accès aux périphériques USB à partir d'un poste de travail distant ou une application est activé dans View Administrator.

   Dans View Administrator, accédez à **Règles > Règles générales** et vérifiez que **Accès USB** est défini sur **Autoriser**.

4 (Facultatif) Configurez les stratégies de groupe d'Horizon Agent pour spécifier les types de périphériques qui peuvent être redirigés.

   Reportez-vous à la section « Utilisation de règles pour contrôler la redirection USB », page 257.

5 (Facultatif) Configurez des paramètres similaires sur le périphérique client.

   Vous pouvez également préciser si les périphériques sont automatiquement connectés lorsque Horizon Client se connecte à l'application ou au poste de travail distant, ou lorsque l'utilisateur final branche un périphérique USB. La méthode de configuration des paramètres USB sur le périphérique client dépend du type de périphérique. Par exemple, pour les points de terminaison clients Windows, vous pouvez configurer des stratégies de groupe, tandis que pour les points de terminaison Mac OS X, vous utilisez une commande de ligne de commande. Pour obtenir des instructions, reportez-vous au document « Utilisation de VMware Horizon Client » pour le type de périphérique client spécifique.

6 Demandez aux utilisateurs finaux de se connecter à une application ou un poste de travail distant, et de brancher leur périphérique USB sur leur système client local.

   Si le pilote du périphérique USB n'est pas déjà installé sur le poste de travail distant ou l'hôte RDS, le système d'exploitation invité détecte le périphérique USB et recherche un pilote adéquat, comme il le ferait sur un ordinateur Windows physique.

## Trafic réseau et redirection USB

La redirection USB fonctionne indépendamment du protocole d'affichage (RDP ou PCoIP) et le trafic USB utilise habituellement le port TCP 32111.

Le trafic réseau entre un système client et une application ou un poste de travail distant peut prendre différentes routes, selon que le système client se trouve sur le réseau de l'entreprise et en fonction de la façon dont l'administrateur a choisi de configurer la sécurité.

1 Si le système client se trouve sur le réseau de l'entreprise, pour qu'une connexion directe puisse s'établir entre le client et le poste de travail ou l'application, le trafic USB utilise le port TCP 32111.

2 Si le système client se trouve à l'extérieur du réseau de l'entreprise, le client peut se connecter via un serveur de sécurité View.

   Un serveur de sécurité réside dans une zone DMZ et agit comme un hôte proxy pour les connexions dans votre réseau approuvé. Cette conception fournit une couche supplémentaire de sécurité en protégeant l'instance du Serveur de connexion View contre l'Internet public et en forçant toutes les demandes de session non protégées via le serveur de sécurité.

   Un déploiement de serveur de sécurité basé sur une zone DMZ requiert l'ouverture de quelques ports sur le pare-feu afin d'autoriser des clients à se connecter à des serveurs de sécurité dans la zone DMZ. Vous devez également configurer des ports pour la communication entre des serveurs de sécurité et les instances du Serveur de connexion View sur le réseau interne.

   Pour plus d'informations sur les ports spécifiques, reportez-vous à « Règles de pare-feu pour les serveurs de sécurité basés sur une zone DMZ » dans le document *Guide de planification de l'architecture de View*.

3 Si le système client se trouve à l'extérieur du réseau de l'entreprise, vous pouvez utiliser View Administrator pour activer le tunnel sécurisé HTTPS. Le client établit ensuite une autre connexion HTTPS avec l'hôte du Serveur de connexion View ou du serveur de sécurité lorsque des utilisateurs se connectent à une application ou un poste de travail distant. La connexion est établie par tunnel à l'aide du port HTTPS 443 vers le serveur de sécurité, puis les connexions ultérieures pour le trafic USB entre le serveur et l'application ou le poste de travail distant utilisent le port TCP 32111. Les performances du périphérique USB sont légèrement dégradées lors de l'utilisation de ce tunnel.

**Remarque** Si vous utilisez un client ultra léger, le trafic USB est redirigé à l'aide d'un canal virtuel PCoIP et ne passe pas par le port TCP 32111. Les données sont encapsulées et chiffrées par PCoIP Secure Gateway à l'aide du port TCP/UDP 4172. Si vous utilisez uniquement des clients ultra légers, il n'est pas nécessaire d'ouvrir le port TCP 32111.

## Connexions automatiques aux périphériques USB

Sur certains systèmes clients, les administrateurs, les utilisateurs finaux ou les deux peuvent configurer des connexions automatiques de périphériques USB à un poste de travail distant. Il est possible d'établir une connexion automatique lorsque l'utilisateur branche un périphérique USB sur le système client ou lorsque le client se connecte au poste de travail distant.

Certains périphériques comme les smartphones et les tablettes ont besoin de connexions automatiques, car ils sont redémarrés, et donc déconnectés, pendant une mise à niveau. Si ces périphériques ne sont pas configurés pour se reconnecter automatiquement au poste de travail distant, après avoir redémarré suite à la mise à niveau ils se connecteront plutôt au système client local.

Les propriétés de configuration des connexions USB automatiques que les administrateurs définissent sur le client ou que les utilisateurs finaux définissent à l'aide d'un élément de menu d'Horizon Client s'appliquent à tous les périphériques USB, sauf si ceux-ci sont configurés pour être exclus de la redirection USB. Par exemple, dans certaines versions de clients, les webcams et les microphones sont exclus de la redirection USB par défaut, car ces périphériques fonctionnent mieux avec la fonctionnalité Audio-vidéo en temps réel. Dans certains cas, un périphérique USB peut ne pas être exclu de la redirection par défaut, mais nécessiter que les administrateurs l'excluent de façon explicite de la redirection. Par exemple, les types de périphériques USB suivants ne sont pas recommandés pour la redirection USB et ne doivent pas être connectés automatiquement à un poste de travail distant :

- Périphériques Ethernet USB. Si vous redirigez un périphérique Ethernet USB, votre système client peut perdre la connectivité réseau si ce périphérique est le seul périphérique Ethernet.
- Périphériques à écran tactile. Si vous redirigez un périphérique à écran tactile, le poste de travail distant recevra une entrée tactile mais pas une entrée de clavier.

Si vous avez défini le poste de travail distant pour qu'il se connecte automatiquement aux périphériques USB, vous pouvez configurer une stratégie visant à exclure des périphériques spécifiques, comme les écrans tactiles et les périphériques réseau. Pour plus d'informations, reportez-vous à la section « Configuration de paramètres de règle de filtre pour des périphériques USB », page 261.

Sur les clients Windows, plutôt que de définir des paramètres qui connectent automatiquement tous les périphériques à l'exception de ceux qui sont exclus, vous pouvez modifier un fichier de configuration sur le client qui définit Horizon Client de sorte qu'il reconnecte uniquement un ou plusieurs périphériques spécifiques, comme les smartphones et les tablettes, au poste de travail distant. Pour plus d'information, reportez-vous à *Utilisation de VMware Horizon Client pour Windows*.

# Déploiement de périphériques USB dans un environnement View sécurisé

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

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

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

## Désactivation de la redirection USB pour tous les types de périphériques

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

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

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

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

Si vous définissez la stratégie `Exclude All Devices` sur **`true`**, Horizon Client empêche la redirection de tous les périphériques USB. Vous pouvez utiliser d'autres paramètres de règle pour autoriser la redirection de périphériques spécifiques ou de familles de périphériques. Si vous définissez la stratégie sur **`false`**, Horizon Client autorise la redirection de tous les périphériques USB sauf ceux qui sont bloqués par d'autres

paramètres de stratégie. Vous pouvez définir la stratégie dans Horizon Agent et Horizon Client. Le tableau suivant décrit comment la stratégie `Exclude All Devices` que vous pouvez définir pour Horizon Agent et Horizon Client se combinent pour produire une stratégie efficace pour l'ordinateur client. Par défaut, tous les périphériques USB sont autorisés à être redirigés, sauf blocage contraire.

**Tableau 15-1.** Effet de la combinaison de règles Exclure tous les périphériques

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

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

Ces stratégies sont incluses dans le fichier de modèle d'administration de configuration d'Horizon Agent (`vdm_agent.adm`). Pour plus d'informations, reportez-vous à la section « Paramètres USB du modèle d'administration de configuration d'Horizon Agent », page 265.

## Désactivation de la redirection USB pour des périphériques spécifiques

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

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

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

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

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

```
ExcludeAllDevices   Enabled

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

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

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

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

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

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

```
ExcludeAllDevices     Enabled

IncludeDeviceFamily   o:storage
```

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

Sachez que si vous bloquez le port TCP 32111 pour désactiver l'accès externe aux périphériques USB, la synchronisation de fuseau horaire ne fonctionnera pas, car le port 32111 est également utilisé pour la synchronisation de fuseau horaire. Pour les clients zéro, le trafic USB est intégré dans un canal virtuel sur le port UDP 4172. Comme le port 4172 est utilisé pour le protocole d'affichage ainsi que pour la redirection USB, vous ne pouvez pas bloquer le port 4172. Si nécessaire, vous pouvez désactiver la redirection USB sur les clients zéro. Pour plus d'informations, reportez-vous à la documentation du produit client zéro et contactez son fournisseur.

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

## Utilisation de fichiers journaux pour le dépannage et pour déterminer les ID de périphérique USB

Des fichiers journaux pour USB très utiles se trouvent sur le système client et sur le système d'exploitation du poste de travail distant ou l'hôte RDS. Utilisez les fichiers journaux de ces deux emplacements à des fins de dépannage. Pour trouver les ID de produits de périphériques spécifiques, utilisez les journaux côté client.

Si vous tentez de configurer les fonctionnalités de partitionnement et de filtre de périphériques USB, ou si vous tentez de déterminer pourquoi un périphérique particulier ne s'affiche pas dans un menu Horizon Client, effectuez une recherche dans les journaux côté client. Des journaux clients sont produits pour l'arbitrage USB et le service USB d'Horizon View. La journalisation sur les clients Windows et Linux est activée par défaut. Sur les clients Mac OS X, la journalisation est désactivée par défaut. Pour activer la journalisation sur les clients Mac OS X, reportez-vous à *Utilisation de VMware Horizon Client pour Mac OS X*.

Lorsque vous configurez des stratégies pour le fractionnement et le filtrage de périphériques USB, certaines valeurs que vous définissez nécessitent le VID (ID de fournisseur) et le PID (ID de produit) du périphérique USB. Pour connaître le VID et le PID, vous pouvez rechercher le nom du produit sur Internet, associé à `vid` et `pid`. Vous pouvez également consulter le fichier journal côté client après la connexion du périphérique USB au système local lorsqu'Horizon Client est en cours d'exécution. Le tableau suivant montre l'emplacement par défaut des fichiers journaux.

**Tableau 15-2.** Emplacements des fichiers journaux

| Client ou Agent | Chemin d'accès aux fichiers journaux |
|---|---|
| Client Windows | `%PROGRAMDATA%\VMware\VDM\logs\debug-*.txt`<br>`C:\Windows\Temp\vmware-SYSTEM\vmware-usbarb-*.log` |
| Horizon Agent | `%PROGRAMDATA%\VMware\VDM\logs\debug-*.txt` |
| Client Mac OS X | `/var/root/Library/Logs/VMware/vmware-view-usbd-xxxx.log`<br>`/Library/Logs/VMware/vmware-usbarbitrator-xxxx.log` |
| Client Linux | (Emplacement par défaut) `/tmp/vmware-root/vmware-view-usbd-*.log` |

Si un problème sur le périphérique se produit après la redirection de ce dernier vers l'application ou le poste de travail distant, consultez les journaux côté client et côté agent.

## Utilisation de règles pour contrôler la redirection USB

Vous pouvez configurer des stratégies USB pour l'application ou le poste de travail distant (Horizon Agent) et Horizon Client. Ces stratégies spécifient si le périphérique client doit fractionner des périphériques USB composites en composants distincts pour la redirection. Vous pouvez fractionner les périphériques pour limiter les types de périphériques USB que le client met à disposition pour la redirection et pour qu' Horizon Agent empêche le transfert de certains périphériques USB à partir d'un ordinateur client.

Si d'anciennes versions d'Horizon Agent ou d'Horizon Client sont installées, certaines fonctionnalités des stratégies de redirection USB ne sont pas disponibles. Tableau 15-3 indique comment View applique les stratégies pour différentes combinaisons d'Horizon Agent et d'Horizon Client.

**Tableau 15-3.** Compatibilité des paramètres de stratégie USB

| Version d'Horizon Agent | Version d'Horizon Client | Effet des paramètres de stratégie USB sur la redirection USB |
|---|---|---|
| 5.1 ou version ultérieure | 5.1 ou version ultérieure | Les paramètres de stratégie USB s'appliquent à Horizon Agent et à Horizon Client. Vous pouvez utiliser les paramètres de stratégie USB d'Horizon Agent pour empêcher le transfert de périphériques USB vers un poste de travail. Horizon Agent peut envoyer des paramètres de stratégie de fractionnement et de filtrage de périphériques à Horizon Client. Vous pouvez utiliser les paramètres de stratégie USB d'Horizon Client pour empêcher la redirection de périphériques USB d'un ordinateur client vers un poste de travail.<br>**Remarque** Dans View Agent 6.1 ou version ultérieure et Horizon Client 3.3 ou version ultérieure, ces paramètres de stratégie de redirection USB s'appliquent aux postes de travail et applications RDS ainsi qu'aux postes de travail distants qui s'exécutent sur des machines mono-utilisateur. |
| 5.1 ou version ultérieure | 5.0.x ou version antérieure | Les paramètres de stratégie USB s'appliquent uniquement à Horizon Agent. Vous pouvez utiliser les paramètres de stratégie USB d'Horizon Agent pour empêcher le transfert de périphériques USB vers un poste de travail. Vous ne pouvez pas utiliser les paramètres de stratégie USB d'Horizon Client pour contrôler les périphériques pouvant être redirigés d'un ordinateur client vers un poste de travail. Horizon Client ne peut pas recevoir de paramètres de stratégie de fractionnement et de filtrage de périphériques provenant d'Horizon Agent. Les paramètres de Registre existants pour la redirection USB par Horizon Client demeurent valides. |

**Tableau 15-3.** Compatibilité des paramètres de stratégie USB (suite)

| Version d'Horizon Agent | Version d'Horizon Client | Effet des paramètres de stratégie USB sur la redirection USB |
|---|---|---|
| 5.0.x ou version antérieure | 5.1 ou version ultérieure | Les paramètres de stratégie USB s'appliquent uniquement à Horizon Client. Vous pouvez utiliser les paramètres de stratégie USB d'Horizon Client pour empêcher la redirection de périphériques USB d'un ordinateur client vers un poste de travail. Vous ne pouvez pas utiliser les paramètres de stratégie USB d'Horizon Agent pour empêcher le transfert de périphériques USB vers un poste de travail. Horizon Agent ne peut pas envoyer des paramètres de stratégie de fractionnement et de filtrage de périphériques à Horizon Client. |
| 5.0.x ou version antérieure | 5.0.x ou version antérieure | Les paramètres de stratégie USB ne s'appliquent pas. Les paramètres de Registre existants pour la redirection USB par Horizon Client demeurent valides. |

Si vous mettez à niveau Horizon Client, tous les paramètres de Registre existants pour la redirection USB, par exemple `HardwareIdFilters`, restent valides jusqu'à ce que vous définissiez des stratégies USB pour Horizon Client.

Sur les périphériques clients qui ne prennent pas en charge les stratégies USB côté client, vous pouvez utiliser les stratégies USB pour Horizon Agent afin de contrôler les périphériques USB autorisés à être transférés du client vers un poste de travail.

## Configuration de paramètres de règle de fractionnement de périphérique pour des périphériques USB composites

Les périphériques USB composites sont composés d'au moins deux périphériques distincts, tels qu'un périphérique d'entrée vidéo et un périphérique de stockage, ou un microphone et une souris. Si vous souhaitez rendre un ou plusieurs des composants disponibles pour la redirection, vous pouvez fractionner le périphérique composite en interfaces de son composant, exclure certaines interfaces de la redirection et en inclure d'autres.

Vous pouvez définir une stratégie qui fractionne automatiquement les périphériques composites. Si le fractionnement automatique de périphériques ne fonctionne pas pour un périphérique spécifique ou s'il ne produit pas les résultats requis par votre application, vous pouvez fractionner manuellement les périphériques composites.

### Fractionnement automatique de périphérique

Si vous activez le fractionnement automatique de périphérique, View tente de fractionner les fonctions ou les périphériques en un périphérique composite selon les règles de filtre en vigueur. Par exemple, un dictaphone peut être fractionné automatiquement de sorte que la souris demeure locale pour le client, mais que le reste des périphériques soit transmis au poste de travail distant.

Le tableau suivant indique comment la valeur du paramètre `Allow Auto Device Splitting` détermine si Horizon Client tente de fractionner automatiquement des périphériques USB composites. Par défaut, le fractionnement automatique est désactivé.

**Tableau 15-4.** Effet de la combinaison de règles de désactivation du fractionnement automatique

| Stratégie Autoriser le fractionnement automatique de périphérique sur Horizon Agent | Stratégie Autoriser le fractionnement automatique de périphérique sur Horizon Client | Règle Autoriser le fractionnement automatique de périphérique effective combinée |
|---|---|---|
| `Allow – Default Client Setting` | **`false`** (fractionnement automatique désactivé) | Fractionnement automatique désactivé |
| `Allow – Default Client Setting` | **`true`** (fractionnement automatique activé) | Fractionnement automatique activé |
| `Allow – Default Client Setting` | Non défini | Fractionnement automatique activé |

**Tableau 15-4.** Effet de la combinaison de règles de désactivation du fractionnement automatique (suite)

| Stratégie Autoriser le fractionnement automatique de périphérique sur Horizon Agent | Stratégie Autoriser le fractionnement automatique de périphérique sur Horizon Client | Règle Autoriser le fractionnement automatique de périphérique effective combinée |
|---|---|---|
| `Allow – Override Client Setting` | Aucun ou non défini | Fractionnement automatique activé |
| Non défini | Non défini | Fractionnement automatique désactivé |

**Remarque** Ces stratégies sont incluses dans le fichier de modèle d'administration de configuration d'Horizon Agent (`vdm_agent.adm`). Pour plus d'informations, reportez-vous à la section « Paramètres USB du modèle d'administration de configuration d'Horizon Agent », page 265.

Par défaut, View désactive le fractionnement automatique et exclut de la redirection tous les composants de sortie audio, de carte à puce, de clavier ou de souris d'un périphérique USB composite.

View applique les paramètres de stratégie de fractionnement de périphériques avant d'appliquer des paramètres de stratégie de filtre. Si vous avez activé le fractionnement automatique et que vous n'excluez pas explicitement un périphérique USB composite du fractionnement en spécifiant ses ID de fournisseur et de produit, View examine chaque interface du périphérique USB composite afin de décider des interfaces à exclure ou à inclure selon les paramètres de stratégie de filtre. Si vous avez désactivé le fractionnement automatique de périphérique et que vous ne spécifiez pas explicitement les ID de fournisseur et de produit d'un périphérique USB composite que vous souhaitez fractionner, View applique les paramètres de stratégie de filtre à l'ensemble du périphérique.

Si vous activez le fractionnement automatique, vous pouvez utiliser la règle `Exclude Vid/Pid Device From Split` pour spécifier les périphériques USB composites que vous voulez exclure du fractionnement.

## Fractionnement manuel de périphérique

Vous pouvez utiliser la règle `Split Vid/Pid Device` pour spécifier les ID de fournisseur et de produit d'un périphérique USB composite que vous voulez fractionner. Vous pouvez également spécifier les interfaces des composants d'un périphérique USB composite que vous voulez exclure de la redirection. View n'applique aucun paramètre de stratégie de filtre aux composants que vous excluez de cette façon.

**Important** Si vous utilisez la stratégie `Split Vid/Pid Device`, View n'inclut pas automatiquement les composants que vous n'avez pas explicitement exclus. Vous devez spécifier une règle de filtre telle que `Include Vid/Pid Device` pour inclure ces composants.

Tableau 15-5 indique les modificateurs définissant la façon dont Horizon Client gère un paramètre de stratégie de fractionnement de périphérique Horizon Agent si un paramètre de stratégie de fractionnement de périphérique équivalent pour Horizon Client est présent. Ces modificateurs s'appliquent à tous les paramètres de règles de fractionnement de périphérique.

**Tableau 15-5.** Modificateurs de fractionnement pour des paramètres de règle de fractionnement de périphérique sur Horizon Agent

| Modificateur | Description |
|---|---|
| **m** (fusionner) | Horizon Client applique le paramètre de stratégie de fractionnement de périphérique Horizon Agent en plus du paramètre de stratégie de fractionnement de périphérique Horizon Client. |
| **o** (remplacer) | Horizon Client utilise le paramètre de stratégie de fractionnement de périphérique Horizon Agent à la place du paramètre de stratégie de fractionnement de périphérique Horizon Client. |

Tableau 15-6 montre des exemples de la façon dont Horizon Client traite les paramètres de stratégie `Exclude Device From Split by Vendor/Product ID` lorsque vous spécifiez différents modificateurs de fractionnement.

**Tableau 15-6.** Exemples d'application de modificateurs de fractionnement sur des paramètres de règle de fractionnement de périphérique

| Exclure le périphérique du fractionnement par ID de fournisseur/de produit sur Horizon Agent | Exclure le périphérique du fractionnement par ID de fournisseur/de produit sur Horizon Client | Paramètre effectif de la stratégie Exclure le périphérique du fractionnement par ID de fournisseur/de produit utilisé par Horizon Client |
|---|---|---|
| `m:vid-XXXX_pid-XXXX` | `vid-YYYY_pid-YYYY` | `vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY` |
| `o:vid-XXXX_pid-XXXX` | `vid-YYYY_pid-YYYY` | `vid-XXXX_pid-XXXX` |
| `m:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY` | `vid-YYYY_pid-YYYY` | `vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY` |
| `o:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY` | `vid-YYYY_pid-YYYY` | `vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY` |

Horizon Agent n'applique pas les paramètres de stratégie de fractionnement de périphérique de son côté de la connexion.

Horizon Client évalue les paramètres de stratégie de fractionnement de périphérique dans l'ordre de priorité suivant.

- `Exclude Vid/Pid Device From Split`
- `Split Vid/Pid Device`

Un paramètre de règle de fractionnement de périphérique qui exclut un périphérique du fractionnement est prioritaire sur tout autre paramètre de règle pour fractionner le périphérique. Si vous définissez des interfaces ou des périphériques à exclure du fractionnement, Horizon Client exclut de la redirection les périphériques de composant correspondants.

## Exemples de définition de règles pour fractionner des périphériques USB composites

Définissez des stratégies de fractionnement pour des postes de travail afin d'exclure de la redirection les périphériques avec des ID de fournisseur et de produit spécifiques après le fractionnement automatique, et transmettez ces stratégies aux ordinateurs clients :

- Pour Horizon Agent, définissez la stratégie `Allow Auto Device Splitting` sur `Allow – Override Client Setting`.
- Pour Horizon Agent, définissez la stratégie `Exclude VidPid From Split` sur **`o:vid-`*`xxx`*`_pid-`*`yyyy`***, où *xxx* et *yyyy* sont les ID appropriés.

Autorisez le fractionnement automatique de périphérique pour des postes de travail et spécifiez des stratégies de fractionnement pour des périphériques spécifiques sur des ordinateurs clients :

- Pour Horizon Agent, définissez la stratégie `Allow Auto Device Splitting` sur `Allow – Override Client Setting`.
- Pour le périphérique client, définissez la stratégie de filtre `Include Vid/Pid Device` de façon qu'elle inclue le périphérique spécifique à fractionner, par exemple, **`vid-0781_pid-554c`**.
- Pour le périphérique client, définissez la stratégie `Split Vid/Pid Device` sur **`vid-0781_pid-554c(exintf:00;exintf:01)`**, par exemple, pour fractionner un périphérique USB composite spécifié afin d'exclure de la rediction l'interface 00 et l'interface 01.

## Configuration de paramètres de règle de filtre pour des périphériques USB

Les paramètres de stratégie de filtre que vous configurez pour Horizon Agent et Horizon Client déterminent les périphériques USB pouvant être redirigés d'un ordinateur client vers une application ou un poste de travail distant. Le filtrage des périphériques USB est généralement utilisé par les entreprises pour empêcher le recours à des périphériques de stockage de masse sur les postes de travail distants ou pour bloquer le transfert d'un type de périphérique spécifique, comme l'adaptateur USB vers Ethernet qui connecte le périphérique client au poste de travail distant.

Lorsque vous vous connectez à un poste de travail ou une application, Horizon Client télécharge les paramètres de stratégie USB d'Horizon Agent et les utilise avec les paramètres de stratégie USB d' Horizon Client afin de décider quels périphériques USB il vous autorisera à rediriger à partir de l'ordinateur client.

View applique tous les paramètres de stratégie de fractionnement de périphérique avant d'appliquer les paramètres de stratégie de filtre. Si vous avez fractionné un périphérique USB composite, View examine les interfaces de chacun des périphériques pour décider laquelle exclure ou inclure, conformément aux paramètres de stratégie de filtre. Dans le cas contraire, View applique les paramètres de stratégie de filtre à l'ensemble du périphérique.

Les stratégies de fractionnement de périphérique sont incluses dans le fichier de modèle d'administration pour la configuration d'Horizon Agent (`vdm_agent.adm`). Pour plus d'informations, reportez-vous à la section « Paramètres USB du modèle d'administration de configuration d'Horizon Agent », page 265.

### Interaction des paramètres USB appliqués par l'agent

Le tableau suivant présente les modificateurs qui spécifient de quelle manière Horizon Client gère un paramètre de stratégie de filtre d'Horizon Agent pour un paramètre applicable par l'agent, s'il existe un paramètre de stratégie de filtre équivalent pour Horizon Client.

**Tableau 15-7.** Modificateurs de filtre pour des paramètres exécutables par un agent

| Modificateur | Description |
|---|---|
| **`m`** (fusionner) | Horizon Client applique le paramètre de stratégie de filtre d'Horizon Agent en plus du paramètre de stratégie de filtre d'Horizon Client. En cas de paramètres booléens ou vrai/faux, si la stratégie du client n'est pas définie, les paramètres de l'agent sont utilisés. Si la stratégie du client est définie, les paramètres de l'agent sont ignorés, à l'exception du paramètre `Exclude All Devices`. Si la stratégie `Exclude All Devices` est définie du côté de l'agent, elle remplace le paramètre du client. |
| **`o`** (remplacer) | Horizon Client utilise le paramètre de stratégie de filtre d'Horizon Agent à la place de celui d'Horizon Client. |

Par exemple, la stratégie suivante du côté de l'agent remplace toutes les règles d'inclusion du côté du client, et une règle d'inclusion sera appliquée uniquement au périphérique VID-0911_PID-149a :

```
IncludeVidPid: o:VID-0911_PID-149a
```

Vous pouvez également utiliser des astérisques comme caractères génériques ; par exemple :
**`o:vid-0911_pid-****`**

**IMPORTANT** Si vous configurez le côté agent sans le modificateur **`o`** ou **`m`**, la règle de configuration est considérée comme non valide et sera ignorée.

### Interaction des paramètres USB interprétés par le client

Le tableau suivant présente les modificateurs qui spécifient de quelle manière Horizon Client gère un paramètre de stratégie de filtre d'Horizon Agent pour un paramètre interprété par le client.

**Tableau 15-8.** Modificateurs de filtre pour des paramètres interprétés par un client

| Modificateur | Description |
|---|---|
| `Default` (**`d`** dans le paramètre de registre) | En l'absence de paramètre de stratégie de filtre d'Horizon Client, Horizon Client utilise le paramètre de stratégie de filtre d'Horizon Agent.<br>S'il existe un paramètre de stratégie de filtre d'Horizon Client, Horizon Client applique celui-ci et ignore celui d'Horizon Agent. |
| `Override` (**`o`** dans le paramètre de registre) | Horizon Client utilise le paramètre de stratégie de filtre d'Horizon Agent à la place d'un paramètre de stratégie de filtre équivalent d'Horizon Client. |

Horizon Agent n'applique pas les paramètres de stratégie de filtre pour des paramètres interprétés par un client de son côté de la connexion.

Le tableau suivant montre les différentes manières dont Horizon Client traite les valeurs de l'option `Allow Smart Cards` lorsque vous spécifiez différents modificateurs de filtre.

**Tableau 15-9.** Exemples d'application de modificateurs de filtre sur des paramètres interprétés par un client

| Paramètre Autoriser les cartes à puce dans Horizon Agent | Paramètre Autoriser les cartes à puce dans Horizon Client | Paramètre de stratégie Autoriser les cartes à puce effectif utilisé par Horizon Client |
|---|---|---|
| `Disable – Default Client Setting` (**`d:false`** dans le paramètre de registre) | **`true`** (autoriser) | **`true`** (autoriser) |
| `Disable – Override Client Setting` (**`o:false`** dans le paramètre de registre) | **`true`** (autoriser) | **`false`** (désactiver) |

Si vous définissez la stratégie `Disable Remote Configuration Download` sur la valeur **`true`**, Horizon Client ignore les paramètres de stratégie de filtre qu'il reçoit d'Horizon Agent.

Horizon Agent applique toujours les paramètres de stratégie de filtre aux paramètres applicables par l'agent de son côté de la connexion, même si vous configurez Horizon Client afin qu'il utilise un paramètre de stratégie de filtre différent ou qu'il désactive le téléchargement de paramètres de stratégie de filtre par Horizon Client auprès d'Horizon Agent. Horizon Client ne signale pas qu'Horizon Agent empêche le transfert d'un périphérique.

## Priorité des paramètres

Horizon Client évalue les paramètres de stratégie de filtre selon un ordre de priorité. Un paramètre de règle de filtre qui exclut la redirection d'un périphérique correspondant est prioritaire sur le paramètre de règle de filtre équivalent qui inclut le périphérique. Si Horizon Client ne rencontre pas de paramètre de stratégie de filtre visant à exclure un périphérique, Horizon Client permet au périphérique d'être redirigé, sauf si vous avez défini la stratégie `Exclude All Devices` sur **`true`**. Toutefois, si vous avez configuré un paramètre de stratégie de filtre sur Horizon Agent afin d'exclure le périphérique, l'application ou le poste de travail bloque toute tentative de redirection du périphérique vers lui.

Horizon Client évalue les paramètres de stratégie de filtre par ordre de priorité, en tenant compte des paramètres d'Horizon Client et de ceux d'Horizon Agent, ainsi que des valeurs de modificateur que vous appliquez aux paramètres d'Horizon Agent. La liste suivante répertorie l'ordre de priorité, l'élément 1 ayant la priorité la plus élevée.

1. `Exclude Path`
2. `Include Path`
3. `Exclude Vid/Pid Device`
4. `Include Vid/Pid Device`
5. `Exclude Device Family`

6 `Include Device Family`

7 `Allow Audio Input Devices`, `Allow Audio Output Devices`, `Allow HIDBootable`, `Allow HID (Non Bootable and Not Mouse Keyboard)`, `Allow Keyboard and Mouse Devices`, `Allow Smart Cards` et `Allow Video Devices`

8 Règle `Exclude All Devices` effective combinée évaluée pour exclure ou inclure tous les périphériques USB

Vous pouvez définir les paramètres de stratégie de filtre `Exclude Path` et `Include Path` uniquement pour Horizon Client. Les paramètres de règle de filtre `Allow` qui font référence à des familles de périphériques séparés ont la même priorité.

Si vous configurez un paramètre de stratégie afin d'exclure les périphériques en fonction des valeurs d'ID de fournisseur et de produit, Horizon Client exclut un périphérique dont les valeurs d'ID de fournisseur et de produit correspondent à cette stratégie, même si vous auriez pu configurer une stratégie `Allow` pour la famille à laquelle appartient le périphérique.

L'ordre de priorité des paramètres de règle résout des conflits entre les paramètres de règle. Si vous configurez `Allow Smart Cards` pour autoriser la redirection de cartes à puce, tout paramètre de règle d'exclusion avec une priorité supérieure remplace ce paramètre. Par exemple, vous pouvez avoir configuré un paramètre de règle `Exclude Vid/Pid Device` pour exclure les périphériques à carte à puce avec un chemin ou des valeurs d'ID de fournisseur et de produit correspondants, ou vous pouvez avoir configuré un paramètre de règle `Exclude Device Family` qui exclut également la famille de périphériques `smart-card` entièrement.

Si vous avez configuré un paramètre de stratégie de filtre d'Horizon Agent, Horizon Agent évalue et applique les paramètres de stratégie de filtre dans l'ordre de priorité suivant sur l'application ou le poste de travail distant, l'élément 1 ayant la priorité la plus élevée.

1 `Exclude Vid/Pid Device`

2 `Include Vid/Pid Device`

3 `Exclude Device Family`

4 `Include Device Family`

5 Règle `Exclude All Devices` appliquée par un agent définie pour exclure ou inclure tous les périphériques USB

Horizon Agent applique cet ensemble limité de paramètres de règle de filtre de son côté de la connexion.

En définissant des paramètres de règle de filtre pour Horizon Agent, vous pouvez créer un paramètre de filtrage pour des ordinateurs client non gérés. Cette fonctionnalité vous permet également de bloquer le transfert des périphériques depuis les ordinateurs clients, même si les paramètres de stratégie de filtre d'Horizon Client autorisent la redirection.

Par exemple, si vous configurez une stratégie permettant à Horizon Client d'autoriser la redirection d'un périphérique, Horizon Agent bloque celui-ci si vous configurez une stratégie pour qu'Horizon Agent l'exclue.

## Exemples de définition de règles pour filtrer des périphériques USB

Les ID de fournisseurs et de produits utilisés dans ces exemples sont employés uniquement à titre d'exemple. Pour plus d'informations sur la détermination des ID de fournisseur et de produit d'un périphérique spécifique, reportez-vous à « Utilisation de fichiers journaux pour le dépannage et pour déterminer les ID de périphérique USB », page 256.

- Sur le client, excluez la redirection d'un périphérique particulier :

  ```
  Exclude Vid/Pid Device:     Vid-0341_Pid-1a11
  ```

- Bloquez la redirection de tous les périphériques de stockage vers ce pool d'applications ou de postes de travail. Utilisez un paramètre côté agent :

  ```
  Exclude Device Family:      o:storage
  ```

- Pour tous les utilisateurs d'un pool de postes de travail, bloquez les périphériques audio et vidéo pour vous assurer qu'ils seront toujours disponibles pour la fonctionnalité Audio-vidéo en temps réel. Utilisez un paramètre côté agent :

  ```
  Exclude Device Family:      o:video;audio
  ```

  Notez qu'une autre stratégie consisterait à exclure des périphériques spécifiques par ID de fournisseur et de produit.

- Sur le client, bloquez la redirection de tous les périphériques, à l'exception d'un périphérique particulier :

  ```
  Exclude All Devices:        true
  Include Vid/Pid Device:     Vid-0123_Pid-abcd
  ```

- Excluez tous les périphériques fabriqués par une entreprise spécifique, car ils posent problème à vos utilisateurs finaux. Utilisez un paramètre côté agent :

  ```
  Exclude Vid/Pid Device:     o:Vid-0341_Pid-*
  ```

- Sur le client, incluez deux périphériques spécifiques mais excluez tous les autres :

  ```
  Exclude All Devices:        true
  Include Vid/Pid Device:     Vid-0123_Pid-abcd;Vid-1abc_Pid-0001
  ```

## Familles de périphériques USB

Vous pouvez spécifier une famille lorsque vous créez des règles de filtrage USB pour Horizon Client ou pour View Agent ou Horizon Agent.

**Remarque** Certains périphériques ne lisent pas certaines familles de périphériques.

**Tableau 15-10.** Familles de périphériques USB

| Nom de la famille de périphériques | Description |
|---|---|
| `audio` | Tout périphérique d'entrée ou de sortie audio. |
| `audio-in` | Périphériques d'entrée audio, tels que des microphones. |
| `audio-out` | Périphériques de sortie audio, tels que des haut-parleurs et des écouteurs. |
| `bluetooth` | Périphériques connectés par Bluetooth. |
| `comm` | Périphériques de communication, tels que des modems et des adaptateurs réseau filaires. |
| `hid` | Périphériques d'interface humaine, à l'exclusion des claviers et des pointeurs. |
| `hid-bootable` | Périphériques d'interface humaine disponibles au démarrage, à l'exclusion des claviers et des pointeurs. |
| `imaging` | Périphériques graphiques tels que des scanners. |
| `keyboard` | Périphérique de type clavier. |
| `mouse` | Périphérique de pointage tel qu'une souris. |
| `other` | Famille non spécifiée. |
| `pda` | Assistants numériques personnels. |
| `physical` | Périphériques à retour de force, tels que les joysticks à retour de force. |
| `printer` | Périphériques d'impression. |

**Tableau 15-10.** Familles de périphériques USB (suite)

| Nom de la famille de périphériques | Description |
|---|---|
| `security` | Périphériques de sécurité, tels que des lecteurs d'empreintes digitales. |
| `smart-card` | Périphériques à carte à puce. |
| `storage` | Périphériques de stockage de masse tels que des disques à mémoire flash et des disques durs externes. |
| `unknown` | Famille inconnue. |
| `vendor` | Périphériques disposant de fonctions spécifiques au fournisseur. |
| `video` | Périphériques d'entrée vidéo. |
| `wireless` | Adaptateurs réseau sans fil. |
| `wusb` | Périphériques USB sans fil. |

## Paramètres USB du modèle d'administration de configuration d' Horizon Agent

Vous pouvez définir des paramètres de stratégie USB pour Horizon Agent et Horizon Client. Lors de la connexion, Horizon Client télécharge les paramètres de stratégie USB depuis Horizon Agent et les utilise avec les paramètres de stratégie USB d'Horizon Client, afin de décider des périphériques qu'il va rendre disponibles pour la redirection depuis l'ordinateur client.

Le fichier de modèle d'administration pour la configuration d'Horizon Agent (`vdm_agent.adm`) contient des paramètres de stratégie liés aux composants d'authentification et d'environnement d'Horizon Agent, notamment la redirection USB. Les paramètres s'appliquent au niveau de l'ordinateur. Horizon Agent lit de préférence les paramètres de l'objet de stratégie de groupe au niveau de l'ordinateur. Sinon, il lit ceux du registre dans `HKLM\Software\Policies\VMware, Inc.\VMware VDM\Agent\USB`.

### Paramètres pour la configuration du fractionnement de périphérique USB

Le tableau suivant décrit chaque paramètre de fractionnement de périphériques USB composites situé dans le fichier de modèle d'administration pour la configuration d'Horizon Agent. Horizon Agent n'applique pas ces paramètres. Horizon Agent transmet les paramètres à Horizon Client pour qu'il les interprète et les applique, selon que vous spécifiez le modificateur de fusion (`m`) ou de remplacement (`o`). Horizon Client utilise les paramètres pour décider s'il faut fractionner des périphériques USB composites en périphériques composants et exclure les périphériques composants de la redirection. Pour voir une description de la façon dont View applique les règles pour le fractionnement de périphériques USB composites, reportez-vous à la section « Configuration de paramètres de règle de fractionnement de périphérique pour des périphériques USB composites », page 258.

**Tableau 15-11.** Modèle de configuration d' Horizon Agent : paramètres de fractionnement de périphérique

| Paramètre | Propriétés |
|---|---|
| `Allow Auto Device Splitting`<br>Propriété : `AllowAutoDeviceSplitting` | Autorise le fractionnement automatique de périphériques USB composites.<br>La valeur par défaut est indéfinie, ce qui correspond à **`false`**. |
| `Exclude Vid/Pid Device From Split`<br>Propriété : `SplitExcludeVidPid` | Exclut un périphérique USB composite spécifié par des ID de fournisseur et de produit du fractionnement. Le format du paramètre est {`m`\|`o`}`:vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]...<br>Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (`*`) à la place de chiffres dans un ID.<br>Par exemple : **`o:vid-0781_pid-55**`**<br>La valeur par défaut n'est pas définie. |
| `Split Vid/Pid Device`<br>Propriété : `SplitVidPid` | Traite les composants d'un périphérique USB composite spécifiés par des ID de fournisseur et de produit en tant que périphériques séparés. Le format du paramètre est<br>{`m`\|`o`}`:vid-`*xxxx*`_pid-`*yyyy*`(exintf:`*zz*[`;exintf:`*ww*])<br>ou<br>{`m`\|`o`}`:vid-`*xxxx*`_pid-`*yyyy*`(exintf:`*zz*[`;exintf:`*ww*])<br>Vous pouvez utiliser le mot-clé `exintf` pour exclure des composants de la redirection en spécifiant leur numéro d'interface. Vous devez spécifier les numéros d'ID au format hexadécimal et les numéros d'interface au format décimal en incluant les zéros à gauche. Vous pouvez utiliser le caractère générique (`*`) à la place de chiffres dans un ID.<br>Par exemple : **`o:vid-0781_pid-554c(exintf:01;exintf:02)`**<br>**Remarque** View n'inclut pas automatiquement les composants que vous n'avez pas explicitement exclus. Vous devez spécifier une règle de filtre telle que `Include Vid/Pid Device` pour inclure ces composants.<br>La valeur par défaut n'est pas définie. |

## Paramètres USB appliqués par Horizon Agent

Le tableau suivant décrit chaque paramètre de stratégie appliqué par un agent pour USB dans le fichier de modèle d'administration pour la configuration d'Horizon Agent. Horizon Agent utilise les paramètres pour décider si un périphérique USB peut être transmis à la machine hôte. Horizon Agent transmet également les paramètres à Horizon Client pour qu'il les interprète et les applique, selon que vous spécifiez le modificateur de fusion (`m`) ou de remplacement (`o`). Horizon Client utilise les paramètres pour décider si un périphérique USB est disponible pour la redirection. Comme Horizon Agent applique toujours un paramètre de stratégie appliqué par un agent que vous spécifiez, l'effet peut être la neutralisation de la stratégie que vous avez définie pour Horizon Client. Pour voir une description de la façon dont View applique les règles pour le filtrage de périphériques USB, reportez-vous à la section « Configuration de paramètres de règle de filtre pour des périphériques USB », page 261.

**Tableau 15-12.** Modèle de configuration d' Horizon Agent : paramètres appliqués par l'agent

| Paramètre | Propriétés |
|---|---|
| `Exclude All Devices`<br>Propriété : `ExcludeAllDevices` | Exclut tous les périphériques USB de la transmission. Si ce paramètre est défini sur **`true`**, vous pouvez utiliser d'autres paramètres de règle pour autoriser la transmission de périphériques spécifiques ou de familles de périphériques. Si ce paramètre est défini sur **`false`**, vous pouvez utiliser d'autres paramètres de règle pour empêcher la transmission de périphériques spécifiques ou de familles de périphériques.<br>Si ce paramètre est défini sur **`true`** et transmis à Horizon Client, il remplace toujours celui sur Horizon Client. Vous ne pouvez pas utiliser le modificateur de fusion (`m`) ou de remplacement (`o`) avec ce paramètre.<br>La valeur par défaut est indéfinie, ce qui correspond à **`false`**. |
| `Exclude Device Family`<br>Propriété : `ExcludeFamily` | Exclut des familles de périphériques de la transmission. Le format du paramètre est {`m`\|`o`}`:`*family_name_1*[`;`*family_name_2*]...<br>Par exemple : **`o:bluetooth;smart-card`**<br>Si vous avez activé le fractionnement automatique de périphérique, View examine la famille de périphériques de chaque interface d'un périphérique USB composite pour décider quelles interfaces doivent être exclues. Si vous avez désactivé le fractionnement automatique de périphérique, View examine la famille de périphérique de l'ensemble du périphérique USB composite.<br>La valeur par défaut n'est pas définie. |
| `Exclude Vid/Pid Device`<br>Propriété : `ExcludeVidPid` | Exclut des périphériques avec des ID de fournisseur et de produit spécifiés de la transmission. Le format du paramètre est {`m`\|`o`}`:vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]...<br>Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (`*`) à la place de chiffres dans un ID.<br>Par exemple : **`m:vid-0781_pid-****;vid-0561_pid-554c`**<br>La valeur par défaut n'est pas définie. |
| `Include Device Family`<br>Propriété : `IncludeFamily` | Inclut des familles de périphériques pouvant être transmises. Le format du paramètre est {`m`\|`o`}`:`*family_name_1*[`;`*family_name_2*]...<br>Par exemple : **`m:storage`**<br>La valeur par défaut n'est pas définie. |
| `Include Vid/Pid Device`<br>Propriété : `IncludeVidPid` | Inclut des périphériques avec des ID de fournisseur et de produit spécifiés pouvant être transmis. Le format du paramètre est {`m`\|`o`}`:vid-`*xxx1*`_pid-`*yyy2*[`;vid-`*xxx2*`_pid-`*yyy2*]...<br>Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (`*`) à la place de chiffres dans un ID.<br>Par exemple : **`o:vid-0561_pid-554c`**<br>La valeur par défaut n'est pas définie. |

## Paramètres USB interprétés par un client

Le tableau suivant décrit chaque paramètre de stratégie interprété par un client dans le fichier de modèle d'administration pour la configuration d'Horizon Agent. Horizon Agent n'applique pas ces paramètres. Horizon Agent transmet les paramètres à Horizon Client pour qu'il les interprète et les applique. Horizon Client utilise les paramètres pour décider si un périphérique USB est disponible pour la redirection.

**Tableau 15-13.** Modèle de configuration d' Horizon Agent : paramètres interprétés par un client

| Paramètre | Propriétés |
|---|---|
| `Allow Audio Input Devices`<br>Propriété : `AllowAudioIn` | Permet la transmission de périphériques d'entrée audio.<br>La valeur par défaut est indéfinie, ce qui correspond à **`true`**. |
| `Allow Audio Output Devices`<br>Propriété : `AllowAudioOut` | Permet la transmission de périphériques de sortie audio.<br>La valeur par défaut est indéfinie, ce qui correspond à **`false`**. |

**Tableau 15-13.** Modèle de configuration d' Horizon Agent : paramètres interprétés par un client (suite)

| Paramètre | Propriétés |
|---|---|
| `Allow HIDBootable`<br>Propriété : `AllowHIDBootable` | Permet la transmission de périphériques d'entrée autres que des claviers et des souris qui sont disponibles au démarrage (ou périphériques démarrables par HID).<br>La valeur par défaut est indéfinie, ce qui correspond à **`true`**. |
| `Allow Other Input Devices` | Permet la transmission de périphériques d'entrée autres que des périphériques démarrables par HID ou des claviers avec périphériques de pointage intégrés.<br>La valeur par défaut n'est pas définie. |
| `Allow Keyboard and Mouse Devices`<br>Propriété : `AllowKeyboardMouse` | Permet la transmission de claviers avec périphériques de pointage intégrés (souris, Trackball ou pavé tactile).<br>La valeur par défaut est indéfinie, ce qui correspond à **`false`**. |
| `Allow Smart Cards`<br>Propriété : `AllowSmartcard` | Permet la transmission de périphériques à carte à puce.<br>La valeur par défaut est indéfinie, ce qui correspond à **`false`**. |
| `Allow Video Devices`<br>Propriété : `AllowVideo` | Permet la transmission de périphériques vidéo.<br>La valeur par défaut est indéfinie, ce qui correspond à **`true`**. |

# Résolution de problèmes de redirection USB

Plusieurs problèmes peuvent se produire avec la redirection USB dans Horizon Client.

### Problème

La redirection USB dans Horizon Client ne parvient pas à rendre disponibles des périphériques locaux sur le poste de travail distant ou certains périphériques ne semblent pas être disponibles pour la redirection dans Horizon Client.

### Cause

Voici des causes possibles d'échec du fonctionnement correct ou prévu de la redirection USB.

- Le périphérique est un périphérique USB composite et l'un des périphériques qu'il inclut est bloqué par défaut. Par exemple, un périphérique de dictée qui inclut une souris est bloqué par défaut parce que les souris sont bloquées par défaut. Pour contourner ce problème, reportez-vous à « Configuration de paramètres de règle de fractionnement de périphérique pour des périphériques USB composites », page 258.
- La redirection USB n'est pas prise en charge sur les hôtes Windows Server 2008 RDS qui déploient des applications et des postes de travail distants. La redirection USB est prise en charge sur les hôtes RDS Windows Server 2012 avec View Agent 6.1 et versions ultérieures, mais uniquement pour les périphériques de stockage USB. La redirection USB est prise en charge sur les systèmes Windows Server 2008 R2 et Windows Server 2012 R2 utilisés comme postes de travail mono-utilisateur.
- Seuls les lecteurs flash et les disques durs USB sont pris en charge sur les postes de travail et applications RDS. Vous ne pouvez pas rediriger d'autres types de périphériques USB (par exemple, d'autres types de périphériques de stockage USB tels que les lecteurs de stockage de sécurité et les CD-ROM USB) vers un poste de travail ou une application RDS.
- Les webcams ne sont pas prises en charge pour la redirection.
- La redirection de périphériques audio USB dépend de l'état du réseau et n'est pas fiable. Certains périphériques requièrent un débit de données élevé même lorsqu'ils sont inactifs.
- La redirection USB n'est pas prise en charge pour les périphériques d'amorçage. Si vous exécutez Horizon Client sur un système Windows qui démarre à partir d'un périphérique USB, et que vous redirigez ce périphérique vers le poste de travail distant, le système d'exploitation local risque de ne plus répondre ou de devenir inutilisable. Reportez-vous à la section http://kb.vmware.com/kb/1021409.

- Par défaut, Horizon Client pour Windows ne vous permet pas de sélectionner des périphériques clavier, souris, carte à puce et sortie audio pour la redirection. Reportez-vous à la section http://kb.vmware.com/kb/1011600.
- RDP ne prend pas en charge la redirection pour les périphériques HID USB pour la session de console, ou pour les lecteurs de cartes à puce. Reportez-vous à la section http://kb.vmware.com/kb/1011600.
- Windows Mobile Device Center peut empêcher la redirection de périphériques USB pour des sessions RDP. Reportez-vous à la section http://kb.vmware.com/kb/1019205.
- Pour certains périphériques HID USB, vous devez configurer la machine virtuelle afin d'actualiser la position du pointeur de la souris. Reportez-vous à la section http://kb.vmware.com/kb/1022076.
- Pour certains périphériques audio, vous devrez éventuellement modifier les paramètres de règle ou de Registre. Reportez-vous à la section http://kb.vmware.com/kb/1023868.
- La latence réseau peut ralentir l'interaction entre périphériques ou rendre les applications figées car elles sont conçues pour interagir avec des périphériques locaux. Les disques durs USB très volumineux peuvent prendre plusieurs minutes pour apparaître dans Windows Explorer.
- Le chargement des cartes flash USB formatées avec le système de fichiers FAT32 est lent. Reportez-vous à la section http://kb.vmware.com/kb/1022836.
- Un processus ou un service sur le système local a ouvert le périphérique avant votre connexion à l'application ou au poste de travail distant.
- Un périphérique USB redirigé arrête de fonctionner si vous reconnectez une session de poste de travail ou d'application, même si le poste de travail ou l'application indique que le périphérique est disponible.
- La redirection USB est désactivée dans View Administrator.
- Des pilotes de redirection USB sont manquants ou désactivés sur le client.

### Solution

- S'il est disponible, utilisez PCoIP au lieu de RDP comme protocole.
- Si un périphérique redirigé reste indisponible ou arrête de fonctionner après une déconnexion temporaire, éjectez le périphérique, rebranchez-le et tenter de nouveau l'opération de redirection.
- Dans View Administrator, accédez à **Règles > Règles générales**, et vérifiez que l'accès USB est défini sur **Autoriser** sous Règles de View.
- Dans le journal de l'invité, recherchez des entrées de la classe `ws_vhub` et, dans le journal du client, recherchez des entrées de la classe `vmware-view-usbd`.

  Les entrées avec ces classes sont inscrites dans les journaux si un utilisateur n'est pas un administrateur, ou si les pilotes de redirection USB ne sont pas installés ou ne fonctionnent pas. Pour connaître l'emplacement de ces fichiers journaux, reportez-vous à « Utilisation de fichiers journaux pour le dépannage et pour déterminer les ID de périphérique USB », page 256.
- Ouvrez le Gestionnaire de périphériques sur l'invité, développez les contrôleurs USB (Universal Serial Bus) et réinstallez les pilotes VMware View Virtual USB Host Controller et VMware View Virtual USB Hub s'ils sont manquants ou réactivez-les s'ils sont désactivés.

# Réduction et gestion des exigences de stockage 16

Le déploiement de postes de travail sur des machines virtuelles gérées par vCenter Server offre toutes les performances de stockage qui étaient auparavant réservées aux serveurs virtualisés. L'utilisation de clones instantanés ou de clones liés View Composer en tant que machines de poste de travail améliore les économies de stockage, car toutes les machines virtuelles dans un pool partagent un disque virtuel avec une image de base.

Ce chapitre aborde les rubriques suivantes :



## Gestion du stockage avec vSphere

vSphere vous permet de virtualiser des volumes de disque et des systèmes de fichiers pour que vous puissiez gérer et configurer le stockage sans vous soucier de l'emplacement de stockage physique des données.

Les baies Fibre Channel SAN, iSCSI SAN et NAS sont des technologies de stockage largement utilisées et prises en charge par vSphere pour répondre à différents besoins de stockage de centre de données. Les baies de stockage sont connectées à et partagées entre des groupes de serveurs via des réseaux de stockage. Cette configuration permet l'agrégation des ressources de stockage et fournit plus de flexibilité dans leur approvisionnement aux machines virtuelles.

## Fonctionnalités compatibles avec vSphere 5.0 et 5.1 ou version ultérieure

Avec vSphere 5.0 ou version ultérieure, vous pouvez utiliser les fonctionnalités suivantes :

- Avec la fonction d'accélérateur de stockage View, vous pouvez configurer des hôtes ESXi pour mettre en cache des données de disque de machine virtuelle.

  L'utilisation de ce cache de lecture basé sur le contenu (CBRC) peut réduire le nombre d'opérations d'E/S par seconde et améliorer les performances au cours des tempêtes de démarrage, lorsque plusieurs machines démarrent et exécutent des analyses antivirus en même temps. Au lieu de lire tout le système d'exploitation depuis le système de stockage encore et encore, un hôte peut lire des blocs de données communes depuis le cache.

- Si des postes de travail distants utilisent le format de disque à optimisation d'espace disponible avec vSphere 5.1 et version ultérieure, les données périmées ou supprimées dans un système d'exploitation invité sont automatiquement récupérées avec un processus d'effacement et de réduction.

- Vous pouvez déployer un pool de postes de travail sur un cluster contenant jusqu'à 32 hôtes ESXi, avec certaines restrictions.

  Les disques de réplica doivent être stockés sur des magasins de données VMFS5 ou supérieur ou sur des magasins de données NFS. Si vous stockez les réplicas sur une version VMFS antérieure à VMFS5, un cluster peut contenir 8 hôtes au maximum. Les disques du système d'exploitation et les disques persistants peuvent être stockés sur des magasins de données NFS ou VMFS.

## Fonctionnalités compatibles avec vSphere 5.5 Update 1 ou version ultérieure

Avec vSphere 5.5 Update 1 ou version ultérieure, vous pouvez utiliser Virtual SAN qui virtualise les disques SSD et les disques durs locaux physiques disponibles sur les hôtes ESXi dans une banque de données unique partagée par tous les hôtes d'un cluster. Virtual SAN fournit un stockage haute performance avec une gestion basée sur la stratégie, de sorte que vous pouvez spécifier une seule banque de données lors de la création d'un pool de postes de travail, et que les différents composants, comme les fichiers, les réplicas, les données utilisateur et les fichiers du système d'exploitation de la machine virtuelle sont placés sur des disques SSD ou sur des disques durs appropriés.

Virtual SAN vous permet également de gérer le stockage et les performances du stockage de la machine virtuelle et en utilisant des profils de stratégie de stockage. Si la stratégie devient non conforme en raison d'un hôte, d'un disque, d'une panne réseau ou de changements de charge de travail, Virtual SAN reconfigure les données des machines virtuelles affectées et optimise l'utilisation des ressources dans le cluster. Vous pouvez déployer un pool de postes de travail sur un cluster contenant jusqu'à 20 hôtes ESXi.

**Important** La fonctionnalité Virtual SAN disponible avec vSphere 6.0 et versions ultérieures contient de nombreuses améliorations de performance par rapport à la fonctionnalité disponible avec vSphere 5.5 Update 1. Avec vSphere 6.0, cette fonctionnalité dispose également d'une compatibilité matérielle (HCL) élargie. Pour plus d'informations sur Virtual SAN dans vSphere 6 ou version ultérieure, reportez-vous au document *Administration de VMware Virtual SAN*.

**Remarque** Virtual SAN est compatible avec la fonctionnalité d'accélérateur de stockage View mais pas avec la fonctionnalité de format de disque à optimisation d'espace qui récupère de l'espace disque en effaçant et en réduisant les disques.

## Fonctionnalités compatibles avec vSphere 6.0 ou version ultérieure

Avec vSphere 6.0 ou version ultérieure, vous pouvez utiliser Virtual Volumes (VVols). Cette fonctionnalité mappe les disques virtuels et leurs dérivés, clones, snapshots et réplicas, directement à des objets nommés volumes virtuels sur un système de stockage. Ce mappage permet à vSphere de décharger des opérations de stockage intensives telles que la prise de snapshots, le clonage et la réplication sur le système de stockage.

La fonctionnalité Virtual Volumes vous permet également de gérer le stockage et les performances du stockage de la machine virtuelle dans vSphere. Ces profils de stratégie de stockage déterminent les services de stockage utilisés au niveau de chaque machine virtuelle. Ce type de provisionnement granulaire augmente le degré d'utilisation de la capacité. Vous pouvez déployer un pool de postes de travail sur un cluster contenant jusqu'à 32 hôtes ESXi.

**Remarque** Virtual Volumes est compatible avec la fonctionnalité d'accélérateur de stockage View, mais pas avec la fonctionnalité de format de disque à optimisation d'espace qui récupère de l'espace disque en effaçant et en réduisant les disques.

**Remarque** Les clones instantanés ne prennent pas en charge Virtual Volumes.

## Utilisation de Virtual SAN pour un stockage haute performance et une gestion basée sur les stratégies

VMware Virtual SAN est une couche de stockage définie par logiciel, disponible avec vSphere 5.5 Update 1 ou version ultérieure, qui virtualise les disques de stockage physiques disponibles sur un cluster d'hôtes vSphere. Vous spécifiez une seule banque de données lors de la création d'un pool de postes de travail automatisé ou d'une batterie de serveurs automatisée, et les différents composants, comme les fichiers, réplicas, données utilisateur et fichiers de système d'exploitation de la machine virtuelle sont placés sur des disques SSD ou des disques durs appropriés.

Virtual SAN met en œuvre une approche à la gestion du stockage basée sur les stratégies. Lorsque vous utilisez Virtual SAN, View définit les exigences du stockage de la machine virtuelle, comme la capacité, les performances et la disponibilité, sous la forme de profils de stratégie de stockage par défaut que vous pouvez modifier. Le stockage est approvisionné et configuré automatiquement selon les stratégies affectées. Vous pouvez utiliser Virtual SAN pour des pools de postes de travail de clone lié, des pools de postes de travail de clone instantané, des pools de postes de travail de clone complet ou une batterie de serveurs automatisée.

Chaque machine virtuelle maintient sa stratégie, quel que soit son emplacement physique dans le cluster. Si la stratégie devient non conforme en raison d'une panne d'hôte, de disque, de réseau ou à la suite de modifications dans la charge de travail, Virtual SAN reconfigure les données des machines virtuelles affectées et des équilibrages de charge pour satisfaire les stratégies de chaque machine virtuelle.

Tout en prenant en charge les fonctionnalités VMware qui nécessitent un stockage partagé, tel que HA, vMotion et DRS, Virtual SAN élimine le besoin d'une infrastructure de stockage partagé externe et simplifie les activités de configuration de stockage et d'approvisionnement de machines virtuelles.

**Important** La fonctionnalité Virtual SAN disponible avec vSphere 6.0 et versions ultérieures contient de nombreuses améliorations de performance par rapport à la fonctionnalité disponible avec vSphere 5.5 Update 1. Avec vSphere 6.0, cette fonctionnalité dispose également d'une compatibilité matérielle (HCL) élargie. De plus, VMware Virtual SAN 6.0 prend en charge une architecture entièrement flash qui utilise des périphériques basés sur le flash pour la mise en cache et le stockage persistant.

### Workflow de Virtual SAN dans View

1 Utilisez vCenter Server 5.5 Update 1 ou une version ultérieure pour activer Virtual SAN. Pour plus d'informations sur Virtual SAN dans vSphere 5.5 Update 1, reportez-vous au document *Stockage de vSphere*. Pour plus d'informations sur Virtual SAN dans vSphere 6 ou version ultérieure, reportez-vous au document *Administration de VMware Virtual SAN*.

2 Lors de la création d'un pool de postes de travail automatisé ou d'une batterie de serveurs automatisée dans View Administrator, sous la **Gestion des stratégies de stockage**, sélectionnez **Utiliser VMware Virtual SAN** et sélectionnez la banque de données Virtual SAN à utiliser.

Après la sélection de **Utiliser VMware Virtual SAN**, seules les banques de données Virtual SAN s'affichent.

Les profils de stratégies de stockage par défaut sont créés conformément aux options que vous choisissez. Par exemple, si vous créez un clone lié, un pool de postes de travail flottants, un profil de disque de réplica et un profil de disque de système d'exploitation sont automatiquement créés. Si vous créez un clone lié, un pool de postes de travail persistants, un profil de disque de réplica et un profil de disque persistant sont créés. Pour une batterie de serveurs automatisée, un profil de disque de réplica est créé. Pour les deux types de pools de postes de travail et de batteries de serveurs automatisées, un profil est créé pour les fichiers de machine virtuelle.

3 Pour déplacer les pools de postes de travail View Composer existants d'un autre type de banque de données vers une banque de données Virtual SAN, dans View Administrator, modifiez le pool pour annuler la sélection de l'ancienne banque de données et sélectionnez plutôt la banque de données Virtual SAN, et utilisez la commande Rééquilibrer. Cette opération n'est pas possible pour les batteries de serveurs automatisées car vous ne pouvez pas rééquilibrer une batterie de serveurs automatisée.

4 (Facultatif) Utilisez vCenter Server pour modifier les paramètres des profils de stratégie de stockage, qui incluent par exemple le nombre de pannes à tolérer et la quantité de cache de lecture SSD à réserver.

   Les noms des stratégies sont OS_DISK (pour les fichiers du système d'exploitation), PERSISTENT_DISK (pour les fichiers de données utilisateur), REPLICA_DISK (pour les réplicas) et VM_HOME (pour les fichiers de machine virtuelle tels que les fichiers `.vmx` et `.vmsn`). Les modifications apportées à la stratégie sont propagées aux machines virtuelles récemment créées et à toutes les machines virtuelles existantes dans le pool de postes de travail ou la batterie de serveurs automatisée.

5 Utilisez vCenter Server pour surveiller le cluster Virtual SAN et les disques qui participent à la banque de données. Pour plus d'informations, reportez-vous au document *Stockage de vSphere* et à la documentation *Surveillance et performance de vSphere*. Pour vSphere 6 ou version ultérieure, reportez-vous au document *Administration de VMware Virtual SAN*.

6 (Facultatif) Pour les pools de postes de travail de clone lié View Composer, utilisez les commandes Actualiser et Recomposer comme vous le feriez normalement. Pour les batteries de serveurs automatisées, seule la commande Recomposer est prise en charge, quel que soit le type de banque de données.

## Exigences et limitations

La fonctionnalité Virtual SAN présente les limitations suivantes lors d'une utilisation dans un déploiement View :

- Cette version ne prend pas en charge l'utilisation de la fonctionnalité de format de disque à optimisation d'espace d'View qui récupère de l'espace en effaçant et en réduisant les disques.
- Virtual SAN ne prend pas en charge la fonctionnalité VCAI (View Composer Array Integration), car Virtual SAN n'utilise pas les périphériques NAS.
- Les banques de données Virtual SAN ne sont pas compatibles avec les banques de données Virtual Volumes pour cette version.

---

**Remarque** Virtual SAN est compatible avec la fonctionnalité View Storage Accelerator. Virtual SAN fournit une couche de mise en cache sur les disques SSD, et la fonctionnalité View Storage Accelerator fournit un cache basé sur le contenu qui réduit les opérations d'E/S et améliore les performances lors des tempêtes de démarrage.

---

La fonctionnalité Virtual SAN impose les exigences suivantes :

- vSphere 5.5 Update 1 ou une version ultérieure.

- Matériel approprié. Par exemple, VMware recommande une carte réseau 10 Gbits/s et au moins un disque SSD et un disque dur pour chaque nœud constituant la capacité. Pour obtenir des informations spécifiques, reportez-vous au Guide de compatibilité VMware.
- Un cluster d'au moins trois hôtes ESXi. Vous avez besoin d'un nombre suffisant d'hôtes ESXi pour recevoir votre installation. Pour plus d'informations, reportez-vous au document *Configurations maximales pour vSphere*, disponible à l'adresse https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html.
- Capacité de disque SSD correspondant au moins à 10 pour cent de la capacité du disque dur.
- Suffisamment de disques durs pour recevoir votre installation. Ne dépassez pas le seuil de 75 % de l'utilisation sur un disque magnétique.

Pour plus d'informations sur les conditions requises de Virtual SAN, reportez-vous à « Utilisation de Virtual SAN » dans le document *Stockage de vSphere 5.5 Update 1*. Pour vSphere 6 ou version ultérieure, reportez-vous au document *Administration de VMware Virtual SAN*. Pour obtenir des instructions sur le dimensionnement et la conception des composants clés des infrastructures de postes de travail View pour VMware Virtual SAN, reportez-vous au livre blanc proposé à l'adresse http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf.

## Profils de stratégie de stockage par défaut pour banques de données Virtual SAN

Lorsque vous utilisez Virtual SAN, View définit les exigences du stockage de la machine virtuelle, comme la capacité, les performances et la disponibilité, sous la forme de profils de stratégie de stockage par défaut que vous pouvez modifier. Le stockage est approvisionné et configuré automatiquement selon les stratégies affectées.

Les stratégies par défaut qui sont créées lors de la création d'un pool de postes de travail dépendent du type de pool que vous créez. Les noms des stratégies sont OS_DISK (pour les fichiers du système d'exploitation), PERSISTENT_DISK (pour les fichiers de données utilisateur), REPLICA_DISK (pour les réplicas) et VM_HOME (pour les fichiers de machine virtuelle tels que les fichiers `.vmx` et `.vmsn`). Par exemple, une stratégie REPLICA_DISK est créée uniquement pour des pools de clone lié. Les modifications apportées à la stratégie sont propagées aux machines virtuelles récemment créées et à toutes les machines virtuelles existantes dans le pool de postes de travail.

Virtual SAN fournit une infrastructure de stratégie de stockage vous permettant de contrôler le comportement des différents objets de machine virtuelle qui résident dans la banque de données Virtual SAN. Un exemple d'objet dans Virtual SAN est un fichier de disque virtuel (VMDK), et une stratégie contrôle quatre caractéristiques de chaque objet :

- **Bandes** : nombre de bandes de données. Le nombre de bandes de disque affecte le nombre de disques magnétiques (HDD) dont vous disposez.
- **Résilience** : nombre de pannes à tolérer. Le nombre de pannes d'hôte à tolérer dépend, évidemment, du nombre d'hôtes dont vous disposez.
- **Provisionnement de stockage** : statique ou dynamique.
- **Réservation de cache** : réservation de cache de lecture.

Les paramètres de réservation de bandes et de cache sont utilisés pour contrôler les performances. Le paramètre de résilience contrôle la disponibilité. Le paramètre de provisionnement de stockage contrôle la capacité. Ces paramètres, regroupés, affectent le nombre d'hôtes vSphere et de disques magnétiques requis.

Par exemple, si vous définissez le nombre de bandes de disque par objet sur 2, Virtual SAN agrège l'objet par bandes sur au moins 2 HDD. En liaison avec ce paramètre, si vous définissez le nombre de pannes d'hôte à tolérer sur 1, Virtual SAN crée une copie supplémentaire pour la résilience et a donc besoin de 4 HDD. En outre, la définition du nombre de pannes d'hôtes à tolérer sur 1 nécessite au moins 3 hôtes ESXi : 2 pour la résilience et un troisième pour les départager en cas de partitionnement.

**Remarque** Si vous tentez par inadvertance d'utiliser des paramètres qui se contredisent, lorsque vous appliquerez ces paramètres, l'opération échouera et un message d'erreur vous informera, par exemple, que vous n'avez pas suffisamment d'hôtes.

L'action de l'utilisateur associée à ces stratégies par défaut n'est soumise à aucune exigence particulière. Des stratégies sont créées pour des pools de postes de travail de clone lié, des pools de postes de travail de clone complet et des batteries de serveurs automatisées.

Vous pouvez aussi bien utiliser l'interface de ligne de commande de vSphere (`esxcli`) que vSphere Web Client pour modifier les profils de stratégie de stockage par défaut. Chaque machine virtuelle maintient sa stratégie, quel que soit son emplacement physique dans le cluster. Si la stratégie devient non conforme en raison d'une panne d'hôte, de disque, de réseau ou à la suite de modifications dans la charge de travail, Virtual SAN reconfigure les données des machines virtuelles affectées et des équilibrages de charge pour satisfaire les stratégies de chaque machine virtuelle.

## Utilisation de Virtual Volumes pour un stockage centré sur une machine virtuelle et une gestion basée sur la stratégie

Avec Virtual Volumes (VVols), disponible dans vSphere 6.0 ou version ultérieure, une machine virtuelle individuelle, pas la banque de données, devient une unité de gestion de stockage. Le matériel de stockage obtient le contrôle sur le contenu, la disposition et la gestion d'un disque virtuel.

Avec Virtual Volumes, des conteneurs de stockage abstraits remplacent les volumes de stockage traditionnels basés sur des LUN ou des partages NFS. Virtual Volumes mappe les disques virtuels et leurs dérivés, clones, snapshots et réplicas, directement à des objets nommés volumes virtuels sur un système de stockage. Ce mappage permet à vSphere de décharger des opérations de stockage intensives telles que la prise de snapshots, le clonage et la réplication sur le système de stockage. Une opération de stockage qui mettait précédemment une heure s'exécute dorénavant en seulement quelques minutes à l'aide de Virtual Volumes.

**Important** Bien que l'un des principaux avantages de Virtual Volumes soit la possibilité d'utiliser la gestion basée sur la stratégie du logiciel (SPBM, Software Policy-Based Management), pour cette version de View, aucune stratégie de stockage granulaire par défaut n'est créée par View comme celles créées lors de l'utilisation de la fonctionnalité Virtual SAN. Vous pouvez plutôt définir une stratégie de stockage par défaut dans vCenter Server qui s'appliquera à toutes les banques de données Virtual Volume.

Virtual Volumes offre les avantages suivants :

- Virtual Volumes gère la décharge d'un certain nombre d'opérations sur le matériel de stockage. Ces opérations incluent la prise de snapshots, le clonage et Storage DRS.
- Avec Virtual Volumes, vous pouvez utiliser des services de stockage avancés qui incluent notamment la réplication, le chiffrement, la déduplication et la compression sur des disques virtuels individuels.
- Virtual Volumes prend en charge diverses fonctionnalités vSphere telles que vMotion, Storage vMotion, snapshots, clones liés, Flash Read Cache et DRS.
- Vous pouvez utiliser Virtual Volumes avec des baies de stockage qui prennent en charge la technologie VAAI (vSphere APIs for Array Integration).

### Exigences et limitations

La fonctionnalité Virtual Volumes présente les limitations suivantes lors d'une utilisation dans un déploiement View :

- Cette version ne prend pas en charge l'utilisation de la fonctionnalité de format de disque à optimisation d'espace d'View qui récupère de l'espace en effaçant et en réduisant les disques.
- Virtual Volumes ne prend pas en charge l'utilisation de la technologie VAAI (View Composer Array Integration).
- Les banques de données Virtual Volumes ne sont pas compatibles avec les banques de données Virtual SAN pour cette version.
- Les banques de données Virtual Volumes ne sont pas prises en charge pour les pools de postes de travail de clone instantané.

---

**Remarque** Virtual Volumes est compatible avec la fonctionnalité View Storage Accelerator. Virtual SAN fournit une couche de mise en cache sur les disques SSD, et la fonctionnalité View Storage Accelerator fournit un cache basé sur le contenu qui réduit les opérations d'E/S et améliore les performances lors des tempêtes de démarrage.

---

La fonctionnalité Virtual Volumes impose la configuration requise suivante :

- vSphere 6.0 ou version ultérieure.
- Matériel approprié. Certains fournisseurs de stockage sont responsables de l'apport de fournisseurs de stockage pouvant s'intégrer avec vSphere et apporter la prise en charge de Virtual Volumes. Chaque fournisseur de stockage doit être certifié par VMware et correctement déployé.
- Tous les disques virtuels que vous provisionnez sur une banque de données virtuelle doivent être un multiple entier de 1 Mo.

Virtual Volumes est une fonctionnalité vSphere 6.0. Pour plus d'informations sur les conditions requises, la fonctionnalité, l'arrière-plan et la configuration requise pour l'installation, reportez-vous aux rubriques sur Virtual Volumes dans le document *vSphere Storage*.

## Réduction des exigences de stockage avec des clones instantanés

La fonctionnalité de clones instantanés exploite la technologie vSphere vmFork (disponible avec vSphere 6.0U1 et versions ultérieures) afin de suspendre une image de base en cours d'exécution, ou une machine virtuelle parente, et de la cloner à chaud pour créer un pool de 2 000 clones instantanés maximum.

Les clones instantanés partagent les disques virtuels avec la machine virtuelle parente au moment de la création, mais également la mémoire du parent. Chaque clone instantané agit comme un poste de travail indépendant, avec un nom d'hôte et une adresse IP uniques. Pourtant le clone lié requiert beaucoup moins de stockage. Les clones instantanés réduisent la capacité de stockage requise de 50 à 90 %. Les exigences de mémoire globale sont également réduites au moment de la création des clones.

### Clones réplica et instantanés sur la même banque de données

Lorsque vous créez un pool de postes de travail de clone instantané, un clone complet est d'abord créé depuis la machine virtuelle maître. Le clone complet, ou réplica, et ses clones liés peuvent être placés sur le même magasin de données, ou LUN (Logical Unit Number).

### Clones réplica et instantanés sur des banques de données différentes

Vous pouvez également placer des réplicas de clones instantanés et des clones instantanés sur des banques de données séparées avec différentes caractéristiques de performance. Par exemple, vous pouvez stocker les machines virtuelles réplicas sur un disque électronique. Les disques électroniques ont une capacité de stockage faible et des performances de lecture élevées. En général, ils prennent en charge des dizaines de milliers d'E/S par seconde (IOPS).

Vous pouvez stocker des clones instantanés sur des banques de données sur des supports de rotation traditionnels. Ces disques sont moins performants, mais ils sont moins chers et fournissent une plus grande capacité de stockage. Ils sont donc adaptés pour le stockage des nombreux clones instantanés d'un pool volumineux. Les configurations de stockage étagées peuvent être utilisées pour gérer de façon rentable les scénarios d'E/S intensifs tels que l'exécution simultanée d'analyses antivirus programmées.

Si vous utilisez des banques de données Virtual SAN, vous ne pouvez pas sélectionner manuellement différentes banques de données pour les réplicas ou clones instantanés. Comme Virtual SAN place automatiquement les objets sur le type de disque approprié et met en cache toutes les opérations d'E/S, il n'est pas nécessaire d'utiliser la hiérarchisation des réplicas pour les banques de données Virtual SAN. Les pools de clones instantanés sont pris en charge sur les banques de données Virtual SAN. Les pools de clones instantanés ne sont pas pris en charge sur les disques de stockage locaux ordinaires.

### Différences entre les clones instantanés et les clones liés View Composer

Les clones instantanés peuvent être créés beaucoup plus rapidement que les clones liés. Les fonctionnalités suivantes de clones liés ne sont plus nécessaires lorsque vous provisionnez un pool de clones instantanés :

- Les pools de clones instantanés ne prennent pas en charge la configuration d'un disque virtuel supprimable séparé pour stocker les fichiers d'échange et temporaires du système d'exploitation invité. Chaque fois qu'un utilisateur se déconnecte d'un poste de travail de clone instantané, View supprime automatiquement le clone, puis provisionne et met sous tension un autre clone instantané en fonction de la dernière image de système d'exploitation disponible pour le pool. Les fichiers d'échange et temporaires des systèmes d'exploitation invités sont automatiquement supprimés lors de l'opération de déconnexion.
- Les pools de clones instantanés ne prennent pas en charge la création d'un disque virtuel persistant séparé pour chaque poste de travail virtuel. Vous pouvez plutôt stocker le profil Windows et les données d'application de l'utilisateur final sur des disques accessibles en écriture utilisateur App Volumes. Le disque accessible en écriture utilisateur de l'utilisateur final est lié à un poste de travail de clone instantané lorsque l'utilisateur final se connecte. De plus, des disques accessibles en écriture utilisateur peuvent être utilisés pour conserver des applications installées par l'utilisateur.
- Comme les postes de travail de clone instantané ont une courte durée de vie, le format de disque à optimisation d'espace (SE Sparse), avec son processus d'effacement et de réduction, n'est pas nécessaire.

## Réduction des exigences de stockage avec View Composer

Comme View Composer crée des images de poste de travail qui partagent des disques virtuels avec une image de base, vous pouvez réduire la capacité de stockage requise de 50 à 90 %.

View Composer utilise une image de base, ou une machine virtuelle parente, et crée un pool de 2,000 machines virtuelles de clone lié maximum. Chaque clone lié agit comme un poste de travail indépendant, avec un nom d'hôte et une adresse IP uniques. Pourtant le clone lié requiert beaucoup moins de stockage.

## Clones réplica et liés sur le même magasin de données

Lorsque vous créez un pool de postes de travail de clone lié ou une batterie de serveurs d'hôtes RDS Microsoft, un clone complet est d'abord créé à partir de la machine virtuelle parente. Le clone complet, ou réplica, et ses clones liés peuvent être placés sur le même magasin de données, ou LUN (Logical Unit Number). Si nécessaire, vous pouvez utiliser la fonctionnalité de rééquilibrage pour déplacer le réplica et les pools de postes de travail de clone lié d'un LUN vers un autre ou des pools de postes de travail de clone lié vers une banque de données Virtual SAN ou d'une banque de données Virtual SAN vers un LUN.

## Clones réplica et liés sur des magasins de données différents

Vous pouvez également placer des réplicas et des clones liés View Composer sur des magasins de données séparés avec différentes caractéristiques de performance. Par exemple, vous pouvez stocker les machines virtuelles réplicas sur un disque électronique. Les disques électroniques ont une capacité de stockage faible et des performances de lecture élevées. En général, ils prennent en charge des dizaines de milliers d'E/S par seconde (IOPS). Vous pouvez stocker des clones liés sur des magasins de données sur des supports de rotation traditionnels. Ces disques sont moins performants, mais ils sont moins chers et fournissent une plus grande capacité de stockage. Ils sont donc adaptés pour le stockage des nombreux clones liés d'un pool volumineux. Les configurations de stockage étagées peuvent être utilisées pour gérer de façon rentable les scénarios d'E/S intensifs tels que le redémarrage simultané de plusieurs machines virtuelles ou l'exécution d'analyses antivirus programmées.

Pour plus d'informations, consultez le guide de meilleures pratiques intitulé *Storage Considerations for VMware View*.

Si vous utilisez des banques de données Virtual SAN ou des banques de données Virtual Volumes, vous ne pouvez pas sélectionner manuellement différentes banques de données pour les réplicas ou clones liés. Comme les fonctionnalités de Virtual SAN et de Virtual Volumes placent automatiquement les objets sur le type de disque approprié et mettent en cache toutes les opérations d'E/S, il n'est pas nécessaire d'utiliser la hiérarchisation des réplicas pour les banques de données Virtual SAN et Virtual Volumes.

## Disques supprimables pour fichiers d'échange et temporaires

Lorsque vous créez un pool de clone lié ou une batterie de serveurs, vous pouvez également configurer de façon facultative un disque virtuel supprimable séparé pour stocker les fichiers d'échange et temporaires du système d'exploitation invité qui sont générés au cours de sessions utilisateur. Quand une machine virtuelle est mise hors tension, le disque pouvant être supprimé est supprimé. L'utilisation de disques supprimables peut économiser de l'espace de stockage en ralentissant la croissance des clones liés et en réduisant l'espace utilisé par les machines virtuelles désactivées.

## Disques persistants pour postes de travail dédiés

Lorsque vous créez des pools de postes de travail d'affectation dédiée, View Composer peut également créer de façon facultative un disque virtuel persistant séparé pour chaque poste de travail virtuel. Le profil Windows et les données d'application de l'utilisateur final sont enregistrés sur le disque persistant. Lorsqu'un clone lié est actualisé, recomposé ou rééquilibré, le contenu du disque virtuel persistant est conservé. VMware vous recommande de conserver les disques persistants View Composer sur un magasin de données séparé. Vous pouvez ensuite sauvegarder l'ensemble de LUN qui conserve les disques persistants.

## Dimensionnement du stockage pour des pools de postes de travail de clone instantané et de clone lié View Composer

View propose des recommandations très utiles qui peuvent vous aider à déterminer la quantité de stockage requise pour un pool de postes de travail de clone instantané ou de clone lié. Un tableau dans l'assistant Ajouter un pool de postes de travail montre une estimation générale des exigences de stockage du pool de postes de travail.

Le tableau de dimensionnement du stockage affiche également l'espace libre sur les magasins de données que vous sélectionnez pour le stockage de disques du système d'exploitation, de disques persistants de View Composer (pour les clones liés View Composer uniquement) et de réplicas. Vous pouvez décider des magasins de données à utiliser en comparant l'espace libre réel et les exigences estimées pour le pool de postes de travail.

Les formules que View utilise ne peuvent fournir qu'une estimation générale de l'utilisation du stockage. La croissance de stockage réelle des clones dépend de nombreux facteurs :

- Quantité de mémoire affectée à la machine virtuelle parente
- Fréquence des opérations d'actualisation (pour les clones liés View Composer uniquement)
- Taille du fichier d'échange du système d'exploitation client
- La redirection éventuelle des fichiers d'échange et temporaires vers un disque séparé (pour les clones liés View Composer uniquement)
- La configuration éventuelle des disques persistants View Composer séparés (pour les clones liés View Composer uniquement)
- Charge de travail sur les machines de poste de travail, déterminée principalement par les types d'applications que les utilisateurs exécutent sur le système d'exploitation invité

---

**Remarque** Dans un déploiement qui inclut des centaines ou des milliers de clones, configurez vos pools de postes de travail pour que des ensembles particuliers de magasins de données soient dédiés à des clusters ESXi particuliers. Ne configurez pas de pools de manière aléatoire sur toutes les banques de données de telle sorte que la plupart ou tous les hôtes ESXi doivent accéder à la plupart ou à tous les LUN.

Lorsqu'un trop grand nombre d'hôtes ESXi tentent d'écrire sur les disques du système d'exploitation sur un LUN particulier, des problèmes de contention peuvent se produire, ce qui dégrade les performances et interfère avec l'évolutivité. Pour plus d'informations sur la planification des magasins de données dans de grands déploiements, consultez le document *Planification de l'architecture de View*.

---

## Recommandations de dimensionnement pour les pools de clone instantané et de clone lié

Lorsque vous créez ou modifiez un pool de postes de travail de clone instantané ou de clone lié, la page Sélectionner des magasins de données de clone lié (ou instantané) affiche un tableau contenant des recommandations de dimensionnement de stockage. Le tableau peut vous aider à décider des magasins de données à sélectionner pour les disques de clone lié. Ces recommandations calculent l'espace nécessaire aux nouveaux clones liés.

### Tableau de dimensionnement pour les disques du système d'exploitation et les disques persistants

Tableau 16-1 montre un exemple de recommandations de dimensionnement du stockage pouvant s'afficher pour un pool de 10 machines virtuelles si la machine virtuelle parente dispose de 1 Go de mémoire et d'un réplica de 10 Go. Dans cet exemple, différents magasins de données sont sélectionnés pour les disques du système d'exploitation et les disques persistants de View Composer.

**Remarque** Les informations sur le disque persistant sont destinées uniquement aux clones liés View Composer. Les clones instantanés ne prennent pas en charge les disques persistants.

**Tableau 16-1.** Exemple de tableau de dimensionnement pour les disques du système d'exploitation et persistants

| Type de données | Espace libre sélectionné (Go) | Min. recommandé (Go) | Utilisation 50 % (Go) | Max. recommandé (Go) |
|---|---|---|---|---|
| Disques du système d'exploitation | 184,23 | 40,00 | 80,00 | 130,00 |
| Disques persistants | 28,56 | 4,00 | 10,00 | 20,00 |

La colonne **Espace libre sélectionné** montre l'espace disponible total sur tous les magasins de données que vous avez sélectionnés pour un type de disque, tel que des disques du système d'exploitation.

La colonne **Min. recommandé** indique la quantité minimale de stockage recommandé pour un pool.

La colonne **Utilisation 50 %** montre le stockage recommandé lorsque des disques atteignent 50 % de la machine virtuelle parente.

La colonne **Max. recommandé** montre le stockage recommandé lorsque des disques approchent de la taille complète de la machine virtuelle parente.

Si vous stockez des disques du système d'exploitation et des disques persistants sur la même banque de données, View calcule les besoins en stockage des deux types de disque. Le **Type de données** indique **Clones liés** ou **Clones instantanés** plutôt qu'un type de disque particulier.

Si vous stockez des réplicas View Composer sur un magasin de données séparé, le tableau montre également des recommandations de stockage pour les réplicas et ajuste les recommandations pour les disques du système d'exploitation.

### Recommandations de dimensionnement pour les clones liés View Composer

Le tableau fournit des recommandations générales. Vos calculs de stockage doivent prendre en compte des facteurs supplémentaires qui peuvent affecter la croissance du stockage réel dans les clones.

Pour les disques du système d'exploitation, vos estimations de dimensionnement dépendent de la fréquence à laquelle vous actualisez et recomposez le pool.

Si vous actualisez votre pool de clone lié entre une fois par jour et une fois par semaine, assurez-vous que le **Espace libre sélectionné** peut s'adapter à l'utilisation du stockage entre les estimations de **Min. recommandé** et **Utilisation 50 %**.

Si vous actualisez ou recomposez rarement le pool, les disques de clone lié continuent de croître. Assurez-vous que l'**Espace libre sélectionné** peut permettre l'utilisation du stockage entre les estimations **Utilisation à 50 %** et **Utilisation maxi. recommandée**.

Pour les disques persistants, vos estimations de dimensionnement dépendent de la quantité de données de profil Windows générées par les utilisateurs sur leurs postes de travail. Les opérations d'actualisation et de recomposition n'affectent pas les disques persistants.

## Recommandations de dimensionnement lorsque vous modifiez un pool de postes de travail existant

View estime l'espace de stockage nécessaire aux nouveaux clones. Lorsque vous créez un pool de postes de travail, les recommandations de dimensionnement portent sur l'intégralité du pool. Lorsque vous modifiez un pool de postes de travail existant, les recommandations portent uniquement sur les nouveaux clones que vous ajoutez au pool.

Par exemple, si vous ajoutez 100 clones à un pool de postes de travail et que vous sélectionnez une nouvelle banque de données, View calcule les besoins en espace pour les 100 nouveaux clones.

Si vous sélectionnez un nouveau magasin de données, mais que vous conservez la taille du pool de postes de travail, ou si vous réduisez le nombre de clones, les recommandations de dimensionnement indiquent 0. Les valeurs de 0 indiquent qu'aucun nouveau clone ne doit être créé sur le magasin de données sélectionné. Les besoins en espace pour les clones existants sont déjà pris en compte.

## Comment View calcule les recommandations de dimensionnement minimales

Pour arriver à une recommandation minimale pour les disques du système d'exploitation, View estime que chaque clone consomme deux fois la taille de sa mémoire lors de sa création et de son premier démarrage. Si aucune mémoire n'est réservée pour un clone, un fichier d'échange ESXi est créé pour lui dès sa mise sous tension. La taille du fichier d'échange du système d'exploitation client affecte également la croissance d'un disque du système d'exploitation d'un clone.

Dans les recommandations minimales pour les disques du système d'exploitation, View inclut également de l'espace pour deux réplicas sur chaque banque de données. View Composer crée un réplica lorsqu'un pool est créé. Lorsque le pool est recomposé pour la première fois, View Composer crée un deuxième réplica sur le magasin de données, ancre les clones au nouveau réplica et supprime le premier réplica si aucun autre clone n'utilise le snapshot d'origine. Le magasin de données doit avoir la capacité de stocker deux réplicas au cours de l'opération de recomposition.

Par défaut, les réplicas utilisent vSphere Thin Provisioning, mais pour que les recommandations restent simples, View prend en compte deux réplicas qui utilisent le même espace que la machine virtuelle parente.

Pour arriver à une recommandation minimale pour des disques persistants, View calcule 20 % de la taille de disque que vous spécifiez sur la page **Disques de View Composer** de l'assistant Ajouter un pool.

---

**Remarque** Les calculs pour les disques persistants sont basés sur des valeurs de seuil statique, en gigaoctets. Par exemple, si vous spécifiez une taille de disque persistant à une valeur comprise entre 1 024 Mo et 2 047 Mo, View calcule une taille de disque persistant de 1 Go. Si vous spécifiez une taille de disque de 2 048 Mo, View calcule une taille de disque de 2 Go.

---

Pour arriver à une recommandation pour le stockage de réplicas sur une banque de données distincte, View alloue de l'espace pour deux réplicas sur la banque de données. La même valeur est calculée pour l'utilisation minimale et maximale.

Pour plus d'informations, reportez-vous à « Formules de dimensionnement pour les pools de clone instantané et de clone lié », page 283.

### Recommandations de dimensionnement et surcharge du stockage pour les clones liés View Composer

**Remarque** Les clones instantanés ne prennent pas en charge la surcharge du stockage.

Dès que vous avez estimé les besoins en stockage, sélectionné les banques de données et déployé le pool, View provisionne des machines virtuelles de clone lié sur des banques de données distinctes en fonction de l'espace disponible et des clones existants sur chaque banque de données.

Selon l'option de surcharge de stockage que vous sélectionnez sur la page Sélectionner des banques de données de clones liés dans l'assistant Ajouter un pool de postes de travail, View arrête de provisionner de nouveaux clones et réserve de l'espace disponible pour les clones existants. Ce comportement garantit l'existence d'une mémoire tampon de croissance pour chaque machine de la banque de données.

Si vous sélectionnez un niveau de surcharge de stockage agressif, les exigences de stockage estimées peuvent dépasser la capacité indiquée dans la colonne **Espace libre sélectionné**. Le niveau de surcharge de stockage affecte le nombre de machines virtuelles que View crée réellement sur une banque de données.

Pour plus d'informations, reportez-vous à « Définir le niveau de surcharge du stockage pour des machines virtuelles de clone lié », page 286.

## Formules de dimensionnement pour les pools de clone instantané et de clone lié

Les formules de dimensionnement du stockage peuvent vous aider à estimer la quantité d'espace disque nécessaire sur les magasins de données que vous sélectionnez pour les disques du système d'exploitation, les disques persistants de View Composer et les réplicas.

**Remarque** Les informations sur le disque persistant sont destinées uniquement aux clones liés View Composer. Les clones instantanés ne prennent pas en charge les disques persistants.

### Formules de dimensionnement du stockage

Tableau 16-2 présente les formules qui calculent les estimations de taille des disques lorsque vous créez un pool et au fur et à mesure que les clones croissent. Ces formules incluent l'espace des disques de réplica stockés avec les clones sur le magasin de données.

Si vous modifiez des répliques de pool ou de banque existantes sur une banque de données distincte, View utilise une autre formule de dimensionnement. Reportez-vous à la section « Formules de dimensionnement pour créer des clones lorsque vous modifiez un pool ou stockez des réplicas sur un magasin de données séparé », page 284.

**Tableau 16-2.** Formules de dimensionnement du stockage des disques de clone sur des magasins de données sélectionnés

| Type de données | Espace libre sélectionné (Go) | Min. recommandé (Go) | Utilisation 50 % (Go) | Max. recommandé (Go) |
|---|---|---|---|---|
| Disques du système d'exploitation | Espace libre sur les magasins de données sélectionnés | Nombre de VM * (2 * mémoire de VM) + (2 * disque de réplica) | Nombre de VM * (50 % de disque de réplica + mémoire de VM) + (2 * disque de réplica) | Nombre de VM * (100 % de disque de réplica + mémoire de VM) + (2 * disque de réplica) |
| Disques persistants | Espace libre sur les magasins de données sélectionnés | Nombre de VM * 20 % de disque persistant | Nombre de VM * 50 % de disque persistant | Nombre de VM * 100 % de disque persistant |

### Exemple d'estimation de dimensionnement du stockage

Dans cet exemple, la machine virtuelle parente est configurée avec 1 Go de mémoire. La taille de disque de la machine virtuelle parente est de 10 Go. Un pool comportant 10 machines est créé. Des disques persistants sont configurés avec une taille de 2 048 Mo.

Les disques du système d'exploitation sont configurés sur un magasin de données dont l'espace disponible est actuellement de 184,23 Go. Les disques persistants sont configurés sur un magasin de données différent avec 28,56 Go d'espace disponible.

Tableau 16-3 montre comment les formules de dimensionnement calculent des exigences de stockage estimées pour le pool de postes de travail en exemple.

**Tableau 16-3.** Exemple d'estimation de dimensionnement des disques de clone déployés sur des magasins de données sélectionnés

| Type de données | Espace libre sélectionné (Go) | Min. recommandé (Go) | Utilisation 50 % (Go) | Max. recommandé (Go) |
|---|---|---|---|---|
| Disques du système d'exploitation | 184,23 | 10 * (2*1 Go) + (2*10 Go) = 40,00 | 10 * (50 % de 10 Go + 1 Go) + (2*10 Go) = 80,00 | 10 * (100 % de 10 Go + 1 Go) + (2*10 Go) = 130,00 |
| Disques persistants | 28,56 | 10 * (20 % de 2 Go) = 4,00 | 10 * (50 % de 2 Go) = 10,00 | 10 * (100 % de 2 Go) = 20,00 |

## Formules de dimensionnement pour créer des clones lorsque vous modifiez un pool ou stockez des réplicas sur un magasin de données séparé

View calcule différentes formules de dimensionnement selon que vous modifiez un pool de postes de travail existant ou stockez des réplicas dans une banque de données distincte, ou que vous créez un pool.

Si vous modifiez un pool existant et que vous sélectionnez des magasins de données pour le pool, View Composer crée de nouveaux clones sur les magasins de données sélectionnés. Les nouveaux clones sont ancrés au snapshot existant et utilisent le disque de réplica existant. Aucun nouveau réplica n'est créé.

View estime les besoins en dimensionnement des nouveaux clones qui sont ajoutés au pool de postes de travail. View n'inclut pas les clones existants dans le calcul.

Si vous stockez des réplicas sur un magasin de données séparé, les autres magasins de données sélectionnés sont dédiés aux disques du système d'exploitation.

Tableau 16-4 montre les formules qui calculent les tailles estimées de disques de clone lorsque vous modifiez un pool ou stockez des réplicas sur un magasin de données séparé.

**Tableau 16-4.** Formules de dimensionnement du stockage des disques de clone lorsque vous modifiez un pool ou stockez des réplicas sur un magasin de données séparé

| Type de données | Espace libre sélectionné (Go) | Min. recommandé (Go) | Utilisation 50 % (Go) | Max. recommandé (Go) |
|---|---|---|---|---|
| Disques du système d'exploitation | Espace libre sur les magasins de données sélectionnés | Nombre de nouvelles machines virtuelles * (2 * mémoire de machine virtuelle) | Nombre de nouvelles machines virtuelles * (50 % de disque de réplica + mémoire de machine virtuelle) | Nombre de nouvelles machines virtuelles * (100 % de disque de réplica + mémoire de machine virtuelle) |
| Disques persistants | Espace libre sur les magasins de données sélectionnés | Nombre de nouvelles machines virtuelles * 20 % de disque persistant | Nombre de nouvelles machines virtuelles * 50 % de disque persistant | Nombre de nouvelles machines virtuelles * 100 % de disque persistant |

### Exemple d'estimation de dimensionnement du stockage lorsque vous modifiez un pool ou stockez des réplicas sur un magasin de données séparé

Dans cet exemple, la machine virtuelle parente est configurée avec 1 Go de mémoire. La taille de disque de la machine virtuelle parente est de 10 Go. Un pool comportant 10 machines est créé. Des disques persistants sont configurés avec une taille de 2 048 Mo.

Les disques du système d'exploitation sont configurés sur un magasin de données dont l'espace disponible est actuellement de 184,23 Go. Les disques persistants sont configurés sur un magasin de données différent avec 28,56 Go d'espace disponible.

Tableau 16-5 montre comment les formules de dimensionnement calculent des exigences de stockage estimées pour le pool en exemple.

**Tableau 16-5.** Exemple d'estimation de dimensionnement des disques de clone lorsque vous modifiez un pool ou stockez des réplicas sur un magasin de données séparé

| Type de données | Espace libre sélectionné (Go) | Min. recommandé (Go) | Utilisation 50 % (Go) | Max. recommandé (Go) |
|---|---|---|---|---|
| Disques du système d'exploitation | 184,23 | 10 * (2*1 Go) = 20,00 | 10 * (50 % de 10 Go + 1 Go) = 60,00 | 10 * (100 % de 10 Go + 1 Go) = 110,00 |
| Disques persistants | 28,56 | 10 * (20 % de 2 Go) = 4,00 | 10 * (50 % de 2 Go) = 10,00 | 10 * (100 % de 2 Go) = 20,00 |

## Surcharge de stockage des machines virtuelles de clone lié View Composer

Avec la fonctionnalité de surcharge de stockage, vous pouvez réduire les coûts de stockage en plaçant plus de machines virtuelles de clone lié sur une banque de données qu'il n'est possible avec des machines virtuelles complètes. Les clones liés peuvent utiliser un espace de stockage logique plusieurs fois supérieur à la capacité physique du magasin de données.

**Remarque** Les clones instantanés ne prennent pas en charge la surcharge du stockage.

Cette fonctionnalité vous aide à choisir un niveau de stockage qui vous permet de surcharger la capacité de la banque de données et définit une limite pour le nombre de clones liés créés par View. Vous pouvez éviter de gaspiller du stockage en provisionnant de façon trop conservatrice ou éviter de risquer que les clones liés n'aient plus d'espace disque et provoquent l'échec du système d'exploitation ou des applications.

Par exemple, vous pouvez créer au plus dix machines virtuelles complètes sur un magasin de données de 100 Go, si chaque machine virtuelle est de 10 Go. Lorsque vous créez des clones liés à partir d'une machine virtuelle parente de 10 Go, chaque clone est une fraction de cette taille.

Si vous définissez un niveau de surcharge classique, View permet aux clones d'utiliser quatre fois la taille physique de la banque de données, en mesurant chaque clone comme s'il était de la taille de la machine virtuelle parente. Sur une banque de données de 100 Go, avec un parent de 10 Go, View provisionne environ 40 clones liés. View ne provisionne pas plus de clones, même si la banque de données dispose d'espace disponible. Cette limite conserve une mémoire tampon de croissance pour les clones existants.

Tableau 16-6 montre les niveaux de surcharge de stockage que vous pouvez définir.

**Tableau 16-6.** Niveaux de surcharge de stockage

| Option | Niveau de surcharge de stockage |
|---|---|
| Aucune | Le stockage n'est pas surchargé. |
| Classique | 4 fois la taille du magasin de données. Il s'agit du niveau par défaut. |
| Modérée | 7 fois la taille du magasin de données. |
| Agressive | 15 fois la taille du magasin de données. |

Les niveaux de surcharge de stockage permettent de déterminer la capacité de stockage de façon très efficace. Pour déterminer le meilleur niveau, surveillez la croissance des clones liés dans votre environnement.

Définissez un niveau agressif si vos disques du système d'exploitation n'atteignent jamais leur taille maximale possible. Un niveau de surcharge agressif demande de l'attention. Pour vous assurer que les clones liés ne manquent pas d'espace disque, vous pouvez périodiquement actualiser ou rééquilibrer le pool de postes de travail et réduire les données de système d'exploitation des clones liés à leur taille d'origine. Les batteries de serveurs automatisées ne prennent pas en charge l'actualisation ou le rééquilibrage. Si les clones liés dans une batterie de serveurs automatisée risquent de manquer d'espace disque, modifiez le niveau de surcharge.

Par exemple, il est judicieux de définir un niveau de surcharge agressif pour un pool de postes de travail à attribution flottante dans lequel les machines virtuelles sont définies pour être supprimées ou actualisées après la fermeture de session.

Vous pouvez varier les niveaux de surcharge de stockage parmi les différents types de magasins de données pour cibler différents niveaux de débit dans chaque magasin de données. Par exemple, un magasin de données NAS peut avoir un paramètre différent d'un magasin de données SAN.

## Définir le niveau de surcharge du stockage pour des machines virtuelles de clone lié

Vous pouvez contrôler le niveau d'agressivité selon lequel View crée des machines virtuelles de clone lié sur une banque de données en utilisant la fonction de surcharge de stockage. Cette fonction vous permet de créer des clones liés ayant une taille logique totale supérieure à la limite de stockage physique du magasin de données.

Cette fonction œuvre uniquement avec des pools de clone lié et des batteries de serveurs automatisées.

Le niveau de surcharge de stockage calcule la quantité de stockage supérieure à la taille physique du magasin de données que les clones utiliseraient si chaque clone était une machine virtuelle complète. Pour plus d'informations, reportez-vous à « Surcharge de stockage des machines virtuelles de clone lié View Composer », page 285. La procédure suivante s'applique à des pools de postes de travail de clone lié. Les étapes sont semblables pour les batteries de serveurs automatisées.

### Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

2 Lorsque vous créez un nouveau pool de postes de travail ou que vous modifiez un pool existant, accédez à la page Paramètres de vCenter.

| Option | Action |
|---|---|
| **New desktop pool (Nouveau pool de postes de travail)** | a Cliquez sur **Ajouter**.<br>b Exécutez l'assistant Ajouter un pool de postes de travail jusqu'à la page Paramètres de vCenter. |
| **Existing desktop pool (Pool de postes de travail existant)** | a Sélectionnez le pool de clone lié et cliquez sur **Modifier**.<br>b Cliquez sur l'onglet **Paramètres de vCenter**. |

3 Dans la page Paramètres de vCenter, cliquez sur **Parcourir** en regard de **Magasins de données**.

4 Sélectionnez la banque de données dans la page Sélectionner des banques de données de clone lié.

Un menu déroulant s'affiche dans la colonne Surcharge du stockage pour la banque de données sélectionnée.

5 Sélectionnez le niveau de surcharge du stockage dans le menu déroulant.

| Option | Description |
|---|---|
| **Aucune** | Le stockage n'est pas surchargé. |
| **Classique** | 4 fois la taille du magasin de données. Il s'agit du niveau par défaut. |
| **Modérée** | 7 fois la taille du magasin de données. |
| **Agressive** | 15 fois la taille du magasin de données. |
| **Illimitée** | View ne limite pas le nombre de postes de travail de clone lié qu'il crée en fonction de la capacité physique de la banque de données. Sélectionnez ce niveau uniquement si vous êtes certain que la banque de données dispose d'une capacité de stockage suffisante pour prendre en charge toutes les machines et leur croissance future. |

6 Cliquez sur **OK**.

# Disques de données de clone lié View Composer

View Composer crée plusieurs disques de données pour stocker les composants d'une machine virtuelle de clone lié.

## Disque du système d'exploitation

View Composer crée un disque du système d'exploitation pour chaque clone lié. Ce disque stocke les données du système dont le clone a besoin pour rester lié à l'image de base et pour fonctionner en tant que machine virtuelle unique.

## Disque de données de configuration QuickPrep

View Composer crée un deuxième disque avec le disque du système d'exploitation. Le deuxième disque stocke les données de configuration QuickPrep et d'autres données liées au système d'exploitation qui doivent être conservées au cours d'opérations d'actualisation et de recomposition. Le disque est de petite taille, généralement aux alentours de 20 Mo. Ce disque est toujours créé, que vous utilisiez QuickPrep ou Sysprep pour personnaliser la machine virtuelle.

Si vous configurez des disques persistants séparés de View Composer pour stocker des profils d'utilisateur, trois disques sont associés à chaque clone lié : le disque du système d'exploitation, le disque de la seconde machine virtuelle et le disque persistant de View Composer.

Le disque de la seconde machine virtuelle est stocké dans la même banque de données que le disque du système d'exploitation. Vous ne pouvez pas configurer ce disque.

### Disque persistant de View Composer

Dans un pool d'affectation dédiée, vous pouvez configurer des disques persistants séparés de View Composer pour stocker des données de profil d'utilisateur Windows. Ce disque est facultatif.

Les disques persistants séparés vous permettent de conserver des données et des paramètres d'utilisateur. Les opérations d'actualisation, de recomposition et de rééquilibrage de View Composer n'affectent pas les disques persistants. Vous pouvez détacher un disque persistant d'un clone lié et l'attacher à un autre clone lié.

Si vous ne configurez pas de disques persistants séparés, le profil Windows est stocké sur le disque du système d'exploitation. Les données et les paramètres d'utilisateur sont supprimés au cours des opérations d'actualisation, de recomposition et de rééquilibrage.

Vous pouvez stocker des disques persistants sur le même magasin de données que le disque du système d'exploitation ou sur un magasin de données différent.

### Disque de données supprimables

Lorsque vous créez un pool de clone lié, vous pouvez configurer un disque non persistant séparé pour stocker les fichiers d'échange et temporaires du système d'exploitation client qui sont générés au cours de sessions utilisateur. Vous devez spécifier la taille du disque en mégaoctets.

Ce disque est facultatif.

Lorsqu'un clone lié est mis hors tension, View remplace le disque de données supprimables par une copie du disque d'origine que View Composer a créé avec le pool de clones liés. La taille des clones liés peut augmenter à mesure que les utilisateurs interagissent avec leurs postes de travail. L'utilisation de disques de données supprimables peut économiser de l'espace de stockage en ralentissant la croissance des clones liés.

Le disque de données supprimables est stocké sur le même magasin de données que le disque du système d'exploitation.

## Stockage de clones liés View Composer sur des magasins de données locaux

Des machines virtuelles de clone lié peuvent être stockées sur des banques de données locales, qui sont des disques de rechange internes sur des hôtes ESXi. Le stockage local offre divers avantages tels que matériel peu coûteux, provisionnement de machine virtuelle rapide, opérations d'alimentation haute performance et gestion simplifiée. Cependant, l'utilisation du stockage local limite les options de configuration de l'infrastructure vSphere qui sont à votre disposition. L'utilisation du stockage local est utile dans certains environnements View mais n'est pas appropriée dans d'autres.

**Remarque** Les limites décrites dans cette section ne s'appliquent pas aux banques de données Virtual SAN qui utilisent également des disques de stockage local mais nécessitent un matériel spécifique.

L'utilisation de magasins de données locaux fonctionnera mieux si les postes de travail View dans votre environnement sont sans état. Par exemple, vous pouvez utiliser des magasins de données locaux si vous déployez des kiosques ou des stations de classe et de formation sans état.

Vous pouvez envisager l'utilisation de banques de données locales si vos machines virtuelles disposent d'attributions flottantes, ne sont pas dédiées à des utilisateurs finaux individuels, ne nécessitent pas de disques persistants pour les données utilisateur, et peuvent être supprimées ou actualisées à intervalles réguliers, par exemple lors de la déconnexion d'un utilisateur. Cette approche vous permet de contrôler l'utilisation des disques sur chaque banque de données locale sans devoir déplacer les machines virtuelles entre des banques de données ni effectuer un équilibrage de charge entre celles-ci.

Cependant, vous devez tenir compte des restrictions qu'impose l'utilisation de banques de données locales sur votre déploiement de postes de travail ou de batterie de serveurs View :

- Vous ne pouvez pas utiliser VMotion pour gérer des volumes.
- Vous ne pouvez pas équilibrer la charge des machines virtuelles dans un pool de ressources. Par exemple, vous ne pouvez pas utiliser l'opération de rééquilibrage de View Composer avec des clones liés qui sont stockés sur des banques de données locales.
- Vous ne pouvez pas utiliser VMware High Availability.
- Vous ne pouvez pas utiliser vSphere Distributed Resource Scheduler (DRS).
- Vous ne pouvez pas stocker un réplica et des clones liés View Composer sur des banques de données séparées si le réplica se trouve sur une banque de données locale.

  Lorsque vous stockez des clones liés sur des banques de données locales, VMware recommande instamment de stocker le réplica sur le même volume que les clones liés. Bien qu'il soit possible de stocker les clones liés sur des banques de données locales et le réplica sur une banque de données partagée, si tous les hôtes ESXi du cluster peuvent accéder au réplica, VMware ne recommande pas cette configuration.
- Si vous sélectionnez des disques dur rotatifs locaux, les performances risquent de ne pas correspondre à celles d'une baie de stockage disponible sur le marché. Les disques durs rotatifs locaux et une baie de stockage peuvent avoir une capacité similaire, mais les disques durs rotatifs locaux n'offrent pas le même débit qu'une baie de stockage. Le débit est directement proportionnel au nombre de piles.

Si vous sélectionnez des disques SSD (solid-state disks) directement raccordés, les performances sont susceptibles de dépasser celles de nombreuses baies de stockage.

Vous pouvez stocker des clones liés sur une banque de données locale sans contrainte si vous configurez le pool de postes de travail ou la batterie de serveurs sur un seul hôte ESXi ou sur un cluster qui contient un seul hôte ESXi. Cependant, l'utilisation d'un seul hôte ESXi limite la taille du pool de postes de travail ou de la batterie de serveurs que vous pouvez configurer.

Pour configurer un grand pool de postes de travail ou une grande batterie de serveurs, vous devez sélectionner un cluster qui contient plusieurs hôtes ESXi disposant de la capacité collective permettant la prise en charge d'un grand nombre de machines virtuelles.

Si vous prévoyez de tirer parti des avantages du stockage local, vous devez soigneusement envisager les conséquences de ne pas disposer de VMotion, HA, DRS et autres fonctionnalités disponibles. Si vous gérez l'utilisation du disque local en contrôlant le nombre de disques de machines virtuelles et leur croissance, et si vous utilisez des attributions flottantes et effectuez régulièrement des opérations d'actualisation et de suppression, vous pouvez réussir à déployer des clones liés sur des banques de données locales.

## Stockage de réplicas et de clones sur des magasins de données séparés pour des clones instantanés et des clones liés View Composer

Vous pouvez placer des réplicas et des clones sur des magasins de données séparés avec différentes caractéristiques de performance. Cette configuration peut accélérer les opérations qui sollicitent le disque dur de manière intensive, telles que le provisionnement ou l'exécution d'analyses antivirus, en particulier pour les clones liés View Composer.

Par exemple, vous pouvez stocker les machines virtuelles réplicas sur un magasin de données sur disque électronique. Les disques électroniques ont une capacité de stockage faible et des performances de lecture élevées. Ils prennent en charge généralement 20 000 E/S par seconde (IOPS). Un environnement classique ne contient qu'un petit nombre de VM réplicas, donc les réplicas ne nécessitent pas autant de stockage.

Vous pouvez stocker des clones sur des magasins de données sur des supports de rotation traditionnels. Ces disques fournissent des performances inférieures et prennent en charge en général 200 IOPS. Ils sont bon marché et fournissent une capacité de stockage élevée ; ils sont donc adaptés au stockage d'un grand nombre de clones.

Configurer les réplicas et les clones de cette manière peut réduire l'impact des tempêtes d'E/S qui se produisent lorsque de nombreux clones sont créés simultanément, en particulier pour les clones liés View Composer. Par exemple, si vous déployez un pool à attribution flottante avec une stratégie de « suppression du poste de travail à la fermeture de session », et que vos utilisateurs commencent tous à travailler en même temps, View doit provisionner simultanément de nouvelles machines pour eux.

---

**Important** Cette fonction est conçue pour des configurations de stockage spécifiques de fournisseurs qui offrent des solutions de disque haute performance. Ne stockez pas de réplicas sur un magasin de données séparé si votre matériel de stockage ne prend pas en charge les performances de lecture élevées.

---

Vous devez satisfaire certaines exigences lorsque vous stockez le réplica et les clones d'un pool sur des magasins de données séparés :

- Vous ne pouvez spécifier qu'un magasin de données réplica séparé pour chaque pool.
- Le magasin de données réplica doit être accessible depuis tous les hôtes ESXi dans le cluster.
- Pour les clones liés View Composer, si les clones se trouvent sur des magasins de données locaux, VMware recommande instamment de stocker le réplica sur le même volume que les clones liés. Bien qu'il soit possible de stocker les clones liés sur des banques de données locales et le réplica sur une banque de données partagée, si tous les hôtes ESXi du cluster peuvent accéder au réplica, VMware ne recommande pas cette configuration.
- Cette fonctionnalité n'est pas disponible si vous utilisez des banques de données Virtual SAN ou des banques de données Virtual Volumes. Ces types de banques de données utilisent la gestion basée sur la stratégie du logiciel afin que les profils de stockage définissent quels composants vont sur quels types de disques.

### Considérations sur la disponibilité pour le stockage de réplicas sur un magasin de données séparé

Vous pouvez stocker des machines virtuelles réplicas sur un magasin de données séparé ou sur les mêmes magasins de données que les clones. Ces configurations affectent la disponibilité du pool de différentes façons.

Lorsque vous stockez des réplicas sur les mêmes magasins de données que les clones, un réplica séparé est créé sur chaque magasin de données pour améliorer la disponibilité. Si un magasin de données devient indisponible, seuls les clones sur ce magasin de données sont affectés. Les clones sur d'autres magasins de données sont toujours exécutés.

Lorsque vous stockez des réplicas sur un magasin de données séparé, tous les clones du pool sont ancrés aux réplicas sur ce magasin de données. Si le magasin de données devient indisponible, l'intégralité du pool est indisponible.

Pour améliorer la disponibilité du pool de postes de travail, vous pouvez configurer une solution haute disponibilité pour le magasin de données sur lequel vous stockez les réplicas.

## Configurer View Storage Accelerator des clones liés View Composer

Vous pouvez configurer des pools de postes de travail de clone lié View Composer afin de permettre aux hôtes ESXi de mettre en cache des données de disque de machine virtuelle. Cette fonction, appelée View Storage Accelerator, utilise la fonction CBRC (Content Based Read Cache) dans les hôtes ESXi. View Storage Accelerator peut réduire l'IOPS et améliorer les performances au cours des tempêtes de démarrage, lorsque

plusieurs machines démarrent ou exécutent des analyses antivirus simultanément. La fonction est également utile lorsque des administrateurs ou des utilisateurs chargent des applications ou des données fréquemment. Pour utiliser cette fonction, vous devez vérifier que View Storage Accelerator est activé pour les pools de postes de travail individuels.

**Remarque** Pour les clones instantanés, cette fonctionnalité est activée automatiquement et n'est pas configurable.

Lorsqu'une machine virtuelle est créée, View indexe le contenu de chaque fichier de disque virtuel. Les index sont stockés dans un fichier condensé de machine virtuelle. Au moment de l'exécution, l'hôte ESXi lit les fichiers condensés et met en cache les blocs de données communs dans la mémoire. Pour maintenir le cache de l'hôte ESXi à jour, View régénère les fichiers condensés à des intervalles spécifiés et lorsque la machine virtuelle est recomposée. Vous pouvez modifier l'intervalle de régénération.

View Storage Accelerator est activé pour un pool par défaut. Vous pouvez activer ou désactiver cette fonctionnalité lors de la création ou de la modification d'un pool. La meilleure approche consiste à activer cette fonctionnalité lorsque vous créez un pool de postes de travail pour la première fois. Si vous activez cette fonctionnalité en modifiant un pool existant, vous devez vous assurer qu'un nouveau réplica et ses disques digest soient créés avant que des clones liés soient provisionnés. Vous pouvez créer un nouveau réplica en recomposant le pool sur un nouveau snapshot ou en rééquilibrant le pool sur une nouvelle banque de données. Les fichiers digest peuvent être configurés uniquement pour des machines virtuelles dans un pool de postes de travail où elles sont désactivées.

Vous pouvez activer View Storage Accelerator sur des pools contenant des clones liés et sur des pools contenant des machines virtuelles complètes.

View Storage Accelerator est maintenant conçu pour fonctionner dans des configurations qui utilisent la hiérarchisation de réplica View, dans lesquelles des réplicas sont stockés dans un magasin de données séparé des clones liés. Bien que les avantages de performance de l'utilisation de View Storage Accelerator avec la hiérarchisation de réplica View ne soient pas matériellement importants, certains avantages liés à la capacité peuvent être atteints en stockant les réplicas sur un magasin de données séparé. Par conséquent, cette combinaison est testée et prise en charge.

**Important** Si vous prévoyez d'utiliser cette fonctionnalité et que vous utilisez plusieurs espaces View qui partagent des hôtes ESXi, vous devez activer la fonction View Storage Accelerator pour tous les pools qui se trouvent sur les hôtes ESXi partagés. Si les paramètres ne sont pas les mêmes sur tous les espaces, cela peut entraîner l'instabilité des machines virtuelles des hôtes ESXi partagés.

### Prérequis

- Vérifiez que vos hôtes vCenter Server et ESXi sont les versions 5.0 ou supérieures.

  Dans un cluster ESXi, vérifiez que la version de tous les hôtes est la version 5.0 ou supérieure.

- Vérifiez que l'utilisateur de vCenter Server a reçu le privilège **Hôte > Configuration > Paramètres avancés** dans vCenter Server. Consultez les rubriques de la documentation *Installation de View* qui décrivent les privilèges de View et de View Composer requis pour l'utilisateur de vCenter Server.
- Vérifiez que View Storage Accelerator est activé dans vCenter Server. Reportez-vous au document *Administration de View*.

### Procédure

1 Dans View Administrator, affichez la page Options de stockage avancées.

| Option | Description |
|---|---|
| **Nouveau pool de postes de travail (recommandé)** | Démarrez l'assistant Ajouter un pool de postes de travail pour commencer à créer un pool de postes de travail automatisé. Suivez les invites de configuration de l'assistant jusqu'à la page Options de stockage avancées. |
| **Existing desktop pool (Pool de postes de travail existant)** | Sélectionnez le pool existant, cliquez sur **Modifier** et cliquez sur l'onglet **Stockage avancé**.<br>Dans un pool existant, les fichiers condensés de View Storage Accelerator ne sont pas configurés pour les machines virtuelles tant qu'elles sont activées. |

2 Pour activer View Storage Accelerator pour le pool, vérifiez que la case **Utiliser View Storage Accelerator** est cochée.

   Ce paramètre est sélectionné par défaut. Pour désactiver le paramètre, décochez la case **Utiliser View Storage Accelerator**.

3 (Facultatif) Spécifiez les types de disques à mettre en cache en sélectionnant **Disques du système d'exploitation** uniquement ou **Disques du système d'exploitation et persistants** dans le menu **Types de disques**.

   **Disques du système d'exploitation** est sélectionné par défaut.

   Si vous configurez View Storage Accelerator pour des machines virtuelles complètes, vous ne pouvez pas sélectionner un type de disque. View Storage Accelerator est exécuté sur toute la machine virtuelle.

4 (Facultatif) Dans la zone de texte **Régénérer l'accélérateur de stockage après**, spécifiez l'intervalle, en jours, après lequel se produit la régénération des fichiers condensés de View Storage Accelerator.

   L'intervalle de régénération par défaut est de 7 jours.

### Suivant

Vous pouvez configurer des jours et des heures d'interruption durant lesquels la récupération d'espace disque et la régénération de View Storage Accelerator n'ont pas lieu. Reportez-vous à la section « Définir les durées d'interruption de Storage Accelerator et de récupération d'espace des clones liés View Composer », page 295.

Si vous activez View Storage Accelerator en modifiant un pool existant, recomposez le pool de postes de travail sur un nouveau snapshot ou rééquilibrez le pool sur une nouvelle banque de données avant que les clones liés soient provisionnés.

## Récupérer l'espace disque sur des clones liés View Composer

Dans vSphere 5.1 et versions ultérieures, vous pouvez configurer la fonction de récupération d'espace disque pour les pools de postes de travail de clone lié View Composer et les batteries de serveurs automatisées. À partir de vSphere 5.1, View crée des machines virtuelles de clone lié dans un format de disque efficace qui permet à des hôtes ESXi de récupérer l'espace disque inutilisé sur les clones liés, ce qui réduit l'espace de stockage total requis pour les clones liés.

**Remarque** Pour les clones instantanés, cette fonctionnalité n'est pas nécessaire, car les clones sont toujours recréés lorsque les utilisateurs se déconnectent.

À mesure que les utilisateurs interagissent avec les machines virtuelles, les disques du système d'exploitation des clones liés augmentent et peuvent finir par utiliser presque autant d'espace disque que des machines virtuelles de clone complet. La récupération d'espace disque réduit la taille des disques du système d'exploitation sans que vous ayez à actualiser ou recomposer les clones liés. L'espace peut être récupéré lorsque les machines virtuelles sont activées et que les utilisateurs interagissent avec les machines.

Dans View Administrator, vous ne pouvez pas initier directement la récupération d'espace disque pour un pool. Vous déterminez le moment auquel View initie la récupération d'espace disque en spécifiant la quantité minimale d'espace disque inutilisé qui doit être atteinte sur un disque du système d'exploitation de clone lié pour déclencher l'opération. Lorsque l'espace disque inutilisé dépasse le seuil spécifié, View demande à l'hôte ESXi de récupérer l'espace sur ce disque du système d'exploitation. View applique le seuil sur chaque machine virtuelle dans le pool.

Vous pouvez utiliser l'option `vdmadmin -M` pour initier la récupération d'espace disque sur une machine virtuelle particulière à des fins de démonstration ou de dépannage. Reportez-vous au document *Administration de View*.

Vous pouvez configurer la récupération d'espace disque sur des clones liés lorsque vous créez un nouveau pool ou lorsque vous modifiez un pool existant. Pour un pool existant, reportez-vous à la section « Tâches de mise à niveau de pools pour utiliser la récupération d'espace » du document *Mises à niveau de View*.

---

**Remarque** Cette fonctionnalité n'est pas disponible pour les machines virtuelles stockées sur une banque de données Virtual SAN ou une banque de données Virtual Volumes.

---

Si View Composer actualise, recompose ou rééquilibre des clones liés, la récupération d'espace disque n'a pas lieu sur ces clones liés.

La récupération d'espace disque fonctionne uniquement sur les disques du système d'exploitation dans des clones liés. La fonction n'affecte pas les disques persistants de View Composer et ne fonctionne pas sur les machines virtuelles de clone complet.

La technologie de snapshot NFS natif (VAAI) n'est pas prise en charge dans les pools contenant des machines virtuelles avec des disques à optimisation d'espace.

La procédure suivante s'applique à des pools de postes de travail de clone lié. Les étapes sont semblables pour les batteries de serveurs automatisées.

### Prérequis

- Vérifiez que vos hôtes de vCenter Server et ESXi, notamment tous les hôtes ESXi d'un cluster, sont à la version 5.1 avec le correctif de téléchargement ESXi 5.1 ESXi510-201212001 ou version ultérieure.
- Vérifiez que VMware Tools fourni avec vSphere 5.1 ou supérieur est installé sur toutes les machines virtuelles de cloné lié dans le pool.
- Vérifiez que toutes les machines virtuelles de cloné lié dans le pool ont la version matérielle virtuelle 9 ou supérieure.
- Vérifiez que les machines virtuelles utilisent des contrôleurs SCSI. La récupération d'espace disque n'est pas prise en charge sur les machines virtuelles avec des contrôleurs IDE.
- Pour les machines virtuelles Windows 10, vérifiez que les machines s'exécutent dans vSphere 5.5 U3 ou version ultérieure.
- Pour les machines virtuelles Windows 8 ou 8.1, vérifiez que les machines s'exécutent dans vSphere 5.5 ou version ultérieure. La récupération d'espace disque est prise en charge sur des machines virtuelles Windows 8 ou 8.1 dans vSphere 5.5 ou version ultérieure.
- Pour les machines virtuelles Windows 7, vérifiez que les machines s'exécutent dans vSphere 5.1 ou version ultérieure.

- Vérifiez que la récupération d'espace disque est activée dans vCenter Server. Cette option garantit que les machines virtuelles dans le pool sont créées au format de disque efficace requis pour récupérer l'espace disque. Reportez-vous au document *Administration de View*.

### Procédure

1 Dans View Administrator, affichez la page Stockage avancé.

| Option | Description |
|---|---|
| **New desktop pool (Nouveau pool de postes de travail)** | Démarrez l'assistant Ajouter un pool de postes de travail pour commencer à créer un pool de postes de travail automatisé. Suivez les invites de configuration de l'assistant jusqu'à la page Options de stockage avancées. |
| **Existing desktop pool (Pool de postes de travail existant)** | Sélectionnez le pool existant, cliquez sur **Modifier** et cliquez sur l'onglet **Stockage avancé**. Pour mettre à niveau un pool afin qu'il prenne en charge la récupération d'espace, reportez-vous à la section « Mettre à niveau des pools de postes de travail pour la récupération d'espace » du document *Mises à niveau de View*. |

2 Cochez la case **Récupérer l'espace disque de machine virtuelle**.

3 Dans le champ **Initier la récupération lorsque l'espace inutilisé de la machine virtuelle dépasse**, tapez la quantité minimale d'espace disque inutilisée, en giga-octets, qui doit être atteinte sur un disque du système d'exploitation de clone lié avant qu'ESXi démarre la récupération de l'espace sur ce disque.

   Par exemple : `2` Go.

   La valeur par défaut est 1 Go.

### Suivant

Vous pouvez configurer des jours et des heures d'interruption durant lesquels la récupération d'espace disque et la régénération de View Storage Accelerator n'ont pas lieu. Reportez-vous à la section « Définir les durées d'interruption de Storage Accelerator et de récupération d'espace des clones liés View Composer », page 295.

Dans View Administrator, vous pouvez sélectionner **Catalogue > Pools de postes de travail** et sélectionner une machine pour afficher l'heure de la dernière récupération d'espace et la dernière quantité d'espace récupérée sur la machine.

## Utilisation du stockage VAAI des clones liés View Composer

Si votre déploiement inclut des périphériques NAS qui prennent en charge la technologie VAAI (vStorage APIs for Array Integration), vous pouvez activer la fonctionnalité VCAI (View Composer Array Integration) sur des pools de postes de travail de clone lié View Composer. Cette fonction utilise la technologie de snapshot NFS natif pour cloner des machines virtuelles.

**Remarque** Dans Horizon 7.0, les clones instantanés ne prennent pas en charge VAAI.

Avec cette technologie, la baie de disques NFS clone les fichiers de la machine virtuelle sans demander à l'hôte ESXi de lire et d'écrire les données. Cette opération peut réduire la durée et la charge réseau nécessaires lors du clonage de machines virtuelles.

Appliquez ces recommandations à l'utilisation de la technologie de snapshot NFS natif :

- Vous pouvez utiliser cette fonction uniquement si vous configurez des pools de postes de travail et des batteries de serveurs automatisées sur des magasins de données résidant sur des périphériques NAS prenant en charge les opérations de clonage natif via VAAI.
- Vous pouvez utiliser des fonctions de View Composer pour gérer des clones liés qui sont créés par la technologie de snapshot NFS natif. Par exemple, vous pouvez actualiser, recomposer, rééquilibrer, créer des disques persistants et exécuter des scripts de personnalisation QuickPrep sur ces clones.

- Vous ne pouvez pas utiliser cette fonction si vous stockez des réplicas et des disques du système d'exploitation sur des magasins de données séparés.
- Cette fonction est prise en charge sur vSphere 5.0 et supérieur.
- Si vous modifiez un pool et si vous sélectionnez ou désélectionnez la fonction de clonage NFS native, des machines virtuelles existantes ne sont pas affectées.

  Pour modifier des machines virtuelles existantes de clones NFS natifs en clones de fichiers journaux traditionnels, vous devez désélectionner la fonction de clonage NFS natif et recomposer le pool vers une nouvelle image de base. Pour modifier la méthode de clonage pour toutes les machines virtuelles dans un pool et utiliser un magasin de données différent, vous devez sélectionner le nouveau magasin de données, désélectionner la fonction de clonage NFS natif, rééquilibrer le pool vers le nouveau magasin de données et recomposer le pool vers une nouvelle image de base.

  De la même façon, pour modifier des machines virtuelles de clones de fichiers journaux traditionnels en clones NFS natifs, vous devez sélectionner un magasin de données NAS prenant en charge VAAI, sélectionner la fonction de clonage NFS natif, rééquilibrer le pool vers le magasin de données NAS et recomposer le pool. Pour plus d'informations, reportez-vous à la section http://kb.vmware.com/kb/2088995.
- Sur un cluster ESXi, pour configurer le clonage natif sur un magasin de données NFS sélectionné dans View Administrator, vous devrez peut-être installer des plug-ins NAS spécifiques du fournisseur qui prennent en charge les opérations de clonage natif sur VAAI sur tous les hôtes ESXi dans le cluster. Pour plus d'informations sur les exigences de configuration, consultez la documentation de votre fournisseur de stockage.
- La technologie de snapshot NFS natif (VAAI) n'est pas prise en charge sur les machines virtuelles comportant des disques à optimisation d'espace.
- Cette fonctionnalité n'est pas disponible si vous utilisez une banque de données Virtual SAN ou une banque de données Virtual Volumes.
- Consultez dans l'article de la base de connaissances VMware KB 2061611 les réponses aux questions fréquemment posées concernant la prise en charge de VCAI dans View.

**Important** Les fournisseurs de stockage NAS peuvent fournir des paramètres supplémentaires qui peuvent affecter les performances et le fonctionnement de VAAI. Vous devez suivre les recommandations du fournisseur et configurer les paramètres appropriés sur la baie de stockage NAS et ESXi. Pour plus d'informations sur la configuration des paramètres recommandés par le fournisseur, consultez la documentation de votre fournisseur de stockage.

## Définir les durées d'interruption de Storage Accelerator et de récupération d'espace des clones liés View Composer

Pour des clones liés View Composer, la régénération des fichiers condensés pour View Storage Accelerator et la récupération de l'espace disque de machine virtuelle peuvent utiliser des ressources ESXi. Pour vous assurer que des ressources ESXi sont dédiées à des tâches de premier plan lorsque cela est nécessaire, vous pouvez empêcher les hôtes ESXi d'exécuter ces opérations pendant des périodes de temps spécifiées certains jours.

**Remarque** Pour les clones instantanés, cette fonctionnalité n'est pas nécessaire.

Par exemple, vous pouvez spécifier une période d'interruption tous les matins du lundi au vendredi, lorsque les utilisateurs commencent à travailler. Des tempêtes de démarrage et des tempêtes d'E/S d'analyse antivirus ont lieu. Vous pouvez spécifier différentes durées d'interruption selon les jours.

La récupération d'espace disque et la régénération des fichiers condensés de View Storage Accelerator n'ont pas lieu lors des heures d'interruption que vous avez définies. Vous ne pouvez pas définir une durée d'interruption séparée pour chaque opération.

View autorise la création de fichiers condensés View Storage Accelerator pour les nouvelles machines lors de l'étape de provisionnement, même au cours d'une interruption.

La procédure suivante s'applique à des pools de postes de travail de clone lié. Les étapes sont semblables pour les batteries de serveurs automatisées.

### Prérequis

- Vérifiez que **Activer View Storage Accelerator**, **Activer la récupération d'espace** ou les deux fonctions sont sélectionnées pour vCenter Server.
- Vérifiez que **Utiliser View Storage Accelerator**, **Récupérer l'espace disque de machine virtuelle** ou les deux fonctions sont sélectionnées pour le pool de postes de travail.

### Procédure

1. Sur la page Stockage avancé de l'assistant Ajouter un pool de postes de travail, accédez à **Durée d'interruption** et cliquez sur **Ajouter**.

   Si vous modifiez un pool existant, cliquez sur l'onglet **Stockage avancé**.

2. Cochez les jours d'interruption et spécifiez les heures de début et de fin.

   Le sélecteur horaire utilise une horloge de 24 heures. Par exemple, 10:00 correspond à 10:00 a.m. et 22:00 à 10:00 p.m.

3. Cliquez sur **OK**.
4. Pour ajouter une autre période d'interruption, cliquez sur **Ajouter** et spécifiez une autre période.
5. Pour modifier ou supprimer une période d'interruption, sélectionnez la période dans la liste Durée d'interruption et cliquez sur **Modifier** ou **Supprimer**.

# Configuration de stratégies pour des pools de postes de travail et d'applications

# 17

Vous pouvez configurer des stratégies pour contrôler le comportement des pools de postes de travail et d'applications, des machines et des utilisateurs. Vous utilisez View Administrator pour configurer des stratégies pour des sessions clientes. Vous pouvez utiliser les paramètres de stratégie de groupe Active Directory pour contrôler le comportement d'Horizon Agent, d'Horizon Client pour Windows et des fonctionnalités qui affectent les machines mono-utilisateur, les hôtes RDS, PCoIP ou VMware Blast.

Ce chapitre aborde les rubriques suivantes :



## Définition de règles dans View Administrator

Vous utilisez View Administrator pour configurer des règles pour des sessions client.

Vous pouvez définir ces règles pour affecter des utilisateurs spécifiques, des pools de postes de travail spécifiques ou tous les utilisateurs de sessions client. Les stratégies qui affectent des utilisateurs et des pools de postes de travail spécifiques sont appelées stratégies au niveau des utilisateurs et stratégies au niveau des pools. Les règles qui affectent toutes les sessions et utilisateurs sont appelées règles générales.

Les stratégies au niveau des utilisateurs héritent des paramètres équivalents des stratégies au niveau des pools de postes de travail. De même, les stratégies au niveau des pools de postes de travail héritent des paramètres équivalents des stratégie globales. Un paramètre de stratégie au niveau des pools de postes de travail a priorité sur le paramètre équivalent de stratégie globale. Un paramètre de stratégie au niveau des utilisateurs a priorité sur les paramètres équivalents de stratégie globale et de stratégie au niveau des pools de postes de travail.

Les paramètres de règle de niveau inférieur peuvent être plus ou moins restrictifs que les paramètres de niveau supérieur équivalents. Par exemple, vous pouvez définir une stratégie globale sur **Refuser** et la stratégie au niveau des pools de postes de travail équivalente sur **Autoriser**, ou l'inverse.

---

**Remarque** Seules les stratégies globales sont disponibles pour les pools de postes de travail et d'applications RDS. Vous ne pouvez pas définir des stratégies de niveau utilisateur ou des stratégies de niveau pools pour les pools de postes de travail et d'applications RDS.

---

## Configurer des paramètres de règle générale

Vous pouvez configurer des règles générales pour contrôler le comportement de tous les utilisateurs de sessions client.

### Prérequis

Familiarisez-vous avec les descriptions de règles. Reportez-vous à la section « Règles de View », page 299.

### Procédure

1 Dans View Administrator, sélectionnez **Règles > Règles générales**.

2 Cliquez sur **Modifier des stratégies** dans le volet **Règles de View**.

3 Cliquez sur **OK** pour enregistrer vos modifications.

## Configurer des règles pour des pools de postes de travail

Vous pouvez configurer des règles de niveau poste de travail pour affecter des pools de postes de travail spécifiques. Les paramètres de règle de niveau poste de travail sont prioritaires par rapport à leurs paramètres de règle générale équivalents.

### Prérequis

Familiarisez-vous avec les descriptions de règles. Reportez-vous à la section « Règles de View », page 299.

### Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

2 Double-cliquez sur l'ID du pool de postes de travail et cliquez sur l'onglet **Règles**.

   L'onglet **Règles** montre les paramètres de règle actuels. Lorsqu'un paramètre est hérité de la stratégie générale équivalente, **Hériter** s'affiche dans la colonne **Stratégie de pools de postes de travail**.

3 Cliquez sur **Modifier les stratégies** dans le volet **Règles de View**.

4 Cliquez sur **OK** pour enregistrer vos modifications.

## Configurer des stratégies pour les utilisateurs

Vous pouvez configurer des règles de niveau utilisateur pour affecter des utilisateurs spécifiques. Les paramètres de stratégie de niveau utilisateur sont toujours prioritaires par rapport aux paramètres de stratégie généraux et de niveau poste de travail équivalents.

### Prérequis

Familiarisez-vous avec les descriptions de règles. Reportez-vous à la section « Règles de View », page 299.

### Procédure

1 Dans View Administrator, sélectionnez **Catalogue > Pools de postes de travail**.

2 Double-cliquez sur l'ID du pool de postes de travail et cliquez sur l'onglet **Règles**.

   L'onglet **Règles** montre les paramètres de règle actuels. Lorsqu'un paramètre est hérité de la stratégie générale équivalente, **Hériter** s'affiche dans la colonne **Stratégie de pools de postes de travail**.

3 Cliquez sur **Remplacements d'utilisateur** et sur **Ajouter un utilisateur**.

4 Pour rechercher un utilisateur, cliquez sur **Ajouter**, saisissez le nom ou la description de l'utilisateur, puis cliquez sur **Rechercher**.

5 Sélectionnez un ou plusieurs utilisateurs dans la liste, cliquez sur **OK**, puis sur **Suivant**.

   La boîte de dialogue Add Individual Policy (Ajouter une règle individuelle) apparaît.

6 Configurez les stratégies de View et cliquez sur **Terminer** pour enregistrer vos modifications.

### Règles de View

Vous pouvez configurer des stratégies View pour affecter toutes les sessions clientes, ou vous pouvez les appliquer pour affecter des pools de postes de travail ou des utilisateurs spécifiques.

Tableau 17-1 décrit chaque paramètre de stratégie View.

**Tableau 17-1.** Règles de View

| Règle | Description |
|---|---|
| Redirection multimédia (MMR) | Détermine si MMR est activé pour les systèmes client.<br>MMR est un filtre de Windows Media Foundation qui permet de transférer des données multimédia de codecs spécifiques sur des postes de travail distants au système client directement via un socket TCP. Les données sont ensuite directement décodées sur le système client, lorsqu'elles sont lues.<br>La valeur par défaut est **Refuser**.<br>Si les systèmes clients disposent de ressources insuffisantes pour gérer le décodage multimédia local, laissez le paramètre défini sur **Refuser**.<br>Les données de redirection multimédia (MMR) sont envoyées sur le réseau sans cryptage basé sur une application et peuvent contenir des données sensibles, selon le contenu redirigé. Pour garantir que les données ne puissent pas être surveillées sur le réseau, utilisez MMR uniquement sur un réseau sécurisé. |
| USB Access (Accès USB) | Détermine si des postes de travail distants peuvent utiliser des périphériques USB connectés au système client.<br>La valeur par défaut est **Autoriser**. Pour empêcher l'utilisation de périphériques externes pour des raisons de sécurité, passez le paramètre sur **Refuser**. |
| Accélération matérielle PCoIP | Détermine l'activation de l'accélération matérielle du protocole d'affichage PCoIP et spécifie la priorité d'accélération affectée à la session utilisateur PCoIP.<br>Ce paramètre a un effet uniquement si un périphérique d'accélération matérielle PCoIP est présent sur l'ordinateur physique qui héberge le poste de travail distant.<br>La valeur par défaut est **Autoriser** avec une priorité **Moyenne**. |

## Utilisation de Stratégies de carte à puce

Vous pouvez utiliser Stratégies de carte à puce pour créer des stratégies qui contrôlent le comportement des fonctionnalités de redirection USB, d'impression virtuelle, de redirection du Presse-papiers, de redirection du lecteur client et de protocole d'affichage PCoIP sur des postes de travail distants spécifiques.

Avec Stratégies de carte à puce, vous pouvez créer des stratégies qui ne prennent effet que si certaines conditions sont respectées. Par exemple, vous pouvez configurer une stratégie qui désactive la fonctionnalité de redirection du lecteur client si un utilisateur se connecte à un poste de travail distant depuis l'extérieur du réseau d'entreprise.

## Configuration requise pour les Stratégies de carte à puce

Pour utiliser des Stratégies de carte à puce, votre environnement View doit satisfaire une certaine configuration requise.

- Vous devez installer Horizon Agent 7.0 ou version ultérieure et VMware User Environment Manager 9.0 ou version ultérieure sur les postes de travail distants que vous voulez gérer avec des Stratégies de carte à puce.
- Les utilisateurs doivent utiliser Horizon Client 4.0 ou version ultérieure pour se connecter à des postes de travail distants que vous gérez avec des Stratégies de carte à puce.

## Installation de User Environment Manager

Pour utiliser Stratégies de carte à puce afin de contrôler le comportement des fonctionnalités de poste de travail distant sur un poste de travail distant, vous devez installer User Environment Manager 9.0 ou version ultérieure sur le poste de travail distant.

Vous pouvez télécharger le programme d'installation de User Environment Manager sur la page de téléchargement de VMware. Vous devez installer le composant client VMware UEM FlexEngine sur chaque poste de travail distant que vous voulez gérer avec User Environment Manager. Vous pouvez installer le composant Console de gestion User Environment Manager sur les postes de travail que vous voulez pour gérer l'environnement User Environment Manager.

Pour un pool de clone lié, vous installez User Environment Manager sur la machine virtuelle parente que vous utilisez comme image de base pour les clones liés. Pour un pool de postes de travail RDS, vous installez User Environment Manager sur l'hôte RDS qui fournit les sessions de poste de travail RDS.

Pour voir des instructions sur la configuration système requise et sur l'installation complète de User Environment Manager, consultez le document *Guide de l'administrateur de User Environment Manager*.

## Configuration d' User Environment Manager

Vous devez configurer User Environment Manager avant de pouvoir l'utiliser pour créer des stratégies pour des fonctionnalités de poste de travail distant.

Pour configurer User Environment Manager, suivez les instructions de configuration dans le *Guide de l'administrateur de User Environment Manager*. Les étapes de configuration suivantes complètent les informations dans ce document.

- Lors de la configuration du composant client VMware UEM FlexEngine sur des postes de travail distants, créez des scripts d'ouverture et de fermeture de session FlexEngine. Utilisez le paramètre **`-HorizonViewMultiSession -r`** pour le script d'ouverture de session et le paramètre **`-HorizonViewMultiSession -s`** pour le script de fermeture de session.

  **Remarque** N'utilisez pas de scripts d'ouverture de session pour démarrer d'autres applications sur un poste de travail distant. Des scripts d'ouverture de session supplémentaires peuvent retarder l'ouverture de session du poste de travail distant de 10 minutes au maximum.

- Activez le paramètre de stratégie de groupe d'utilisateurs `Exécuter les scripts d'ouverture de session simultanément` sur les postes de travail distants. Ce paramètre se trouve dans le dossier `Configuration utilisateur\Stratégies\Modèles d'administration\Système\Scripts`.
- Activez le paramètre de stratégie de groupe d'ordinateurs `Toujours attendre le réseau lors du démarrage de l'ordinateur et de l'ouverture de session` sur les postes de travail distants. Ce paramètre se trouve dans le dossier `Configuration ordinateur\Stratégies\Modèles d'administration\Système\Ouverture de session`.

- Pour les postes de travail distants Windows 8.1, désactivez le paramètre de stratégie de groupe d'ordinateurs `Configurer le délai des scripts d'ouverture de session`. Ce paramètre se trouve dans le dossier `Configuration ordinateur\Stratégies\Modèles d'administration\Système\Stratégie de groupe`.
- Pour s'assurer que les paramètres de stratégie d'Horizon sont actualisés lorsque les utilisateurs se reconnectent à des sessions de poste de travail, utilisez la console de gestion User Environment Manager pour créer une tâche déclenchée. Définissez le déclencheur sur **Reconnecter la session**, définissez l'action sur **Actualiser l'environnement utilisateur** et sélectionnez **Stratégies d'Horizon** pour l'actualisation.

  **Remarque** Si vous créez la tâche déclenchée alors qu'un utilisateur est connecté au poste de travail distant, l'utilisateur doit se déconnecter du poste de travail pour que la tâche déclenchée prenne effet.

## Paramètres de stratégie Horizon

Vous contrôlez le comportement de fonctionnalités de poste de travail distant dans User Environment Manager en créant une stratégie Horizon.

Tableau 17-2 décrit les paramètres que vous pouvez sélectionner lorsque vous définissez une stratégie Horizon dans User Environment Manager.

**Tableau 17-2.** Paramètres de stratégie Horizon

| Paramètre | Description |
|---|---|
| redirection USB | Détermine si la redirection USB est activée sur le poste de travail distant. La fonctionnalité de redirection USB permet aux utilisateurs d'utiliser des périphériques USB connectés localement, tels que des mémoires Flash, des caméras et des imprimantes, à partir du poste de travail distant. |
| Impression | Détermine si l'impression virtuelle est activée sur le poste de travail distant. La fonctionnalité d'impression virtuelle permet aux utilisateurs d'imprimer vers une imprimante virtuelle ou USB qui est connectée à l'ordinateur client depuis le poste de travail distant. |
| Presse-papiers | Détermine le sens dans lequel la redirection du Presse-papiers est autorisée. Vous pouvez sélectionner l'une des valeurs suivantes :<br>■ **Désactiver**. La redirection du presse-papiers est désactivée dans les deux sens.<br>■ **Autoriser tout**. La redirection du presse-papiers est activée. Les utilisateurs peuvent copier et coller depuis le système client vers le poste de travail distant, et vice versa.<br>■ **Autoriser la copie depuis le client vers l'agent**. Les utilisateurs peuvent copier et coller uniquement depuis le système client vers le poste de travail distant.<br>■ **Autoriser la copie depuis l'agent vers le client**. Les utilisateurs peuvent copier et coller uniquement depuis le poste de travail distant vers le système client. |
| Redirection de lecteur client | Détermine si la redirection du lecteur client est activée sur le poste de travail distant et si des lecteurs et des dossiers partagés sont accessibles en écriture. Vous pouvez sélectionner l'une des valeurs suivantes :<br>■ **Désactiver**. La redirection du lecteur client est désactivée sur le poste de travail distant.<br>■ **Autoriser tout**. Les lecteurs clients et les dossiers sont partagés avec le poste de travail distant et sont accessibles en lecture et en écriture.<br>■ **Lecture seule**. Les lecteurs clients et les dossiers sont partagés avec le poste de travail distant et sont accessibles en lecture, mais pas en écriture.<br>Si vous ne configurez pas ce paramètre, l'accessibilité en écriture des lecteurs et des dossiers partagés dépend des paramètres de registre locaux. Pour plus d'informations, reportez-vous à la section « Utiliser des paramètres de registre pour configurer la redirection du lecteur client », page 246. |
| Profil PCoIP | Configure un profil de bande passante pour des sessions PCoIP sur le poste de travail distant. Vous pouvez sélectionner un profil de bande passante prédéfini, par exemple **LAN (10 Mbit/s ou plus)**. La sélection d'un profil de bande passante prédéfini empêche l'agent de tenter de transmettre à un taux supérieur à la capacité de liaison. Si vous sélectionnez le profil par défaut, la bande passante maximale est de 90 000 kilobits par seconde.<br>Pour plus d'informations, reportez-vous à la section « Référence de profil PCoIP », page 302. |

En général, les paramètres de stratégie Horizon que vous configurez pour les fonctionnalités de poste de travail distant dans User Environment Manager remplacent les paramètres de clé de registre et de stratégie de groupe équivalents.

## Référence de profil PCoIP

Avec des stratégies de carte à puce, vous pouvez utiliser le paramètre de stratégie de profil PCoIP pour configurer un profil de bande passante pour des sessions PCoIP sur des postes de travail distants.

Tableau 17-3 décrit chaque profil PCoIP.

**Tableau 17-3.** Profils PCoIP

| Profil PCoIP | Bande passante de session max. (Kbit/s) | Bande passante de session min. (Kbit/s) | Activer BTL | Qualité d'image initiale max. | Qualité d'image min. | Image/s max. | Bande passante audio max. (Kbit/s) | Performance de qualité d'image |
|---|---|---|---|---|---|---|---|---|
| Réseau LAN haute vitesse (20 Mbit/s) | 900 000 | 100 | Oui | 100 | 50 | 60 | 1 600 | 50 |
| Réseau LAN (10 Mbit/s ou plus) | 900 000 | 100 | Oui | 90 | 50 | 30 | 1 600 | 50 |
| Réseau WAN dédié (5 Mbit/s, par défaut) | 900 000 | 100 | Non | 80 | 40 | 30 | 500 | 50 |
| Réseau WAN à large bande (2 Mbit/s) | 5 000 | 100 | Non | 70 | 40 | 20 | 500 | 50 |
| Réseau WAN basse vitesse (1 Mbit/s) | 2 000 | 100 | Non | 70 | 30 | 15 | 200 | 25 |
| Connexion très basse vitesse (jusqu'à 500 kbit/s) | 1 000 | 100 | Non | 70 | 30 | 5 | 90 | 0 |

## Ajout de conditions à des définitions de stratégie Horizon

Lorsque vous définissez une stratégie Horizon dans User Environment Manager, vous pouvez ajouter des conditions qui doivent être satisfaites pour que la stratégie prenne effet. Par exemple, vous pouvez ajouter une condition qui désactive la fonctionnalité de redirection du lecteur client uniquement si un utilisateur se connecte au poste de travail distant depuis l'extérieur du réseau d'entreprise.

Vous pouvez ajouter plusieurs conditions pour la même fonctionnalité de poste de travail distant. Par exemple, vous pouvez ajouter une condition qui active l'impression locale si un utilisateur est membre du groupe RH et une autre condition qui active l'impression locale si le poste de travail distant se trouve dans le pool Win7.

Pour plus d'informations sur l'ajout et la modification des conditions dans la console de gestion User Environment Manager, consultez le *Guide de l'administrateur de User Environment Manager*.

### Utilisation de la condition de propriété d'Horizon Client

Lorsqu'un utilisateur se connecte ou se reconnecte à un poste de travail distant, Horizon Client recueille des informations sur l'ordinateur client et le Serveur de connexion envoie ces informations au poste de travail distant. Vous pouvez ajouter la condition de propriété d'Horizon Client à une définition de stratégie Horizon pour contrôler quand la stratégie prend effet en fonction des informations que le poste de travail distant reçoit.

**Remarque** La condition de propriété d'Horizon Client ne prend effet que si un utilisateur lance le poste de travail distant avec le protocole d'affichage PCoIP ou VMware Blast. Si un utilisateur lance le poste de travail distant avec le protocole d'affichage RDP, la condition de propriété d'Horizon Client n'a aucun effet.

Tableau 17-4 décrit les propriétés prédéfinies que vous pouvez sélectionner dans le menu déroulant **Propriétés** lorsque vous utilisez la condition de propriété d'Horizon Client. Chaque propriété prédéfinie correspond à une clé de registre `ViewClient_`.

**Tableau 17-4.** Propriétés prédéfinies pour la condition de propriété d'Horizon Client

| Propriété | Clé de registre correspondante | Description |
|---|---|---|
| **Emplacement du client** | `ViewClient_Broker_GatewayLocation` | Spécifie l'emplacement du système client de l'utilisateur. Les valeurs valides sont les suivantes :<br>■ Interne : la stratégie prend effet uniquement si un utilisateur se connecte au poste de travail distant à l'intérieur du réseau d'entreprise<br>■ Externe : la stratégie prend effet uniquement si un utilisateur se connecte au poste de travail distant à l'extérieur du réseau d'entreprise<br>Pour plus d'informations sur la configuration de l'emplacement de passerelle d'un hôte de Serveur de connexion ou de serveur de sécurité, consultez le document *Administration de View*.<br>Pour plus d'informations sur la configuration de l'emplacement de passerelle d'un dispositif Access Point, consultez le document *Déploiement et configuration d'Access Point*. |
| **Balise(s) de démarrage** | `ViewClient_Launch_Matched_Tags` | Spécifie une ou plusieurs balises. Séparez les balises avec une virgule ou un point-virgule. La stratégie prend effet uniquement si la balise qui activait le démarrage de poste de travail distant correspond à l'une des balises spécifiées.<br>Pour plus d'informations sur l'attribution de balises à des instances du Serveur de connexion et à des pools de postes de travail, reportez-vous à la section « Restriction de l'accès aux postes de travail distants », page 189. |
| **Nom de pool** | `ViewClient_Launch_ID` | Spécifie un ID de pool de postes de travail. La stratégie prend effet uniquement si l'ID du pool de postes de travail que l'utilisateur a choisi lors du démarrage du poste de travail distant correspond à l'ID du pool de postes de travail spécifié. Par exemple, si l'utilisateur a choisi le pool Win7 et que cette propriété est définie sur Win7, la stratégie prend effet.<br>**Remarque** Vous ne pouvez pas utiliser cette propriété pour spécifier un pool d'applications. |

Le menu déroulant **Propriétés** est également une zone de texte et vous pouvez entrer manuellement une clé de registre `ViewClient_` dans la zone de texte. N'incluez pas le préfixe `ViewClient_` lorsque vous entrez la clé de registre. Par exemple, pour spécifier `ViewClient_Broker_URL`, entrez `Broker_URL`.

Vous pouvez utiliser l'Éditeur du Registre Windows (`regedit.exe`) sur le poste de travail distant pour voir les clés de registre `ViewClient_`. Horizon Client écrit des informations d'ordinateur client dans le chemin d'accès `HKEY_CURRENT_USER\Volatile Environment` du registre système sur les postes de travail distants qui sont déployés sur des machines mono-utilisateur. Pour les postes de travail distants déployés dans des sessions RDS, Horizon Client écrit les informations de l'ordinateur client dans le chemin d'accès `HKEY_CURRENT_USER\Volatile Environment\`*x* du registre système, où *x* est l'ID de la session sur l'hôte RDS.

### Utilisation des autres conditions

La console de gestion User Environment Manager fournit de nombreuses conditions. Les conditions suivantes peuvent être particulièrement utiles lors de la création de stratégies pour des fonctionnalités de poste de travail distant.

**Membre de groupe** Vous pouvez utiliser cette condition pour configurer la stratégie afin qu'elle ne prenne effet que si un utilisateur est membre d'un groupe spécifique.

**Protocole d'affichage distant** Vous pouvez utiliser cette condition pour configurer la stratégie afin qu'elle ne prenne effet que si l'utilisateur choisit un protocole d'affichage particulier. Les paramètres de condition incluent RDP, PCoIP et Blast.

**Adresse IP** Vous pouvez utiliser cette condition pour configurer la stratégie afin qu'elle ne prenne effet que si un utilisateur se connecte à l'intérieur ou à l'extérieur du réseau d'entreprise. Utilisez les paramètres de condition pour spécifier une plage d'adresses IP internes ou une plage d'adresses IP externes.

---

**Remarque** Vous pouvez également utiliser la propriété **Emplacement du client** dans la condition de propriété d'Horizon Client.

---

Pour voir une description de toutes les conditions disponibles, consultez le document *Guide de l'administrateur de User Environment Manager*.

## Créer une stratégie Horizon dans User Environment Manager

Vous utilisez la console de gestion User Environment Manager pour créer une stratégie Horizon dans User Environment Manager. Lorsque vous définissez une stratégie Horizon, vous pouvez ajouter des conditions qui doivent être satisfaites pour que la stratégie prenne effet.

#### Prérequis

- Installez et configurez User Environment Manager. Reportez-vous aux sections « Installation de User Environment Manager », page 300 et « Configuration d'User Environment Manager », page 300.
- Familiarisez-vous avec les paramètres de stratégie Horizon. Reportez-vous à la section « Paramètres de stratégie Horizon », page 301.
- Familiarisez-vous avec les conditions que vous pouvez ajouter à des définitions de stratégie Horizon. Reportez-vous à la section « Ajout de conditions à des définitions de stratégie Horizon », page 302.

Pour obtenir des informations complètes sur l'utilisation de la console de gestion User Environment Manager, consultez le document *Guide de l'administrateur de User Environment Manager*.

#### Procédure

1. Dans la console de gestion User Environment Manager, sélectionnez l'onglet **Environnement utilisateur** et cliquez sur **Stratégies Horizon** dans l'arborescence.

   Les définitions de stratégie Horizon existantes, le cas échéant, apparaissent dans le volet Stratégies Horizon.

2. Cliquez avec le bouton droit sur **Stratégies Horizon** et sélectionnez **Créer une définition de stratégie Horizon** pour créer une stratégie.

   La boîte de dialogue Stratégie Horizon s'affiche.

3 Sélectionnez l'onglet **Paramètres** et définissez les paramètres de stratégie.

   a Dans la section Paramètres généraux, entrez un nom pour la stratégie dans la zone de texte **Nom**.

      Par exemple, si la stratégie affecte la fonctionnalité de redirection du lecteur client, vous pouvez nommer la stratégie CDR.

   b Dans la section Paramètres de stratégie Horizon, sélectionnez les fonctionnalités et les paramètres de poste de travail distant à inclure dans la stratégie.

      Vous pouvez sélectionner plusieurs fonctionnalités de poste de travail distant.

4 (Facultatif) Pour ajouter une condition à la stratégie, sélectionnez l'onglet **Conditions**, cliquez sur **Ajouter** et sélectionnez une condition.

   Vous pouvez ajouter plusieurs conditions à une définition de stratégie.

5 Cliquez sur **Enregistrer** pour enregistrer la stratégie.

User Environment Manager traite la stratégie Horizon chaque fois qu'un utilisateur se connecte ou se reconnecte au poste de travail distant.

User Environment Manager traite plusieurs stratégies dans l'ordre alphabétique en fonction du nom de la stratégie. Les stratégies Horizon apparaissent dans l'ordre alphabétique dans le volet Stratégies Horizon. En cas de conflit de stratégies, la dernière stratégie traitée est prioritaire. Par exemple, s'il existe une stratégie nommée Sophie qui active la redirection USB pour l'utilisatrice Sophie et une autre stratégie nommée Pool qui désactive la redirection USB pour le pool de postes de travail Win7, la fonctionnalité de redirection USB est activée lorsque Sophie se connecte à un poste de travail distant dans le pool de postes de travail Win7.

# Utilisation de stratégies de groupe Active Directory

Vous pouvez utiliser une stratégie de groupe Microsoft Windows pour optimiser et sécuriser des postes de travail distants, contrôler le comportement de composants View et configurer l'impression basée sur l'emplacement.

La stratégie de groupe est une fonction des systèmes d'exploitation Microsoft Windows qui fournit une gestion et une configuration centralisées des ordinateurs et des utilisateurs à distance dans un environnement Active Directory.

Les paramètres de stratégie de groupe sont contenus dans des entités nommées objets de stratégie de groupe (GPO). Des GPO sont associés à des objets Active Directory. Vous pouvez appliquer des GPO à des composants View au niveau d'un domaine pour contrôler diverses zones de l'environnement View. Une fois appliqués, les paramètres de GPO sont stockés dans le Registre Windows local du composant spécifié.

Vous utilisez l'Éditeur d'objets de stratégie de groupe de Microsoft Windows pour gérer des paramètres de stratégie de groupe. L'Éditeur d'objets de stratégie de groupe est un composant logiciel enfichable de Microsoft Management Console (MMC). La MMC fait partie de la Console de gestion des stratégies de groupe (GPMC). Pour plus d'informations sur l'installation et l'utilisation de la GPMC, consultez le site Web Microsoft TechNet.

## Création d'une UO pour des postes de travail distants

Vous devez créer dans Active Directory une unité d'organisation (UO) qui soit propre à vos postes de travail distants.

Pour empêcher l'application des paramètres de stratégie de groupe sur d'autres serveurs ou stations de travail Windows dans le même domaine que vos postes de travail distants, créez un objet de stratégie de groupe (GPO) pour vos stratégies de groupe View et liez-le à l'UO qui contient vos postes de travail distants.

Pour plus d'informations sur la création d'UO et de GPO, consultez la documentation à propos de Microsoft Active Directory sur le site Web Microsoft TechNet.

### Activation du traitement en boucle pour des postes de travail distants

Par défaut, les paramètres de stratégie d'un utilisateur viennent de l'ensemble de GPO appliqués à l'objet utilisateur dans Active Directory. Toutefois, dans l'environnement View, des GPO doivent s'appliquer à des utilisateurs en fonction de l'ordinateur sur lequel ils ouvrent une session.

Lorsque vous activez le traitement en boucle, un ensemble cohérent de règles s'applique à tous les utilisateurs qui ouvrent une session sur un ordinateur particulier, peu importe l'emplacement de ces règles dans Active Directory.

Pour plus d'informations sur l'activation du traitement en boucle, consultez la documentation à propos de Microsoft Active Directory.

---

**Remarque** Le traitement en boucle est seulement une des approches existantes pour gérer les GPO dans View. Vous devrez peut-être implémenter une approche différente.

---

## Utilisation des fichiers de modèle d'administration de stratégie de groupe View

View fournit plusieurs fichiers de modèle d'administration (ADM et ADMX) de stratégie de groupe propres à un composant. Vous pouvez optimiser et sécuriser des applications et des postes de travail distants en ajoutant les paramètres de stratégie de ces fichiers de modèle ADM et ADMX à un nouveau GPO ou à un GPO existant dans Active Directory.

Tous les fichiers ADM et ADMX qui fournissent des paramètres de stratégie de groupe pour View sont disponibles dans un fichier groupé `.zip` nommé `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`, où *x.x.x* est la version et *yyyyyyy* le numéro de build. Vous pouvez télécharger le fichier sur le site de téléchargement de VMware à l'adresse https://my.vmware.com/web/vmware/downloads. Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut le fichier groupé `.zip`.

Les fichiers de modèle ADM et ADMX de View contiennent des stratégies de groupe Configuration d'ordinateur et Configuration d'utilisateur.

- Les stratégies Configuration d'ordinateur définissent des stratégies qui s'appliquent à tous les postes de travail distants, quelle que soit la personne qui se connecte au poste de travail.
- Les stratégies Configuration d'utilisateur définissent des stratégies qui s'appliquent à tous les utilisateurs, quel que soit l'application ou le poste de travail distant auquel ils se connectent. Les stratégies Configuration d'utilisateur remplacent les stratégies Configuration d'ordinateur équivalentes.

Microsoft Windows applique les stratégies au démarrage du poste de travail et lorsque les utilisateurs se connectent.

# Fichiers de modèle d'administration ADM et ADMX de View

Les fichiers de modèle d'administration ADM et ADMX de View fournissent des paramètres de stratégie de groupe qui vous permettent de contrôler et d'optimiser les composants de View.

**Tableau 17-5.** Afficher les fichiers de modèle d'administration ADM et ADMX

| Nom du modèle | Fichier de modèle | Description |
|---|---|---|
| Configuration d'Horizon Agent | `vdm_agent.adm` | Contient des paramètres de stratégie liés aux composants d'authentification et d'environnement d'Horizon Agent.<br>Reportez-vous à la section « Paramètres du modèle d'administration pour la configuration d'Horizon Agent », page 308. |
| Configuration d'Horizon Client | `vdm_client.adm` | Contient des paramètres de stratégie liés à Horizon Client pour Windows.<br>Les clients qui se connectent de l'extérieur du domaine d'hôte du Serveur de connexion View ne sont pas affectés par les stratégies appliquées à Horizon Client.<br>Consultez le document *Utilisation de VMware Horizon Client pour Windows*. |
| Redirection URL de VMware Horizon | `urlRedirection-enUS.adm` | Contient des paramètres de stratégie liés à la fonctionnalité de redirection de contenu URL. Si vous ajoutez ce modèle à un GPO pour un pool de postes de travail distants ou un pool d'applications, certains liens URL sur lesquels vous cliquez à l'intérieur des applications ou des postes de travail distants peuvent être redirigés vers un client Windows et ouverts dans un navigateur côté client.<br>Si vous ajoutez ce modèle à un GPO côté client, lorsqu'un utilisateur clique sur certains liens URL dans un système client Windows, l'URL peut être ouverte dans une application ou un poste de travail distant.<br>Reportez-vous à la section « Paramètres du modèle de redirection de contenu URL VMware Horizon », page 210 et consultez le document *Utilisation de VMware Horizon Client pour Windows*. |
| View Server Configuration | `vdm_server.adm` | Contient des paramètres de stratégie liés au Serveur de connexion View.<br>Consultez le document *Administration de View*. |
| configuration commune de View | `vdm_common.adm` | Contient des paramètres de stratégie communs à tous les composants View.<br>Consultez le document *Administration de View*. |
| Afficher les variables de session PCoIP | `pcoip.adm` | Contient des paramètres de stratégie liés au protocole d'affichage PCoIP.<br>Reportez-vous à la section « Paramètres de stratégie PCoIP », page 314. |
| Variables de la session de client PCoIP de View | `pcoip.client.adm` | Contient des paramètres de stratégie liés au protocole d'affichage PCoIP qui affectent Horizon Client pour Windows.<br>Consultez le document *Utilisation de VMware Horizon Client pour Windows*. |

**Tableau 17-5.** Afficher les fichiers de modèle d'administration ADM et ADMX (suite)

| Nom du modèle | Fichier de modèle | Description |
|---|---|---|
| Configuration de View Persona Management | `ViewPM.adm` | Contient des paramètres de stratégie liés à View Persona Management.<br>Reportez-vous à la section « Paramètres de stratégie de groupe View Persona Management », page 370. |
| Afficher les services Bureau à distance | `vmware_rdsh.admx`<br>`vmware_rdsh_server.admx` | Contient des paramètres de stratégie liés aux services Bureau à distance.<br>Reportez-vous à la section « Utilisation de stratégies de groupe des services Bureau à distance », page 329. |
| Configuration de l'Audio/Vidéo en temps réel | `vdm_agent_rtav.adm` | Contient des paramètres de stratégie liés à des webcams qui sont utilisées avec la fonctionnalité d'Audio/Vidéo en temps réel.<br>Reportez-vous à la section « Paramètres de stratégie de groupe de l'Audio/Vidéo en temps réel », page 227. |
| Redirection de scanner | `vdm_agent_scanner.adm` | Contient des paramètres de stratégie liés à des périphériques d'analyse qui sont redirigés pour une utilisation dans des applications et des postes de travail distants.<br>Reportez-vous à la section « Paramètres de stratégie de groupe de redirection de scanner », page 232. |
| Redirection de port série | `vdm_agent_serialport.adm` | Contient des paramètres de stratégie liés à des ports série (COM) qui sont redirigés pour une utilisation dans des postes de travail VDI distants.<br>Reportez-vous à la section « Paramètres de stratégie de groupe de redirection de port série », page 239. |

# Paramètres du modèle d'administration pour la configuration d' Horizon Agent

Le fichier de modèle d'administration pour la configuration d'Horizon Agent (`vdm_agent.adm`) contient des paramètres de stratégie liés aux composants d'authentification et d'environnement d'Horizon Agent.

Ce fichier ADM est disponible dans un fichier groupé `.zip` nommé `VMware-Horizon-Extras-Bundle-`*`x.x.x-yyyyyyy`*`.zip`, que vous pouvez télécharger sur le site de téléchargement de VMware à l'adresse https://my.vmware.com/web/vmware/downloads. Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut le fichier groupé `.zip`.

Le tableau suivant décrit les paramètres de stratégie du fichier de modèle d'administration de configuration d'Horizon Agent qui ne sont pas utilisés avec des périphériques USB. Le modèle contient les paramètres de Configuration d'ordinateur et de Configuration d'utilisateur. Le paramètre de Configuration d'utilisateur remplace le paramètre de Configuration d'ordinateur équivalent.

**Tableau 17-6.** Paramètres du modèle pour la configuration d' Horizon Agent

| Paramètre | Ordinateur | Utilisateur | Propriétés |
|---|---|---|---|
| `AllowDirectRDP` | X | | Détermine si les clients qui ne sont pas des périphériques Horizon Client peuvent se connecter directement à des postes de travail distants avec RDP. Lorsque ce paramètre est désactivé, l'agent autorise uniquement les connexions gérées par View via Horizon Client.<br>Lorsque vous vous connectez à un poste de travail distant à partir d'Horizon Client pour Mac OS X, ne désactivez pas le paramètre `AllowDirectRDP`. Si ce paramètre est désactivé, la connexion échoue avec une erreur `Access is denied (Accès refusé)`.<br>Par défaut, lorsqu'un utilisateur a ouvert une session de poste de travail View, vous pouvez utiliser RDP pour vous connecter à la machine virtuelle à l'extérieur de View. La connexion RDP met fin à la session du poste de travail View et les données et paramètres non enregistrés de l'utilisateur View risquent d'être perdus. L'utilisateur View ne peut pas se connecter au poste de travail tant que la connexion RDP externe est fermée. Pour éviter cette situation, désactivez le paramètre `AllowDirectRDP`.<br>**Important** Pour que View fonctionne correctement, les services Bureau à distance doivent s'exécuter sur le système d'exploitation invité de chaque poste de travail. Vous pouvez utiliser ce paramètre pour empêcher les utilisateurs de faire des connexions RDP directes sur leurs postes de travail.<br>Ce paramètre est activé par défaut. |
| `AllowSingleSignon` | X | | Détermine si l'authentification unique (Single Sign-On, SSO) est utilisée pour connecter les utilisateurs aux postes de travail et aux applications. Lorsque ce paramètre est activé, les utilisateurs doivent entrer leurs informations d'identification une seule fois, lorsqu'ils se connectent au serveur. Lorsqu'il est désactivé, les utilisateurs doivent s'authentifier de nouveau lorsque la connexion à distance est effectuée.<br>Ce paramètre est activé par défaut. |
| `CommandsToRunOnConnect` | X | | Spécifie une liste de commandes ou de scripts de commande à exécuter lorsqu'une session est connectée pour la première fois.<br>Pour plus d'informations, reportez-vous à « Exécution de commandes sur des postes de travail View », page 314. |
| `CommandsToRunOnDisconnect` | X | | Spécifie la liste des commandes ou des scripts de commande à exécuter lorsqu'une session est déconnectée.<br>Pour plus d'informations, reportez-vous à « Exécution de commandes sur des postes de travail View », page 314. |
| `CommandsToRunOnReconnect` | X | | Spécifie une liste de commandes ou de scripts de commande à exécuter lorsqu'une session est reconnectée après une déconnexion.<br>Pour plus d'informations, reportez-vous à « Exécution de commandes sur des postes de travail View », page 314. |

**Tableau 17-6.** Paramètres du modèle pour la configuration d' Horizon Agent (suite)

| Paramètre | Ordinateur | Utilisateur | Propriétés |
|---|---|---|---|
| `ConnectionTicketTimeout` | X | | Spécifie la durée en secondes pendant laquelle le ticket de connexion View est valide.<br>Les périphériques Horizon Client utilisent un ticket de connexion pour la vérification et l'authentification unique lorsqu'ils se connectent à l'agent. Pour des raisons de sécurité, un ticket de connexion est valide pendant une durée limitée. Lorsqu'un utilisateur se connecte à un poste de travail distant, l'authentification doit avoir lieu pendant le délai d'expiration du ticket de connexion sinon la session expire. Si ce paramètre n'est pas configuré, le délai d'expiration par défaut est de 900 secondes. |
| `CredentialFilterExceptions` | X | | 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. |
| `Disable Time Zone Synchronization` | X | X | Détermine si le fuseau horaire du poste de travail View est synchronisé avec celui du client connecté. Un paramètre activé ne s'applique que si le paramètre `Désactiver le transfert de fuseau horaire` de la stratégie de configuration d'Horizon Client n'est pas définie sur désactivé.<br>Ce paramètre est désactivé par défaut. |
| `Enable multi-media acceleration` | X | | Détermine si la redirection multimédia (MMR) est activée sur le poste de travail View.<br>MMR est un filtre de Windows Media Foundation qui permet de transférer des données multimédia de codecs spécifiques sur le système distant au client directement via un socket TCP. Les données sont ensuite décodées directement sur le client, lorsqu'elles sont lues. Vous pouvez désactiver MMR si le client ne dispose pas de ressources suffisantes pour gérer le décodage multimédia local.<br>Ce paramètre est activé par défaut. |
| `Enable system tray redirection for Hosted Apps` | X | | Détermine si la redirection de la barre d'état système est activée pendant qu'un utilisateur exécute des applications distantes.<br>Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Unity Touch et applications hébergées** dans l'Éditeur de gestion de stratégie de groupe.<br>Ce paramètre est activé par défaut. |
| `Enable Unity Touch` | X | | Détermine si la fonctionnalité Unity Touch est activée dans le poste de travail View. Unity Touch prend en charge la livraison d'applications distantes dans View et permet aux utilisateurs d'appareils mobiles d'accéder aux applications dans la barre latérale Unity Touch.<br>Ce paramètre se trouve dans le dossier **Configuration de VMware View Agent > Unity Touch et applications hébergées** dans l'Éditeur de gestion de stratégie de groupe.<br>Ce paramètre est activé par défaut. |

**Tableau 17-6.** Paramètres du modèle pour la configuration d' Horizon Agent (suite)

| Paramètre | Ordinateur | Utilisateur | Propriétés |
|---|---|---|---|
| `ShowDiskActivityIcon` | X | | Ce paramètre n'est pas pris en charge dans cette version. |
| `Toggle Display Settings Control` | X | | Détermine si l'onglet **Settings (Paramètres)** du panneau de configuration **Display (Affichage)** est désactivé lorsqu'une session client utilise le protocole d'affichage PCoIP.<br>Ce paramètre est activé par défaut. |

**Remarque** Le paramètre `Connect using DNS Name` a été supprimé dans Horizon 6 version 6.1. Vous pouvez définir l'attribut LDAP de View, **pae-PreferDNS**, pour demander au Serveur de connexion View de donner la préférence aux noms DNS lors de l'envoi des adresses de machines de postes de travail et d'hôtes RDS à des clients et des passerelles. Reportez-vous à « Donner la préférence aux noms DNS lorsque le Serveur de connexion View renvoie des informations d'adresse » dans le document *Installation de View*.

## Paramètres USB d' Horizon Agent

Reportez-vous à la section « Paramètres USB du modèle d'administration de configuration d'Horizon Agent », page 265.

## Envoi d'informations sur le système client à des postes de travail View

Lorsqu'un utilisateur se connecte ou se reconnecte à un poste de travail View, Horizon Client recueille des informations sur le système client et le Serveur de connexion View envoie ces informations au poste de travail distant.

Horizon Agent écrit les informations d'ordinateur client dans le chemin d'accès `HKCU\Volatile Environment` du registre système sur les postes de travail distants qui sont déployés sur des machines mono-utilisateur.

Pour les postes de travail distants déployés dans des sessions RDS, Horizon Agent écrit les informations de l'ordinateur client dans le chemin d'accès `HKCU\Volatile Environment\`*x* du registre système, où *x* est l'ID de la session sur l'hôte RDS.

Vous pouvez ajouter des commandes aux paramètres de stratégie de groupe `CommandsToRunOnConnect`, `CommandsToRunOnReconnect` et `CommandsToRunOnDisconnect` d'Horizon Agent pour exécuter des commandes ou des scripts de commande qui lisent ces informations dans le registre système lorsque des utilisateurs se connectent et se reconnectent à des postes de travail. Pour plus d'informations, reportez-vous à « Exécution de commandes sur des postes de travail View », page 314.

Tableau 17-7 décrit les clés de Registre qui contiennent des informations sur le système client et répertorie les types de systèmes client qui les prennent en charge.

**Tableau 17-7.** Informations sur le système client

| Clé de Registre | Description | Postes de travail pris en charge | Systèmes clients pris en charge |
|---|---|---|---|
| `ViewClient_IP_Address` | Adresse IP du système client. | VDI (machine mono-utilisateur)<br>RDS | Windows, Linux, Mac, Android, iOS, Metro |
| `ViewClient_MAC_Address` | Adresse MAC du système client. | VDI (machine mono-utilisateur)<br>RDS | Windows, Linux, Mac, Android |
| `ViewClient_Machine_Name` | Nom de machine du système client. | VDI (machine mono-utilisateur)<br>RDS | Windows, Linux, Mac, Android, iOS, Metro |

**Tableau 17-7.** Informations sur le système client (suite)

| Clé de Registre | Description | Postes de travail pris en charge | Systèmes clients pris en charge |
|---|---|---|---|
| `ViewClient_Machine_Domain` | Domaine du système client. | VDI (machine mono-utilisateur)<br>RDS | Windows, Metro |
| `ViewClient_LoggedOn_Username` | Nom d'utilisateur utilisé pour se connecter au système client. | VDI (machine mono-utilisateur)<br>RDS | Windows, Linux, Mac |
| `ViewClient_LoggedOn_Domainname` | Nom de domaine utilisé pour se connecter au système client. | VDI (machine mono-utilisateur)<br>RDS | Windows, Metro<br>Pour les clients Linux et Mac, consultez `ViewClient_Machine_Domain.ViewClient_LoggedOn_Domainname` n'est pas donné par le client Linux ou Mac, car les comptes Linux et Mac ne sont pas liés à des domaines Windows. |
| `ViewClient_Type` | Nom du client léger ou type de système d'exploitation du système client. | VDI (machine mono-utilisateur)<br>RDS | Windows, Linux, Mac, Android, iOS, Metro |
| `ViewClient_Broker_DNS_Name` | Nom DNS de l'instance du Serveur de connexion View. | VDI (machine mono-utilisateur)<br>RDS | La valeur est envoyée directement par le Serveur de connexion View, elle n'est pas recueillie par Horizon Client. |
| `ViewClient_Broker_URL` | URL de l'instance du Serveur de connexion View. | VDI (machine mono-utilisateur)<br>RDS | La valeur est envoyée directement par le Serveur de connexion View, elle n'est pas recueillie par Horizon Client. |
| `ViewClient_Broker_Tunneled` | État de la connexion tunnel du Serveur de connexion View qui peut être `true` (activé) ou `false` (désactivé). | VDI (machine mono-utilisateur)<br>RDS | La valeur est envoyée directement par le Serveur de connexion View, elle n'est pas recueillie par Horizon Client. |
| `ViewClient_Broker_Tunnel_URL` | URL de la connexion tunnel du Serveur de connexion View, si la connexion tunnel est activée. | VDI (machine mono-utilisateur)<br>RDS | La valeur est envoyée directement par le Serveur de connexion View, elle n'est pas recueillie par Horizon Client. |
| `ViewClient_Broker_Remote_IP_Address` | Adresse IP du système client qui est vue par l'instance de Serveur de connexion View. | VDI (machine mono-utilisateur)<br>RDS | La valeur est envoyée directement par le Serveur de connexion View, elle n'est pas recueillie par Horizon Client. |
| `ViewClient_TZID` | ID du fuseau horaire Olson.<br>Pour désactiver la synchronisation du fuseau horaire, activez le paramètre de stratégie de groupe `Disable Time Zone Synchronization` d'Horizon Agent. | VDI (machine mono-utilisateur)<br>RDS | Windows, Linux, Mac, Android, iOS |

**Tableau 17-7.** Informations sur le système client (suite)

| Clé de Registre | Description | Postes de travail pris en charge | Systèmes clients pris en charge |
|---|---|---|---|
| `ViewClient_Windows_Timezone` | Heure GMT standard.<br>Pour désactiver la synchronisation du fuseau horaire, activez le paramètre de stratégie de groupe `Disable Time Zone Synchronization` d'Horizon Agent. | VDI (machine mono-utilisateur)<br>RDS | Windows, Metro |
| `ViewClient_Broker_DomainName` | Nom de domaine utilisé pour s'authentifier auprès du Serveur de connexion View. | VDI (machine mono-utilisateur)<br>RDS | La valeur est envoyée directement par le Serveur de connexion View, elle n'est pas recueillie par Horizon Client. |
| `ViewClient_Broker_UserName` | Nom d'utilisateur utilisé pour s'authentifier auprès du Serveur de connexion View. | VDI (machine mono-utilisateur)<br>RDS | La valeur est envoyée directement par le Serveur de connexion View, elle n'est pas recueillie par Horizon Client. |
| `ViewClient_Client_ID` | Spécifie l'`Unique Client HardwareId` utilisé comme lien vers la clé de licence. | VDI (machine mono-utilisateur)<br>RDS | Windows, Linux, Mac, Android, iOS, Metro |
| `ViewClient_Displays.Number` | Spécifie le nombre de moniteurs utilisés actuellement par le client. | VDI (machine mono-utilisateur)<br>RDS | Windows, Linux, Mac, Android, iOS, Metro |
| `ViewClient_Displays.Topology` | Spécifie la disposition, la résolution et les dimensions d'affichage du client. | VDI (machine mono-utilisateur)<br>RDS | Windows, Linux, Mac, Android, iOS, Metro |
| `ViewClient_Keyboard.Type` | Spécifie le type de clavier utilisé actuellement par le client. Par exemple : japonais, coréen. | VDI (machine mono-utilisateur)<br>RDS | Windows |
| `ViewClient_Launch_SessionType` | Spécifie le type de session. Il peut s'agir d'un poste de travail ou d'une application. | VDI (machine mono-utilisateur)<br>RDS | La valeur est envoyée directement par le Serveur de connexion View, elle n'est pas recueillie par Horizon Client. |
| `ViewClient_Mouse.Identifier` | Spécifie le type de souris. | VDI (machine mono-utilisateur)<br>RDS | Windows |
| `ViewClient_Mouse.NumButtons` | Spécifie le nombre de boutons pris en charge par la souris. | VDI (machine mono-utilisateur)<br>RDS | Windows |
| `ViewClient_Mouse.SampleRate` | Spécifie le taux, en rapports par seconde, auquel l'entrée d'une souris PS/2 est échantillonnée. | VDI (machine mono-utilisateur)<br>RDS | Windows |
| `ViewClient_Protocol` | Spécifie le protocole en cours d'utilisation. | VDI (machine mono-utilisateur)<br>RDS | Windows, Linux, Mac, Android, iOS, Metro |

**Tableau 17-7.** Informations sur le système client (suite)

| Clé de Registre | Description | Postes de travail pris en charge | Systèmes clients pris en charge |
|---|---|---|---|
| `ViewClient_Language` | Spécifie la langue du système d'exploitation. | VDI (machine mono-utilisateur)<br>RDS | Windows, Linux, Mac, Android, iOS, Metro |
| `ViewClient_Launch_ID` | Spécifie l'ID unique du pool de postes de travail. | VDI (machine mono-utilisateur) | Windows, Linux, Mac, Android, iOS, Metro |

**Remarque** Les définitions de `ViewClient_LoggedOn_Username` et de `ViewClient_LoggedOn_Domainname` dans Tableau 17-7 s'appliquent à Horizon Client 2.2 pour Windows ou version ultérieure.

Pour Horizon Client 5.4 pour Windows ou version antérieure, `ViewClient_LoggedOn_Username` envoie le nom d'utilisateur entré dans Horizon Client, et `ViewClient_LoggedOn_Domainname` envoie le nom de domaine entré dans Horizon Client.

Horizon Client 2.2 pour Windows est une version postérieure à Horizon Client 5.4 pour Windows. À partir d'Horizon Client 2.2, les numéros de versions pour Windows correspondent aux versions d'Horizon Client sur d'autres systèmes d'exploitation et périphériques.

## Exécution de commandes sur des postes de travail View

Vous pouvez utiliser les paramètres de stratégie de groupe `CommandsToRunOnConnect`, `CommandsToRunOnReconnect` et `CommandsToRunOnDisconnect` d'Horizon Agent pour exécuter des commandes et des scripts de commande sur des postes de travail View lorsque les utilisateurs se connectent, se reconnectent et se déconnectent.

Pour exécuter une commande ou un script de commande, ajoutez le nom de commande ou le chemin de fichier du script à la liste de commandes du paramètre de stratégie de groupe. Par exemple :

```
date
```

```
C:\Scripts\myscript.cmd
```

Pour exécuter des scripts qui requièrent un accès à la console, ajoutez en préfixe l'option `-C` ou `-c` suivie d'un espace. Par exemple :

```
-c C:\Scripts\Cli_clip.cmd
```

```
-C e:\procexp.exe
```

Les types de fichiers pris en charge sont `.CMD`, `.BAT` et `.EXE`. Les fichiers `.VBS` ne sont pas exécutés sauf s'ils sont analysés avec `cscript.exe` ou `wscript.exe`. Par exemple :

```
-C C:\WINDOWS\system32\wscript.exe C:\Scripts\checking.vbs
```

La longueur totale de la chaîne, y compris l'option `-C` ou `-c`, ne doit pas dépasser 260 caractères.

# Paramètres de stratégie PCoIP

Le fichier de modèle d'administration PCoIP (`pcoip.adm`) contient des paramètres de stratégie liés au protocole d'affichage PCoIP. Vous pouvez configurer des paramètres sur des valeurs par défaut, qui peuvent être remplacées par un administrateur, ou vous pouvez configurer des paramètres sur des valeurs ne pouvant pas être remplacées.

Ce fichier ADM est disponible dans un fichier groupé `.zip` nommé `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip`, que vous pouvez télécharger sur le site de téléchargement de VMware à l'adresse https://my.vmware.com/web/vmware/downloads. Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut le fichier groupé `.zip`.

Le fichier de modèle d'administration pour les variables de session PCoIP de View contient deux sous-catégories :

| | |
|---|---|
| **Valeurs par défaut remplaçables par l'administrateur** | Spécifie les valeurs par défaut du paramètre de stratégie PCoIP. Ces paramètres peuvent être remplacés par un administrateur. Ces paramètres inscrivent des valeurs de clé de Registre sur `HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin_defaults`. |
| **Paramètres non remplaçables par l'administrateur** | Contient les mêmes paramètres que Valeurs par défaut remplaçables par l'administrateur, mais ces paramètres ne peuvent pas être remplacés par un administrateur. Ces paramètres inscrivent des valeurs de clé de Registre sur `HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin`. |

Le modèle ne contient que des paramètres Configuration d'ordinateur.

## Clés de Registre non liées à des stratégies

Si un paramètre de machine locale doit être appliqué et ne peut pas être placé sous `HKLM\Software\Policies\Teradici`, des paramètres de machine locale peuvent être placés dans des clés de Registre dans `HKLM\Software\Teradici`. Les mêmes clés de Registre peuvent être placées dans `HKLM\Software\Teradici` comme dans `HKLM\Software\Policies\Teradici`. Si la même clé de Registre est présente dans les deux emplacements, le paramètre dans `HKLM\Software\Policies\Teradici` remplace la valeur de machine locale.

## Paramètres généraux PCoIP

Le fichier de modèle d'administration PCoIP de View contient des paramètres de stratégie de groupe qui configurent des paramètres généraux tels que la qualité d'image PCoIP, les périphériques USB et les ports réseau.

**Tableau 17-8.** Paramètres de stratégie généraux PCoIP

| Paramètre | Description |
|---|---|
| `Configure clipboard redirection` | Détermine le sens dans lequel la redirection du Presse-papiers est autorisée. Vous pouvez sélectionner l'une des valeurs suivantes :<br>■ **Activé uniquement de client vers agent** (C'est-à-dire, autoriser le copier-coller uniquement depuis le système client vers le poste de travail distant.)<br>■ **Désactivé dans les deux sens**<br>■ **Activé dans les deux sens**<br>■ **Activé uniquement d'agent vers client** (C'est-à-dire, autoriser le copier-coller uniquement depuis le poste de travail distant vers le système client.)<br>La redirection du presse-papier est implémentée sous forme de canal virtuel. Si des canaux virtuels sont désactivés, la redirection du presse-papier ne fonctionne pas.<br>Ce paramètre s'applique à Horizon Agent uniquement.<br>Lorsque ce paramètre est désactivé ou non configuré, la valeur par défaut est **Activé uniquement de client vers agent**. |
| `Configure PCoIP client image cache size policy` | Contrôle la taille du cache d'images client PCoIP. Le client utilise une mise en cache d'images pour stocker des parties de l'affichage qui ont été précédemment transmises. La mise en cache d'images réduit la quantité de données qui sont retransmises.<br>Ce paramètre s'applique uniquement aux clients Windows, Linux et Mac lorsque la version View 5.0 ou ultérieure est installée pour Horizon Client, Horizon Agent et le Serveur de connexion View.<br>Lorsque ce paramètre n'est pas configuré ou qu'il est désactivé, PCoIP utilise une taille de cache d'images client par défaut de 250 Mo.<br>Avec Horizon Client 3.1 ou version ultérieure, si vous spécifiez une valeur inférieure à la quantité de mémoire disponible divisée par 2, le cache est défini selon la formule suivante :<br>`user-setting – 10 MB`<br>Avec Horizon Client 3.1 ou version ultérieure, si vous spécifiez une valeur supérieure à la quantité de mémoire disponible divisée par 2, le cache est défini selon la formule suivante :<br>`available-memory / 2 – 10 MB`<br>Par exemple, si vous spécifiez une taille de cache maximale de 1 024 Mo et que la mémoire disponible est de 1 600 Mo, la taille du cache maximale est définie sur 790 Mo.<br>Pour toutes les versions de Horizon Client, la taille par défaut est de 250 Mo et la taille minimale est de 50 Mo.<br>Dans Horizon Client 1.6 ou version ultérieure, la taille maximale est de 1 024 Mo. Avec Horizon Client 1.5 ou version antérieure, la taille maximale est de 300 Mo. |

**Tableau 17-8.** Paramètres de stratégie généraux PCoIP (suite)

| Paramètre | Description |
|---|---|
| `Configure PCoIP event log cleanup by size in MB` | Active la configuration du nettoyage du journal des événements PCoIP par taille en Mo.<br>Lorsque cette stratégie est configurée, le paramètre contrôle la taille que peut prendre un fichier journal avant d'être nettoyé. Pour une valeur de *m* différente de zéro, les fichiers journaux dont la taille est supérieure à *m* Mo sont supprimés automatiquement et de manière silencieuse. La valeur 0 indique qu'aucun nettoyage de fichier par taille n'est effectué.<br>Lorsque cette stratégie est désactivée ou non configurée, la valeur par défaut du nettoyage du journal des événements par taille est de 100 Mo.<br>Le nettoyage du fichier journal s'effectue une seule fois au démarrage d'une session. Tout changement apporté au paramètre ne sera appliqué qu'à l'ouverture de la prochaine session. |
| `Configure PCoIP event log cleanup by time in days` | Active la configuration du nettoyage du journal des événements PCoIP par durée en jours.<br>Lorsque cette stratégie est configurée, le paramètre contrôle le nombre de jours qui peuvent s'écouler avant que le fichier journal soit nettoyé. Pour une valeur de *n* différente de zéro, les fichiers journaux antérieurs à *n* jours sont supprimés automatiquement et de manière silencieuse. La valeur 0 indique qu'aucun nettoyage de fichier par durée n'est effectué.<br>Lorsque cette stratégie est désactivée ou non configurée, la valeur par défaut du nettoyage du journal des événements est de 7 jours.<br>Le nettoyage du fichier journal s'effectue une seule fois au démarrage d'une session. Tout changement apporté au paramètre ne sera appliqué qu'à l'ouverture de la prochaine session. |
| `Configure PCoIP event log verbosity` | Définit le niveau de détails du journal des événements PCoIP. Les valeurs sont comprises entre 0 (le moins de détails) et 3 (le plus de détails).<br>Lorsque ce paramètre est activé, vous pouvez définir le niveau de détail entre 0 et 3. Lorsque le paramètre n'est pas configuré ou désactivé, le niveau de détail du journal des événements par défaut est 2.<br>Lorsque ce paramètre est modifié lors d'une session PCoIP active, le nouveau paramètre prend effet immédiatement. |

**Tableau 17-8.** Paramètres de stratégie généraux PCoIP (suite)

| Paramètre | Description |
|---|---|
| `Configure PCoIP image quality levels` | Contrôle comment PCoIP rend les images lors de périodes de surcharge du réseau. Les valeurs **Qualité d'image minimale**, **Qualité d'image initiale maximale** et **Fréquence d'image maximale** interagissent pour contrôler précisément des environnements contraints en termes de bande passante réseau.<br>Utilisez la valeur **Qualité d'image minimale** pour équilibrer la qualité d'image et la fréquence d'image lorsque la bande passante est limitée. Vous pouvez spécifier une valeur comprise entre 30 et 100. La valeur par défaut est 40. Une valeur inférieure permet d'utiliser des fréquences d'image élevées, mais avec un affichage d'une qualité potentiellement inférieure. Une valeur supérieure fournit une qualité d'image supérieure, mais avec des fréquences d'image potentiellement inférieures lorsque la bande passante réseau est contrainte. Lorsque la bande passante réseau n'est pas contrainte, PCoIP conserve la qualité maximale quelle que soit cette valeur.<br>Utilisez la valeur **Qualité d'image initiale maximale** pour réduire les pics de bande passante réseau requis par PCoIP en limitant la qualité initiale des régions modifiées de l'image affichée. Vous pouvez spécifier une valeur comprise entre 30 et 100. La valeur par défaut est 80. Une valeur inférieure réduit la qualité d'image des modifications de contenu et diminue les exigences de bande passante maximale. Une valeur supérieure augmente la qualité d'image des modifications de contenu et augmente les exigences de bande passante maximale. Les régions non modifiées de l'image entraînent progressivement une qualité sans perte (parfaite) quelle que soit cette valeur. Une valeur de 80 ou moins permet d'utiliser au mieux la bande passante disponible.<br>La valeur **Qualité d'image minimale** ne peut pas dépasser la valeur **Qualité d'image initiale maximale**.<br>Utilisez la valeur **Fréquence d'image maximale** pour gérer la bande passante moyenne consommée par utilisateur en limitant le nombre d'actualisations d'écran par seconde. Vous pouvez spécifier une valeur comprise entre 1 et 120 images par seconde. La valeur par défaut est 30. Une valeur supérieure peut utiliser plus de bande passante mais fournit moins de gigue, ce qui permet des transitions plus homogènes entre les images, comme dans une vidéo. Une valeur inférieure utilise moins de bande passante mais entraîne plus de gigue.<br>Ces valeurs de qualité d'image ne s'appliquent qu'à l'hôte léger et n'ont aucun effet sur un client léger.<br>Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les valeurs par défaut sont utilisées.<br>Lorsque ce paramètre est modifié lors d'une session PCoIP active, le nouveau paramètre prend effet immédiatement. |
| `Configure frame rate vs image quality preference` | Configurez la préférence pour la fréquence d'images et la qualité d'image entre 0 (fréquence d'images la plus élevée) et 100 (qualité d'image la plus élevée). Si cette stratégie est désactivée ou non configurée, la valeur par défaut est 50.<br>Une valeur supérieure (max : 100) signifie que vous préférez une qualité d'image élevée même si la fréquence d'images est hachée. Une valeur inférieure (min : 0) signifie que vous préférez une expérience fluide avec une qualité d'image agressive.<br>Ce paramètre peut fonctionner avec le GPO `Configure PCoIP image quality levels`, qui détermine le niveau de qualité d'image initial maximal et le niveau de qualité d'image minimal. Alors que la `Frame rate and image quality preference` peut ajuster le niveau de qualité d'image de chaque image, elle ne peut pas dépasser le seuil de niveau de qualité maximal/minimal configuré par le GPO `Configure PCoIP image quality levels`.<br>Lorsque cette stratégie est modifiée au cours de l'exécution, elle peut prendre effet immédiatement. |

**Tableau 17-8.** Paramètres de stratégie généraux PCoIP (suite)

| Paramètre | Description |
|---|---|
| `Configure PCoIP session encryption algorithms` | Contrôle les algorithmes de cryptage annoncés par le point de terminaison PCoIP lors de la négociation de session.<br>Cocher l'une des cases désactive l'algorithme de cryptage associé. Vous devez activer au moins un algorithme.<br>Ce paramètre s'applique à la fois à l'agent et au client. Les points de terminaison négocient l'algorithme de cryptage de session réel qui est utilisé. Si le mode approuvé FIPS140-2 est activé, la valeur **Disable AES-128-GCM encryption (Désactiver le cryptage AES-128-GCM)** est toujours remplacée pour que le cryptage AES-128-GCM soit activé.<br>Les algorithmes de chiffrement pris en charge, par ordre de préférence, sont SALSA20/12-256, AES-GCM-128 et AES-GCM-256. Par défaut, tous les algorithmes de chiffrement pris en charge sont disponibles à la négociation à partir de ce point de terminaison.<br>Si les deux points de terminaison sont configurés pour prendre en charge ces trois algorithmes et que la connexion n'utilise pas de passerelle de sécurité (Security Gateway, SG), l'algorithme SALSA20 est négocié et utilisé. En revanche, si la connexion utilise une passerelle de sécurité (SG), l'algorithme SALSA20 est désactivé automatiquement et c'est l'algorithme AES128 qui est négocié et utilisé. Si l'un des points de terminaison ou la passerelle de sécurité désactive l'algorithme SALSA20 et que l'un des points de terminaison désactive l'algorithme AES128, c'est l'algorithme AES256 qui est alors négocié et utilisé. |

**Tableau 17-8.** Paramètres de stratégie généraux PCoIP (suite)

| Paramètre | Description |
|---|---|
| `Configure PCoIP USB allowed and unallowed device rules` | Spécifie les périphériques USB autorisés et interdits pour les sessions PCoIP qui utilisent un client zéro exécutant le microprogramme Teradici. Les périphériques USB utilisés dans des sessions PCoIP doivent apparaître dans la table d'autorisation USB. Les périphériques USB qui apparaissent dans la table d'interdiction USB ne peuvent pas être utilisés dans des sessions PCoIP.<br>Vous pouvez définir un maximum de 10 règles d'autorisation USB et un maximum de 10 règles d'interdiction USB. Séparez les valeurs avec le caractère de barre verticale (`\|`).<br>Chaque règle peut être une combinaison d'un ID de fournisseur (VID) et d'un ID de produit (PID), ou une règle peut décrire une classe de périphériques USB. Une règle de classe peut autoriser ou interdire une classe de périphériques entière, une seule sous-classe ou un protocole dans une sous-classe.<br>Le format d'une combinaison de règle VID/PID est **`1xxxxyyyy`**, où **`xxxx`** est le VID au format hexadécimal et **`yyyy`** le PID au format hexadécimal. Par exemple, la règle pour autoriser ou bloquer un périphérique avec le VID **`0x1a2b`** et le PID **`0x3c4d`** est **`11a2b3c4d`**.<br>Pour des règles de classe, utilisez l'un des formats suivants :<br>**Autoriser tous les périphériques USB** — Format : **`23XXXXXX`**<br>Exemple : **`23XXXXXX`**<br>**Autoriser tous les périphériques USB avec un ID de classe spécifique** — Format : **`22`*`class`*`XXXX`**<br>Exemple : **`22aaXXXX`**<br>**Autoriser une sous-classe spécifique** — Format : **`21`*`class-subclass`*`XX`**<br>Exemple : **`21aabbXX`**<br>**Autoriser un protocole spécifique** — Format : **`20`*`class-subclass-protocol`***<br>Exemple : **`20aabbcc`**<br>Par exemple, la chaîne d'autorisation USB pour autoriser les périphériques HID USB (souris et clavier) (ID de classe 0x03) et les webcams (ID de classe 0x0e) est **`2203XXXX\|220eXXXX`**. La chaîne d'interdiction USB pour interdire les périphériques de stockage de masse USB (ID de classe 0x08) est **`2208XXXX`**.<br>Une chaîne d'autorisation USB vide signifie qu'aucun périphérique USB n'est autorisé. Une chaîne d'interdiction USB vide signifie qu'aucun périphérique USB n'est interdit.<br>Ce paramètre s'applique à Horizon Agent uniquement et seulement lorsque le poste de travail distant est dans une session avec un client ultra léger qui exécute le micrologiciel Teradici. L'utilisation de périphérique est négociée entre les points de terminaison.<br>Par défaut, tous les périphériques sont autorisés et aucun n'est interdit. |

**Tableau 17-8.** Paramètres de stratégie généraux PCoIP (suite)

| Paramètre | Description |
|---|---|
| `Configure PCoIP virtual channels` | Spécifie les canaux virtuels qui peuvent et ne peuvent pas fonctionner sur des sessions PCoIP. Ce paramètre détermine également s'il est nécessaire de désactiver le traitement du presse-papier sur l'hôte PCoIP.<br>Les canaux virtuels utilisés dans des sessions PCoIP doivent apparaître dans la liste d'autorisation des canaux virtuels. Les canaux virtuels qui apparaissent dans la liste des canaux virtuels interdits ne peuvent pas être utilisés dans des sessions PCoIP.<br>Vous pouvez spécifier un maximum de 15 canaux virtuels à utiliser dans des sessions PCoIP.<br>Séparez les noms de canal avec le caractère de barre verticale (`\|`). Par exemple, la chaîne d'autorisation des canaux virtuels pour autoriser les canaux virtuels mksvchan et vdp_rdpvcbridge est **`mksvchan\|vdp_vdpvcbridge`**.<br>Si un nom de canal contient le caractère de barre verticale ou de barre oblique inverse (`\`), insérez un caractère de barre oblique inverse avant ce caractère. Par exemple, saisissez le nom de canal awk\|ward\channel comme suit : **`awk\\\|ward\\\\channel`**.<br>Lorsque la liste des canaux virtuels autorisés est vide, tous les canaux virtuels sont interdits. Lorsque la liste des canaux virtuels interdits est vide, tous les canaux virtuels sont autorisés.<br>Le paramètre des canaux virtuels s'applique à la fois à l'agent et au client. Les canaux virtuels doivent être activés à la fois sur l'agent et le client pour pouvoir être utilisés.<br>Le paramètre des canaux virtuels fournit une case séparée qui vous permet de désactiver le traitement du presse-papier à distance sur l'hôte PCoIP. Cette valeur ne s'applique qu'à l'agent.<br>Par défaut, tous les canaux virtuels sont activés, notamment le traitement du presse-papier. |
| `Configure the PCoIP transport header` | Configure l'en-tête de transport PCoIP et définit la priorité de la session de transport.<br>L'en-tête de transport PCoIP est un en-tête 32 bits ajouté à tous les paquets UDP PCoIP (uniquement si l'en-tête de transport est activé et pris en charge des deux côtés). L'en-tête de transport PCoIP permet aux périphériques réseau de prendre de meilleures décisions concernant la hiérarchisation/qualité de service lors du traitement de la surcharge du réseau. L'en-tête de transport est activé par défaut.<br>La priorité de session de transport détermine la priorité de session PCoIP signalée dans l'en-tête de transport PCoIP. Les périphériques réseau prennent de meilleures décisions concernant la hiérarchisation/qualité de service en fonction de la priorité de session de transport spécifiée.<br>Lorsque le paramètre `Configure the PCoIP transport header` est activé, les priorités de session de transport suivantes sont disponibles :<br>■ **Haute**<br>■ **Moyenne** (valeur par défaut)<br>■ **Basse**<br>■ **Non définie**<br>La valeur de priorité de session de transport est négociée par l'agent et le client PCoIP. Si l'agent PCoIP spécifie une valeur de priorité de session de transport, la session utilise la priorité de session spécifiée par l'agent. Si seul le client a spécifié une priorité de session de transport, la session utilise la priorité de session spécifiée par le client. Si ni l'agent ni le client n'a spécifié une priorité de session de transport, ou si **Priorité non définie** est spécifié, la session utilise la valeur par défaut, la priorité **Moyenne**. |

**Tableau 17-8.** Paramètres de stratégie généraux PCoIP (suite)

| Paramètre | Description |
|---|---|
| `Configure the TCP port to which the PCoIP host binds and listens` | Spécifie le port TCP de l'agent lié par des hôtes PCoIP logiciels.<br>La valeur du port TCP spécifie le port TCP de base auquel l'agent tente de se lier. La valeur de plage du port TCP détermine le nombre de ports supplémentaires à essayer si le port de base n'est pas disponible. La plage du port doit être comprise entre 1 et 10.<br>La plage s'étend du port de base à la somme du port de base et de la plage du port. Par exemple, si le port de base est 4172 et que la plage du port est 10, la plage s'étend de 4172 à 4182.<br>Ne définissez pas la taille de la plage de ports sur 0, car cela entraînera un échec de connexion lorsque l'utilisateur se connectera au poste de travail avec le protocole d'affichage PCoIP. Horizon Client renvoie le message d'erreur `Le protocole d'affichage de ce poste de travail n'est pas actuellement disponible. Contactez votre administrateur système`.<br>Ce paramètre s'applique à Horizon Agent uniquement.<br>Sur des machines mono-utilisateur, le port TCP de base par défaut est 4172 dans View 4.5 et version ultérieure. Le port de base par défaut est 50002 dans View 4.0.*x* et version antérieure. Par défaut, la plage de port est 1.<br>Sur des hôtes RDS, le port TCP de base par défaut est 4173. Lorsque PCoIP est utilisé avec des hôtes RDS, un port PCoIP distinct est utilisé pour chaque connexion utilisateur. La plage de ports par défaut qui est utilisée par le service Bureau à distance est suffisamment étendue pour gérer le nombre maximal de connexions utilisateurs simultanées prévu.<br>**Important** Nous vous recommandons de ne pas utiliser ce paramètre de stratégie pour modifier la plage de ports par défaut sur des hôtes RDS ou pour changer la valeur du port TCP par défaut qui est de 4173. Mais surtout, ne définissez pas la valeur du port TCP sur 4172. La réinitialisation de cette valeur à 4172 affecterait les performances PCoIP dans les session RDS. |
| `Configure the UDP port to which the PCoIP host binds and listens` | Spécifie le port UDP de l'agent lié par des hôtes PCoIP logiciels.<br>La valeur du port UDP spécifie le port UDP de base auquel l'agent tente de se lier. La valeur de plage du port UDP détermine le nombre de ports supplémentaires à essayer si le port de base n'est pas disponible. La plage du port doit être comprise entre 1 et 10.<br>Ne définissez pas la taille de la plage de ports sur 0, car cela entraînera un échec de connexion lorsque l'utilisateur se connectera au poste de travail avec le protocole d'affichage PCoIP. Horizon Client renvoie le message d'erreur `Le protocole d'affichage de ce poste de travail n'est pas actuellement disponible. Contactez votre administrateur système`.<br>La plage s'étend du port de base à la somme du port de base et de la plage du port. Par exemple, si le port de base est 4172 et que la plage du port est 10, la plage s'étend de 4172 à 4182.<br>Ce paramètre s'applique à Horizon Agent uniquement.<br>Sur des machines mono-utilisateur, le port UDP de base par défaut est 4172 pour View 4.5 et versions ultérieures, et 50002 pour View 4.0.*x* et version antérieure. Par défaut, la plage de port est 10.<br>Sur des hôtes RDS, le port UDP de base par défaut est 4173. Lorsque PCoIP est utilisé avec des hôtes RDS, un port PCoIP distinct est utilisé pour chaque connexion utilisateur. La plage de ports par défaut qui est utilisée par le service Bureau à distance est suffisamment étendue pour gérer le nombre maximal de connexions utilisateurs simultanées prévu.<br>**Important** Nous vous recommandons de ne pas utiliser ce paramètre de stratégie pour modifier la plage de ports par défaut sur des hôtes RDS ou pour changer la valeur du port UDP par défaut qui est de 4173. Mais surtout, ne définissez pas la valeur du port UDP sur 4172. La réinitialisation de cette valeur à 4172 affecterait les performances PCoIP dans les session RDS. |

**Tableau 17-8.** Paramètres de stratégie généraux PCoIP (suite)

| Paramètre | Description |
|---|---|
| `Enable access to a PCoIP session from a vSphere console` | Détermine s'il est nécessaire d'autoriser une console vSphere Client à afficher une session PCoIP active et à envoyer l'entrée au poste de travail.<br>Par défaut, lorsqu'un client est attaché via PCoIP, l'écran de la console vSphere Client est vide et la console ne peut pas envoyer l'entrée. Le paramètre par défaut garantit qu'un utilisateur malveillant ne peut pas voir le poste de travail de l'utilisateur ou fournir d'entrées sur l'hôte localement lorsqu'une session distante PCoIP est active.<br>Ce paramètre s'applique à Horizon Agent uniquement.<br>Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, l'accès à la console n'est pas autorisé. Lorsque ce paramètre est activé, la console affiche la session PCoIP et l'entrée de console est autorisée.<br>Lorsque ce paramètre est activé, la console peut afficher une session PCoIP exécutée sur un système Windows 7 uniquement lorsque la machine virtuelle Windows 7 est le matériel version v8. La version matérielle v8 est disponible uniquement sur ESXi 5.0 et version ultérieure. A contrario, l'entrée de console sur un système Windows 7 est autorisée quelle que soit la version matérielle de la machine virtuelle. |
| `Enable the FIPS 140-2 approved mode of operation` | Détermine s'il est nécessaire d'utiliser uniquement des algorithmes et des protocoles cryptographiques approuvés FIPS 140-2 pour établir une connexion PCoIP à distance. Activer ce paramètre remplace la désactivation du cryptage AES128-GCM.<br>Ce paramètre s'applique à la fois à l'agent 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.<br>Le mode FIPS est disponible pour View 4.5 et supérieur. Pour View 4.0.*x* et antérieur, le mode FIPS n'est pas disponible, et la configuration de ce paramètre n'a aucun effet.<br>Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, le mode FIPS n'est pas utilisé. |
| `Enable/disable audio in the PCoIP session` | Détermine si le son est activé dans des sessions PCoIP. Le son doit être activé sur les deux points de terminaison. Lorsque ce paramètre est activé, le son PCoIP est autorisé. Lorsqu'il est désactivé, le son PCoIP est désactivé. Lorsque ce paramètre n'est pas configuré, le son est activé par défaut. |
| `Enable/disable microphone noise and DC offset filter in PCoIP session` | Détermine s'il est nécessaire d'activer le bruit microphonique et le filtre de tension de décalage continue pour l'entrée de microphone lors de sessions PCoIP.<br>Ce paramètre ne s'applique qu'à Horizon Agent et au pilote audio Teradici.<br>Lorsque ce paramètre n'est pas configuré, le pilote audio Teradici utilise le bruit microphonique et le filtre de tension de décalage continue par défaut. |
| `Turn on PCoIP user default input language synchronization` | Détermine si la langue d'entrée par défaut pour l'utilisateur dans la session PCoIP est synchronisée avec la langue d'entrée par défaut du point de terminaison du client PCoIP. Lorsque ce paramètre est activé, la synchronisation est autorisée. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, la synchronisation est interdite.<br>Ce paramètre s'applique à Horizon Agent uniquement. |

## Paramètres de bande passante PCoIP

Le fichier de modèle d'administration PCoIP de View contient des paramètres de stratégie de groupe qui configurent des caractéristiques de bande passante PCoIP.

**Tableau 17-9.** Variables de bande passante de la session PCoIP de View

| Paramètre | Description |
|---|---|
| `Configure the maximum PCoIP session bandwidth` | Spécifie la bande passante maximale, en kilobits par seconde, dans une session PCoIP. La bande passante inclut la création d'images, le son, le canal virtuel, USB et le trafic PCoIP de contrôle.<br>Définissez cette valeur sur la capacité globale du lien auquel votre point de terminaison est connecté, en tenant compte du nombre de sessions PCoIP simultanées prévues. Par exemple, avec une configuration VDI à un seul utilisateur (une session PCoIP unique) qui se connecte au moyen d'une connexion Internet 4 Mbits/s, définissez cette valeur sur 4 Mbit, ou 10 % de moins que cette valeur pour prévoir un autre trafic réseau. Lorsque vous prévoyez que plusieurs sessions PCoIP simultanées partageront un lien, comprenant plusieurs utilisateurs VDI ou une configuration RDS, vous pouvez régler ce paramètre en conséquence. Cependant, la diminution de cette valeur limitera la bande passante maximale de chaque session active.<br>La définition de cette valeur empêche l'agent de transmettre un débit supérieur à la capacité de lien, ce qui pourrait entraîner une perte de paquets excessive et une mauvaise expérience utilisateur. Cette valeur est symétrique. Elle force le client et l'agent à utiliser la plus faible des deux valeurs qui sont définies côté client et agent. Par exemple, la définition d'une bande passante maximale de 4 Mbit/s force l'agent à transmettre à un débit plus faible, même si le paramètre est configuré sur le client.<br>Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré sur un point de terminaison, le point de terminaison n'impose aucune contrainte de bande passante. Lorsque ce paramètre est configuré, le paramètre est utilisé comme la contrainte de bande passante maximale du point de terminaison en kilobits par seconde.<br>La valeur par défaut lorsque ce paramètre n'est pas configuré est de 900000 kilobits par seconde.<br>Ce paramètre s'applique à la fois à Horizon Agent et au client. Si les deux points de terminaison ont des paramètres différents, la valeur la plus faible est utilisée. |
| `Configure the PCoIP session bandwidth floor` | Spécifie une limite inférieure, en kilobits par seconde, pour la bande passante réservée par la session PCoIP.<br>Ce paramètre configure le taux de transmission de bande passante minimum attendu pour le point de terminaison. Lorsque vous utilisez ce paramètre pour réserver de la bande passante pour un point de terminaison, l'utilisateur n'a pas à attendre que la bande passante soit disponible, ce qui améliore la réactivité de la session.<br>Assurez-vous que vous ne sursouscrivez pas la bande passante totale réservée pour tous les points de terminaison. Assurez-vous que la somme des valeurs plancher de la bande passante pour toutes les connexions dans votre configuration ne dépasse pas la capacité du réseau.<br>La valeur par défaut est 0, ce qui signifie qu'aucune bande passante minimale n'est réservée. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, aucune bande passante minimale n'est réservée.<br>Ce paramètre s'applique à Horizon Agent et au client, mais le paramètre n'affecte que le point de terminaison sur lequel il est configuré.<br>Lorsque ce paramètre est modifié lors d'une session PCoIP active, la modification prend effet immédiatement. |

**Tableau 17-9.** Variables de bande passante de la session PCoIP de View (suite)

| Paramètre | Description |
|---|---|
| `Configure the PCoIP session MTU` | Spécifie la taille de l'unité de transmission maximale (MTU) pour les paquets UDP d'une session PCoIP.<br>La taille de la MTU inclut les en-têtes de paquet IP et UDP. Le protocole TCP utilise le mécanisme de découverte MTU standard pour définir la MTU et n'est pas affecté par ce paramètre.<br>La taille de la MTU maximale est de 1 500 octets. La taille de la MTU minimale est de 500 octets. La valeur par défaut est de 1 300 octets.<br>En général, vous n'avez pas à modifier la taille de la MTU. Modifiez cette valeur si vous avez une configuration de réseau inhabituelle qui provoque une fragmentation de paquets PCoIP.<br>Ce paramètre s'applique à la fois à Horizon Agent et au client. Si les deux points de terminaison ont des paramètres de taille de MTU différents, la valeur la plus faible est utilisée.<br>Si ce paramètre est désactivé ou qu'il n'est pas configuré, le client utilise la valeur par défaut dans la négociation avec Horizon Agent. |

**Tableau 17-9.** Variables de bande passante de la session PCoIP de View (suite)

| Paramètre | Description |
|---|---|
| `Configure the PCoIP session audio bandwidth limit` | Spécifie la bande passante maximale pouvant être utilisée pour le son (lecture audio) dans une session PCoIP.<br>Le traitement audio surveille la bande passante utilisée pour le son. Le traitement sélectionne l'algorithme de compression audio qui fournit le meilleur son possible, en fonction de l'utilisation actuelle de la bande passante. Si une limite de bande passante est définie, le traitement réduit la qualité en modifiant la sélection de l'algorithme de compression jusqu'à ce que la limite de bande passante soit atteinte. S'il n'est pas possible d'atteindre un son de qualité minimale dans la limite de bande passante spécifiée, le son est désactivé.<br>Pour un son stéréo non compressé de haute qualité, définissez cette valeur sur plus de 1 600 kbit/s. Une valeur de 450 kbit/s et plus permet d'obtenir un son stéréo compressé de haute qualité. Une valeur comprise entre 50 kbit/s et 450 kbit/s donne un son dont la qualité va de celle d'une radio FM à celle d'un appel téléphonique. Une valeur inférieure à 50 kbit/s peut entraîner une lecture sans son.<br>Ce paramètre s'applique à Horizon Agent uniquement. Vous devez activer le son sur les deux points de terminaison avant que ce paramètre ne prenne effet.<br>En outre, ce paramètre n'a pas d'effet sur l'audio USB.<br>Si ce paramètre est désactivé ou qu'il n'est pas configuré, une limite de bande passante audio par défaut de 500 kilobits par seconde est configurée pour contraindre l'algorithme de compression audio sélectionné. Si le paramètre est configuré, la valeur est mesurée en kilobits par seconde, avec une limite de bande passante audio par défaut de 500 kilobits par seconde.<br>Ce paramètre s'applique à View 4.6 et supérieur. Il n'a aucun effet sur les versions antérieures de View.<br>Lorsque ce paramètre est modifié lors d'une session PCoIP active, la modification prend effet immédiatement. |
| `Turn off Build-to-Lossless feature` | Ce paramètre spécifie s'il convient de désactiver ou non la fonctionnalité de développement sans perte du protocole PCoIP. Cette fonctionnalité est désactivée par défaut.<br>Si ce paramètre est activé ou qu'il n'est pas configuré, la fonctionnalité de développement sans perte est désactivée, et les images et autre contenu de poste de travail et d'application ne sont jamais développés pour un état sans perte. Dans les environnements réseau dans lesquels la bande passante est limitée, la désactivation de la fonctionnalité de développement sans perte peut permettre d'économiser de la bande passante.<br>Si ce paramètre est désactivé, la fonctionnalité de développement sans perte est activée. L'activation de la fonctionnalité de développement sans perte est recommandée dans les environnements nécessitant que les images et autre contenu de poste de travail et d'application soient développés pour un état sans perte.<br>Lorsque ce paramètre est modifié lors d'une session PCoIP active, la modification prend effet immédiatement.<br>Pour plus d'informations sur la fonction de développement sans perte PCoIP, reportez-vous à la section « Fonction de développement sans perte PCoIP », page 327. |

## Paramètres de clavier PCoIP

Le fichier de modèle d'administration PCoIP de View contient des paramètres de stratégie de groupe qui configurent des paramètres PCoIP affectant l'utilisation du clavier.

**Tableau 17-10.** Variables de la session PCoIP de View pour le clavier

| Paramètre | Description |
|---|---|
| `Disable sending CAD when users press Ctrl+Alt+Del` | Lorsque cette stratégie est activée, les utilisateurs doivent appuyer sur Ctrl+Alt+Inser plutôt que sur Ctrl+Alt+Suppr pour envoyer une séquence de touches de sécurité (SAS, Secure Attention Sequence) au poste de travail distant pendant une session PCoIP.<br>Vous voulez peut-être activer ce paramètre si des utilisateurs sont confus lorsqu'ils appuient sur Ctrl+Alt+Suppr pour verrouiller le point de terminaison du client et qu'une SAS est envoyée à l'hôte et au client.<br>Ce paramètre s'applique à Horizon Agent uniquement et n'a aucun effet sur un client.<br>Lorsque cette stratégie n'est pas configurée ou est désactivée, les utilisateurs peuvent appuyer sur Ctrl+Alt+Suppr ou sur Ctrl+Alt+Inser pour envoyer une SAS au poste de travail distant. |
| `Use alternate key for sending Secure Attention Sequence` | Spécifie une touche alternative, à la place de la touche Inser, pour l'envoi d'une séquence de touches de sécurité (SAS, Secure Attention Sequence).<br>Vous pouvez utiliser ce paramètre pour conserver la séquence de touches Ctrl+Alt+Inser sur les machines virtuelles lancées de l'intérieur d'un poste de travail distant pendant une session PCoIP.<br>Par exemple, un utilisateur peut démarrer un vSphere Client depuis un poste de travail PCoIP et ouvrir une console sur une machine virtuelle dans vCenter Server. Si la séquence Ctrl+Alt+Inser est utilisée dans le système d'exploitation client sur la machine virtuelle vCenter Server, une SAS Ctrl+Alt+Suppr est envoyée à la machine virtuelle. Ce paramètre permet à la séquence Ctrl+Alt+*Alternate Key* d'envoyer une SAS Ctrl+Alt+Suppr au poste de travail PCoIP.<br>Lorsque ce paramètre est activé, vous devez sélectionner une autre touche depuis un menu déroulant. Vous ne pouvez pas activer ce paramètre et laisser la valeur non spécifiée.<br>Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, la séquence de touches Ctrl+Alt+Inser est utilisée comme SAS.<br>Ce paramètre s'applique à Horizon Agent uniquement et n'a aucun effet sur un client. |

## Fonction de développement sans perte PCoIP

Vous pouvez configurer le protocole d'affichage PCoIP afin qu'il utilise approche de codage nommée développement progressif ou développement sans perte qui permet de fournir une expérience utilisateur globale optimale, même dans des conditions de réseau contraintes. Cette fonctionnalité est désactivée par défaut.

La fonctionnalité de développement sans perte fournit une image initiale hautement compressée, appelée image avec perte, qui est ensuite progressivement développée vers un état sans perte complet. Un état sans perte signifie que l'image apparaît avec la haute fidélité prévue.

Sur un réseau LAN, PCoIP affiche toujours le texte à l'aide de la compression sans perte. Si la fonctionnalité de développement sans perte est activée, et si la bande passante disponible par session passe en dessous de 1 Mbits/s, le protocole PCoIP affiche initialement une image texte avec perte et développe rapidement l'image vers un état sans perte. Cette approche permet au poste de travail de rester réactif et d'afficher la meilleure image possible lorsque les conditions de réseau changent, ce qui offre aux utilisateurs une expérience optimale.

La fonction de développement sans perte fournit les caractéristiques suivantes :

- règle dynamiquement la qualité d'image ;
- réduit la qualité d'image sur les réseaux encombrés ;
- maintient la réactivité en réduisant la latence de mise à jour de l'écran ;
- reprend la qualité d'image maximale lorsque le réseau n'est plus encombré.

Vous pouvez activer la fonctionnalité le développement sans perte en désactivant le paramètre de stratégie de groupe `Turn off Build-to-Lossless feature`. Reportez-vous à la section « Paramètres de bande passante PCoIP », page 324.

## Paramètres de stratégie VMware Blast

Le fichier de modèle de stratégie de groupe VMware Blast `vdm_blast.adm` contient des paramètres de stratégie pour le protocole d'affichage VMware Blast. Une fois la stratégie appliquée, les paramètres sont stockés dans la clé de registre `HKLM\Software\Policies\VMware, Inc.\VMware Blast\config`.

Ces paramètres s'appliquent à HTML Access et toutes les instances d'Horizon Client.

**Tableau 17-11.** Paramètres de stratégie VMware Blast

| Paramètre | Description |
|---|---|
| `Max Session Bandwidth` | Spécifie la bande passante maximale, en kilobits par seconde (Kbit/s), pour une session VMware Blast. La bande passante inclut la création d'images, le son, le canal virtuel, USB et le trafic de contrôle VMware Blast. La valeur par défaut est de 1 Gbit/s. |
| `Min Session Bandwidth` | Spécifie la bande passante minimale, en kilobits par seconde (Kbit/s), qui est réservée pour une session VMware Blast. La valeur par défaut est de 128 Kbit/s. |
| `Max Frame Rate` | Spécifie le nombre maximal d'actualisations d'écran. Utilisez ce paramètre pour gérer la bande passante moyenne que les utilisateurs consomment. La valeur par défaut est de 30 actualisations par seconde. |
| `UDP Protocol` | Spécifie si vous voulez utiliser le protocole UDP ou TCP. L'option par défaut est de ne pas utiliser le protocole UDP, c'est-à-dire d'utiliser le protocole TCP. Activez ce paramètre pour utiliser le protocole UDP. Ce paramètre ne s'applique pas à HTML Access, qui utilise toujours le protocole TCP. |
| `H264` | Spécifie si vous voulez utiliser le codage H.264 ou JPEG/PNG. L'option par défaut est d'utiliser le codage H.264. |
| `Screen Blanking` | Spécifie si vous voulez que la console de la machine virtuelle de poste de travail affiche le poste de travail réel que l'utilisateur voit ou si vous voulez afficher un écran vide lorsque le poste de travail a une session active. L'option par défaut est d'afficher un écran vide. |
| `Session Garbage Collection` | Spécifie comment le nettoyage de la mémoire des sessions distantes abandonnées s'exécute. Vous indiquez deux valeurs :<br>■ **Intervalle (ms)** détermine la fréquence, en millisecondes, à laquelle est exécuté le nettoyage de la mémoire. La valeur par défaut est de 100 ms.<br>■ **Seuil (s)** détermine la durée, en secondes, que doit avoir une session abandonnée avant de pouvoir être supprimée. La valeur par défaut est de 1 seconde. |

**Tableau 17-11.** Paramètres de stratégie VMware Blast (suite)

| Paramètre | Description |
|---|---|
| `Image Quality` | Spécifie la qualité d'image de l'écran du poste de travail. Vous pouvez spécifier deux paramètres de qualité faible, deux paramètres de qualité élevée et un paramètre de qualité moyenne. Les paramètres de qualité faible sont destinés aux zones de l'écran qui changent souvent, par exemple, lors du défilement. Les paramètres de qualité élevée sont destinés aux zones de l'écran qui sont plus statiques, ce qui se traduit par une meilleure qualité d'image. Vous pouvez spécifier les paramètres suivants :<br>■ **Qualité JPEG faible** (plage de valeurs disponible : 1 - 100, valeur par défaut : 25)<br>■ **Sous-échantillonnage chromatique JPEG faible** (plage de valeurs disponible : 4:1:0 (le plus faible), 4:1:1, 4:2:0, 4:2:2 et 4:4:4 (le plus élevé), valeur par défaut : 4:1:0)<br>■ **Qualité JPEG moyenne** (plage de valeurs disponible : 1 - 100, valeur par défaut : 35)<br>■ **Qualité JPEG élevée** (plage de valeurs disponible : 1 - 100, valeur par défaut : 90)<br>■ **Sous-échantillonnage chromatique JPEG élevé** (plage de valeurs disponible : 4:1:0 (le plus faible), 4:1:1, 4:2:0, 4:2:2 et 4:4:4 (le plus élevé), valeur par défaut : 4:4:4) |
| `HTTP Service` | Spécifie le port utilisé pour la communication sécurisée (HTTPS) entre le serveur de sécurité ou un dispositif Access Point et un poste de travail. Le pare-feu doit être configuré pour que ce port soit ouvert. La valeur par défaut est 22443. |
| `Audio Playback` | Spécifie si vous voulez que la lecture audio soit activée pour les postes de travail distants. Ce paramètre permet d'activer la lecture audio. |
| `Configure Clipboard Redirection` | Spécifie le comportement autorisé de la redirection du Presse-papiers. Les options sont :<br>■ **Activé dans les deux sens**<br>■ **Désactivé dans les deux sens**<br>■ **Activé du client vers le serveur uniquement** (Les utilisateurs peuvent copier/coller uniquement depuis le client vers le poste de travail.)<br>■ **Activé du serveur vers le client uniquement** (Les utilisateurs peuvent copier/coller uniquement depuis le poste de travail vers le client.)<br>La valeur par défaut est **Activé du client vers le serveur uniquement**. |

# Utilisation de stratégies de groupe des services Bureau à distance

Vous pouvez utiliser les stratégies de groupe des services Bureau à distance (Remote Desktop Services, RDS) pour contrôler la configuration et les performances des hôtes RDS, ainsi que des sessions de poste de travail et d'application RDS. View fournit des fichiers ADMX contenant les stratégies de groupe Microsoft RDS prises en charge dans View.

Nous vous recommandons de configurer les stratégies de groupe fournies dans les fichiers ADMX de View plutôt que les stratégies de groupe Microsoft correspondantes. En effet, les stratégies de groupe de View sont certifiées pour la prise en charge de déploiements de View.

## Configurer le stockage de la licence d'accès utilisateur des services Bureau à distance par périphérique

Vous pouvez configurer les options de stockage de la licence d'accès utilisateur des services Bureau à distance par périphérique afin de spécifier l'emplacement des licences d'accès utilisateur à stocker. Cette fonctionnalité vous permet de choisir si vous voulez stocker les licences d'accès utilisateur ou pas.

Parfois, il peut exister une surutilisation potentielle des licences d'accès utilisateur par périphérique, par exemple les déploiements de View RDS peuvent disposer des deux systèmes Windows Server 2008 et Windows Server 2012. L'activation de cette fonctionnalité rend l'utilisation des licences d'accès utilisateur efficace dans les déploiements de View RDS. Pour cela, la licence émise est stockée, elle est fournie lorsque le client tente de se connecter à l'hôte RDS, puis elle est stockée de nouveau en cas d'éventuelle mise à niveau de licence.

Vous pouvez configurer la licence d'accès utilisateur des services Bureau à distance par périphérique dans View Administrator ou manuellement dans la base de données View LDAP.

### Procédure

1 Dans View Administrator, cliquez sur **Configuration de View** > **Paramètres généraux**.

2 Dans le volet Général, cliquez sur **Modifier**.

3 Sélectionnez l'une des configurations suivantes dans le menu déroulant **Options de stockage de la licence d'accès utilisateur des services Bureau à distance par périphérique**.

| Option | Description |
|---|---|
| **Enregistrer uniquement sur le broker** | Les licences d'accès utilisateur par périphérique sont enregistrées uniquement sur le broker.<br>REMARQUE L'entrée LDAP, `cs-enablerdslicensing=true` et `sendRdsLicense=false`. |
| **Enregistrer sur les clients et sur le broker** | Les licences d'accès utilisateur par périphérique sont stockées sur les clients et sur le broker.<br>REMARQUE Les entrées LDAP `cs-enablerdslicensing=true` et `sendRdsLicense=true`. |
| **Ne pas enregistrer la licence d'accès utilisateur par périphérique** | Les licences d'accès utilisateur par périphérique ne sont stockées nulle part.<br>REMARQUE Les entrées LDAP, `cs-enablerdslicensing=false` et `sendRdsLicense=false`. |

4 Cliquez sur **OK**.

## Ajouter les fichiers ADMX des services Bureau à distance à Active Directory

Vous pouvez ajouter les paramètres de stratégie dans les fichiers RDS ADMX de View pour les objets de stratégie de groupe (GPO) dans Active Directory. Vous pouvez également installer les fichiers RDS ADMX sur des hôtes RDS individuels.

### Prérequis

- Créez des objets de stratégie de groupe pour les paramètres de stratégie de groupe et liez-les à l'UO qui contient vos hôtes RDS.
- Vérifiez que la fonctionnalité Gestion de stratégie de groupe est disponible sur votre serveur Active Directory.

  La procédure d'ouverture de la Console de gestion de stratégie de groupe varie entre les versions Windows 2012, Windows 2008 et Windows 2003 d'Active Directory. Reportez-vous à la section « Créer des GPO pour les stratégies de groupe View », page 348.

### Procédure

1 Téléchargez le fichier View GPO Bundle `.zip` sur le site de téléchargement de VMware à l'adresse https://my.vmware.com/web/vmware/downloads.

  Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut GPO Bundle.

  Le fichier se nomme `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip`, où *x.x.x* est la version et *yyyyyyy* le numéro de build. Tous les fichiers ADM et ADMX qui fournissent des paramètres de stratégie de groupe pour View sont disponibles dans ce fichier.

2 Décompressez le fichier `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` et copiez les fichiers RDS ADMX sur votre hôte Active Directory ou RDS.

   a Copiez les fichiers `vmware_rdsh.admx` et `vmware_rdsh_server.admx`, ainsi que le dossier `en-US` dans le dossier `C:\Windows\PolicyDefinitions` sur votre hôte Active Directory ou RDS.

   b (Facultatif) Copiez les fichiers ressources de la langue `vmware_rdsh.adml` et `vmware_rdsh_server.adml` dans le sous-dossier correspondant dans `C:\Windows\PolicyDefinitions\` sur votre hôte Active Directory ou RDS.

3 Sur l'hôte Active Directory, ouvrez l'Éditeur de gestion des stratégies de groupe.

   Sur un hôte RDS individuel, vous pouvez ouvrir l'Éditeur de stratégie de groupe locale avec l'utilitaire `gpedit.msc`.

   Les paramètres de la stratégie de groupe RDS de View sont installés dans le dossier **Configuration de l'ordinateur > Stratégies > Modèles d'administration > Composants Windows > Services RDSH d'Horizon View > Hôte de session Bureau à distance**.

4 (Facultatif) Configurez les paramètres de stratégie de groupe dans le dossier **Services RDSH d'Horizon View > Hôte de session Bureau à distance**.

## Paramètres de compatibilité des applications RDS

Les paramètres de la stratégie de groupe Compatibilité des applications des services Bureau à distance (RDS) contrôlent la compatibilité de Windows Installer, la virtualisation IP des services Bureau à distance, la sélection de l'adaptateur réseau et l'utilisation de l'adresse IP de l'hôte RDS.

**Tableau 17-12.** Paramètres de la stratégie de groupe Compatibilité des applications RDS

| Paramètre | Description |
|---|---|
| `Turn off Windows Installer RDS Compatibility` | Ce paramètre de stratégie indique si la compatibilité des services Bureau à distance de Windows Installer est exécutée en fonction d'une stratégie par utilisateur pour les applications entièrement installées. Windows Installer ne permet qu'à une seule instance du processus `msiexec` de s'exécuter à la fois. Par défaut, la compatibilité RDS de Windows Installer est activée.<br>Si vous activez ce paramètre de stratégie, la compatibilité RDS de Windows Installer est désactivée et une seule instance du processus `msiexec` peut s'exécuter à la fois.<br>Si vous ne désactivez pas ou si vous ne configurez pas ce paramètre de stratégie, la compatibilité RDS de Windows Installer est activée et plusieurs demandes d'installation d'application par utilisateur sont placées en file d'attente et gérées par le processus `msiexec` selon leur ordre de réception. |
| `Turn on Remote Desktop IP Virtualization` | Ce paramètre de stratégie spécifie si la virtualisation des adresses IP des services Bureau à distance est activée.<br>Par défaut, la virtualisation IP des services Bureau à distance est désactivée.<br>Si vous activez ce paramètre de stratégie, la virtualisation IP des services Bureau à distance est activée. Vous pouvez sélectionner le mode d'application de ce paramètre. Si vous utilisez le mode Par programme, vous devez entrer la liste des programmes pour utiliser des adresses IP virtuelles. Répertoriez chaque programme sur une ligne distincte (n'insérez pas de ligne vierge entre les programmes). Par exemple :<br>`explorer.exe`<br>`mstsc.exe`<br>Si vous désactivez ou si vous ne configurez pas ce paramètre de stratégie, la virtualisation IP des services Bureau à distance est désactivée. |

**Tableau 17-12.** Paramètres de la stratégie de groupe Compatibilité des applications RDS (suite)

| Paramètre | Description |
|---|---|
| `Select the network adapter to be used for Remote Desktop IP Virtualization` | Ce paramètre de stratégie spécifie l'adresse IP et le masque réseau correspondant à l'adaptateur réseau utilisé pour les adresses IP virtuelles. L'adresse IP et le masque réseau doivent être entrés conformément à la notation CIDR (Classless Inter-Domain Routing). Par exemple : 192.0.2.96/24.<br>Si vous activez ce paramètre de stratégie, l'adresse IP et le masque réseau spécifiés sont utilisés pour sélectionner l'adaptateur réseau employé pour les adresses IP virtuelles.<br>Si vous désactivez ou si vous ne configurez pas ce paramètre de stratégie, la virtualisation IP des services Bureau à distance est désactivée. Un adaptateur réseau doit être configuré pour que la virtualisation IP des services Bureau à distance fonctionne. |
| `Do not use Remote Desktop Session Host server IP address when virtual IP address is not available` | Ce paramètre de stratégie spécifie si une session utilise l'adresse IP du serveur Hôte de session Bureau à distance si aucune adresse IP virtuelle n'est disponible.<br>Si vous activez ce paramètre de stratégie, l'adresse IP du serveur Hôte de session Bureau à distance n'est pas utilisée si aucune adresse IP virtuelle n'est disponible. La session ne disposera pas de connectivité réseau.<br>Si vous désactivez ou si vous ne configurez pas ce paramètre de stratégie, l'adresse IP du serveur Hôte de session Bureau à distance est utilisée si aucune adresse IP virtuelle n'est disponible. |

## Paramètres de connexion RDS

Le paramètre de stratégie de groupe Connexions RDS vous permet de désactiver la planification de la répartition de charge équilibrée du temps processeur.

**Tableau 17-13.** Paramètres de la stratégie de groupe Connexions RDS

| Paramètre | Description |
|---|---|
| `Turn off Fair Share CPU Scheduling` | La planification de répartition de charge équilibrée du temps processeur distribue dynamiquement le temps processeur entre toutes les sessions de services Bureau à distance sur le même serveur d'hôtes RDS, en fonction du nombre de sessions et de la demande de temps processeur dans chaque session.<br>Si vous activez ce paramètre de stratégie, la planification de répartition de charge équilibrée du temps processeur est désactivée.<br>Si vous désactivez ou ne configurez pas ce paramètre de stratégie, la planification de répartition de charge équilibrée du temps processeur est activée. |

## Paramètres de redirection de ressources et de périphériques RDS

Les paramètres de stratégie de groupe de redirection des ressources et des périphériques RDS contrôlent l'accès aux périphériques et aux ressources sur un ordinateur client dans des sessions des services Bureau à distance.

**Tableau 17-14.** Paramètres de stratégie de groupe de redirection des ressources et des périphériques RDS

| Paramètre | Description |
|---|---|
| `Allow time zone redirection` | Ce paramètre de stratégie détermine si l'ordinateur client redirige ses paramètres de fuseau horaire vers la session des services Bureau à distance.<br>Si vous activez ce paramètre de stratégie, les clients capables de rediriger un fuseau horaire envoient leurs informations de fuseau horaire au serveur. L'heure de base du serveur est alors utilisée pour calculer l'heure de la session actuelle (heure de la session actuelle = heure de base du serveur + fuseau horaire du client).<br>Si vous désactivez ou ne configurez pas ce paramètre de stratégie, l'ordinateur client ne redirige pas ses informations de fuseau horaire et le fuseau horaire de la session est identique à celui du serveur. |

## Paramètres d'attribution de licence RDS

Les paramètres de stratégie de groupe Licences RDS contrôlent l'ordre dans lequel les serveurs de licences RDS sont localisés, si des notifications de problèmes s'affichent et si des licences par utilisateur ou par périphérique sont utilisées pour les licences d'accès client RDS.

**Tableau 17-15.** Paramètre de stratégie de groupe de licences RDS

| Paramètre | Description |
|---|---|
| `Use the specified Remote Desktop license servers` | Ce paramètre de stratégie vous permet de spécifier l'ordre dans lequel un serveur Hôte de session Bureau à distance tente de localiser les serveurs de licences des services Bureau à distance.<br>Si vous activez ce paramètre de stratégie, un serveur Hôte de session Bureau à distance tente d'abord de localiser les serveurs de licences que vous spécifiez. Si les serveurs de licences spécifiés ne peuvent pas être localisés, le serveur Hôte de session Bureau à distance tentera une découverte de serveurs de licences automatique.<br>Dans le processus de découverte de serveurs de licences automatique, un serveur Hôte de session Bureau à distance dans un domaine basé sur Windows Server tente de contacter un serveur de licences dans l'ordre suivant :<br>1 Serveurs de licences qui sont spécifiés dans l'outil Configuration d'hôte de session Bureau à distance<br>2 Serveurs de licences qui sont publiés dans les Services de domaine Active Directory<br>3 Serveurs de licences qui sont installés sur des contrôleurs de domaine dans le même domaine que le serveur Hôte de session Bureau à distance<br>Si vous désactivez ou ne configurez pas ce paramètre de stratégie, le serveur Hôte de session Bureau à distance utilise le mode de découverte de serveurs de licences spécifié dans l'outil Configuration d'hôte de session Bureau à distance. |
| `Hide notifications about RD Licensing problems that affect the RD Session Host server` | Ce paramètre de stratégie détermine si des notifications s'affichent sur un serveur Hôte de session Bureau à distance en présence de problèmes avec les licences RD qui affectent le serveur Hôte de session Bureau à distance.<br>Par défaut, des notifications s'affichent sur un serveur Hôte de session Bureau à distance après que vous avez ouvert une session en tant qu'administrateur local si des problèmes concernant les licences RD affectent le serveur Hôte de session Bureau à distance. Le cas échéant, une notification s'affiche également pour indiquer le nombre de jours qu'il reste avant l'expiration de la période de grâce des licences pour le serveur Hôte de session Bureau à distance.<br>Si vous activez ce paramètre de stratégie, ces notifications ne s'afficheront pas sur le serveur Hôte de session Bureau à distance.<br>Si vous désactivez ou ne configurez pas ce paramètre de stratégie, ces notifications s'afficheront sur le serveur Hôte de session Bureau à distance après que vous avez ouvert une session en tant qu'administrateur local. |
| `Set the Remote Desktop licensing mode` | Ce paramètre de stratégie vous permet de spécifier le type de licence d'accès client aux services Bureau à distance Services requis pour se connecter à ce serveur Hôte de session Bureau à distance.<br>Vous pouvez utiliser ce paramètre de stratégie pour sélectionner l'un des deux modes de licence : par utilisateur ou par périphérique. |

**Tableau 17-15.** Paramètre de stratégie de groupe de licences RDS (suite)

| Paramètre | Description |
|---|---|
| | Le mode de licence par utilisateur impose que chaque compte d'utilisateur se connectant à ce serveur Hôte de session Bureau à distance dispose d'une licence d'accès utilisateur des services Bureau à distance par utilisateur.<br>Le mode de licence par périphérique impose que chaque périphérique se connectant à ce serveur Hôte de session Bureau à distance dispose d'une licence d'accès utilisateur des services Bureau à distance par périphérique.<br>Si vous activez ce paramètre de stratégie, le mode de licence que vous spécifiez a priorité sur le mode de licence qui est spécifié lors de l'installation de l'Hôte de session Bureau à distance ou spécifié dans l'outil Configuration d'hôte de session Bureau à distance.<br>Si vous désactivez ou ne configurez pas ce paramètre de stratégie, le mode de licence qui est spécifié lors de l'installation du service de rôle Hôte de session Bureau à distance ou spécifié dans l'outil Configuration d'hôte de session Bureau à distance est utilisé. |

## Paramètres de profils RDS

Les paramètres de stratégie de groupe des profils RDS contrôlent les paramètres de profil itinérant et de répertoire de base des sessions des services Bureau à distance.

**Tableau 17-16.** Paramètres de stratégie de groupe des profils RDS

| Paramètre | Description |
|---|---|
| `Limit the size of the entire roaming user profile cache` | Ce paramètre de stratégie vous permet de limiter la taille de l'ensemble du cache de profils d'utilisateur itinérant sur le disque local. Il s'applique uniquement à un ordinateur sur lequel le service du rôle Hôte de session Bureau à distance est installé.<br>**Remarque** Si vous souhaitez limiter la taille d'un profil d'utilisateur individuel, utilisez le paramètre de stratégie `Limiter la taille du profil` situé dans **Configuration utilisateur\Stratégies\Modèles d'administration\Système\Profils d'utilisateur**.<br>Si vous activez ce paramètre de stratégie, vous devez spécifier un intervalle de surveillance (en minutes) et une taille maximale (en giga-octets) pour l'ensemble du cache de profils d'utilisateur itinérant. L'intervalle de surveillance détermine la fréquence de vérification de la taille de l'ensemble du cache de profils d'utilisateur itinérant. Lorsque la taille de l'ensemble du cache de profils d'utilisateur itinérant dépasse la taille maximale que vous avez spécifiée, les profils d'utilisateur itinérant les plus anciens (utilisés le moins récemment) sont supprimés jusqu'à ce que la taille de l'ensemble du cache de profils d'utilisateur itinérant soit inférieure à la taille maximale spécifiée.<br>Si vous désactivez ou si vous ne configurez pas ce paramètre de stratégie, aucune limitation n'est imposée à la taille de l'ensemble du cache de profils d'utilisateur itinérant sur le lecteur local.<br>Remarque : ce paramètre de stratégie est ignoré si le paramètre de stratégie `Empêcher la propagation des modifications de profils itinérants vers le serveur` situé dans **Configuration de l'ordinateur\Stratégies\Modèles d'administration\Système\Profils d'utilisateur** est activé. |
| `Set Remote Desktop Services User Home Directory` | Spécifie si les services Bureau à distance utilisent le partage réseau spécifié ou un chemin de répertoire local en tant que racine du répertoire de base de l'utilisateur pour une session des services Bureau à distance.<br>Pour utiliser ce paramètre, sélectionnez l'emplacement du répertoire de base (réseau ou local) dans la liste déroulante Emplacement. Si vous choisissez de placer le répertoire sur un partage réseau, tapez le chemin racine du répertoire de base sous la forme `\\NomOrdinateur\NomPartage`, puis sélectionnez la lettre du lecteur auquel vous souhaitez mapper le partage réseau. |

**Tableau 17-16.** Paramètres de stratégie de groupe des profils RDS (suite)

| Paramètre | Description |
|---|---|
| | Si vous choisissez de conserver le répertoire de base sur l'ordinateur local, tapez le chemin d'accès racine au répertoire de base sous la forme `Lecteur:\Chemin`, sans variables d'environnement, ni ellipses. Ne spécifiez pas d'espace réservé pour l'alias de l'utilisateur, car les services Bureau à distance l'ajoutent automatiquement à l'ouverture de session.<br>**Remarque** Le champ Lettre du lecteur est ignoré si vous choisissez de spécifier un chemin local. Si vous choisissez de spécifier un chemin local, mais que vous tapez ensuite le nom d'un partage réseau dans le chemin d'accès racine au répertoire de base, les services Bureau à distance placent les répertoires de base des utilisateurs dans l'emplacement réseau.<br>Si l'état est défini sur Activé, les services Bureau à distance créent le répertoire de base de l'utilisateur dans l'emplacement spécifié sur l'ordinateur local ou le réseau. Le chemin d'accès au répertoire de base de chaque utilisateur correspond au chemin d'accès racine au répertoire de base et à l'alias de l'utilisateur.<br>Si l'état est défini sur Désactivé ou Non configuré, le répertoire de base de l'utilisateur est celui qui est spécifié au niveau du serveur. |

**Tableau 17-16.** Paramètres de stratégie de groupe des profils RDS (suite)

| Paramètre | Description |
|---|---|
| `Use mandatory profiles on the RD Session Host server` | Ce paramètre de stratégie vous permet de spécifier si les services Bureau à distance utilisent un profil obligatoire pour tous les utilisateurs se connectant à distance au serveur Hôte de session RDS.<br>Si vous activez ce paramètre de stratégie, les services Bureau à distance utilisent le chemin d'accès spécifié dans le paramètre de stratégie `Définir le chemin d'accès au profil d'utilisateur itinérant des services Bureau à distance` en tant que dossier racine du profil d'utilisateur obligatoire. Tous les utilisateurs se connectant à distance au serveur Hôte de session RDS utilisent le même profil d'utilisateur.<br>Si vous désactivez ou si vous ne configurez pas ce paramètre de stratégie, les profils utilisateurs obligatoires sont pas utilisés par les utilisateurs qui se connectent à distance au serveur Hôte de session Bureau à distance.<br>**Remarque** Pour que ce paramètre de stratégie entre en vigueur, vous devez également activer et configurer le paramètre de stratégie `Définir le chemin d'accès au profil d'utilisateur itinérant des services Bureau à distance`. |
| `Set path for Remote Desktop Services Roaming User Profile` | Ce paramètre de stratégie vous permet de spécifier le chemin d'accès réseau que les services Bureau à distance utilisent pour les profils d'utilisateur itinérant.<br>Par défaut, les services Bureau à distance stockent tous les profils d'utilisateur localement sur le serveur Hôte de session RDS. Vous pouvez utiliser ce paramètre de stratégie pour spécifier un partage réseau sur lequel les profils d'utilisateur peuvent être centralisés, ce qui permet aux utilisateurs d'accéder au même profil lors de sessions sur tous les serveurs Hôtes de session RDS configurés pour utiliser le partage réseau pour les profils d'utilisateur.<br>Si vous activez ce paramètre de stratégie, les services Bureau à distance utilisent le chemin d'accès spécifié en tant que répertoire de base pour tous les profils utilisateurs. Les profils sont situés dans des sous-dossiers portant le nom de compte de chaque utilisateur.<br>Pour configurer ce paramètre de stratégie, tapez le chemin d'accès au partage réseau sous la forme `\\NomOrdinateur\NomPartage`. Ne spécifiez pas d'espace réservé pour le nom de compte de l'utilisateur, car les services Bureau à distance l'ajoutent automatiquement lors de l'ouverture de session de l'utilisateur et de la création du profil. Si le partage réseau spécifié n'existe pas, les services Bureau à distance affichent un message d'erreur sur le serveur Hôte de session RDS et stockent les profils d'utilisateur localement sur ce serveur.<br>Si vous désactivez ou si vous ne configurez pas ce paramètre de stratégie, les profils d'utilisateur sont stockés localement sur le serveur Hôte de session RDS. Vous pouvez configurer le chemin d'accès au profil d'un utilisateur dans l'onglet Profil des services Bureau à distance de la boîte de dialogue Propriétés du compte de l'utilisateur. |

**Tableau 17-16.** Paramètres de stratégie de groupe des profils RDS (suite)

| Paramètre | Description |
|---|---|
| | Remarques :<br>1 Les profils utilisateurs itinérants activés par le paramètre de stratégie s'appliquent uniquement aux connexions des services Bureau à distance. Un utilisateur peut également posséder un profil d'utilisateur itinérant Windows configuré. Le profil d'utilisateur itinérant des services Bureau à distance est toujours prioritaire dans une session des services Bureau à distance.<br>2 Pour configurer un profil d'utilisateur itinérant des services Bureau à distance obligatoire pour tous les utilisateurs se connectant à distance au serveur Hôte de session RDS, utilisez ce paramètre de stratégie conjointement au paramètre de stratégie `Utiliser les profils obligatoires sur le serveur Hôte de la session Bureau à distance` situé dans **Configuration ordinateur\Modèles d'administration\Composants Windows\Services Bureau à distance\Hôte session Bureau à distance\Profils**. Le chemin d'accès défini dans le paramètre de stratégie `Définir le chemin d'accès au profil d'utilisateur itinérant des services Bureau à distance` doit contenir le profil obligatoire. |

## Paramètres d'environnement de session distante RDS

La stratégie de groupe Environnement de session distante RDS contrôle la configuration de l'interface utilisateur dans les sessions RDS.

**Tableau 17-17.** Paramètres de la stratégie de groupe de l'environnement de session distante RDS

| Paramètre | Description |
|---|---|
| `Remove Windows Security item from Start menu` | Spécifie s'il convient de supprimer l'élément Sécurité de Windows du menu Paramètres sur les clients Bureau à distance. Vous pouvez utiliser ce paramètre pour empêcher les utilisateurs inexpérimentés de se déconnecter accidentellement des services Bureau à distance.<br>Si l'état est défini sur Activé, Sécurité de Windows ne s'affiche pas sous Paramètres dans le menu Démarrer. Par conséquent, les utilisateurs doivent taper une séquence d'attention de sécurité, telle que CTRL+ALT+FIN, pour ouvrir la boîte de dialogue Sécurité de Windows sur l'ordinateur client.<br>Si l'état est défini sur Désactivé ou Non configuré, Sécurité de Windows figure toujours dans le menu Paramètre. |

## Paramètres de sécurité RDS

Le paramètre de stratégie de groupe de sécurité RDS contrôle si les administrateurs locaux peuvent personnaliser les autorisations.

**Tableau 17-18.** Paramètres de la stratégie de groupe de sécurité RDS

| Paramètre | Description |
|---|---|
| `Do not allow local administrators to customize permissions` | Spécifie si vous devez désactiver les droits de l'administrateur à personnaliser des autorisations de sécurité dans l'outil de configuration de l'hôte RDS.<br>Vous pouvez utiliser ce paramètre pour empêcher les administrateurs d'apporter des changements aux groupes d'utilisateurs sur l'onglet Autorisations de l'outil de configuration de l'hôte de session Bureau à distance. Par défaut, les administrateurs peuvent apporter ces changements.<br>Si l'état est défini sur Activé, l'onglet Autorisations de l'outil de configuration de l'hôte de session Bureau à distance ne peut pas servir à personnaliser les descripteurs de sécurité par connexion ou à modifier les descripteurs de sécurité par défaut d'un groupe existant. Tous les descripteurs de sécurité sont en lecture seule.<br>Si l'état est défini sur Désactivé ou Non configuré, les administrateurs du serveur disposent de privilèges de lecture/écriture complets sur les descripteurs de sécurité de l'utilisateur de l'onglet Autorisations dans l'outil de configuration de l'hôte de session Bureau à distance.<br>**Remarque** Le mode de gestion préféré de l'accès utilisateur consiste à ajouter un utilisateur au groupe Utilisateurs de poste de travail distant. |

## Paramètres de dossiers temporaires RDS

Les paramètres de stratégie du groupe Connexion RDS contrôlent la création et la suppression de dossiers temporaires pour les sessions des services Bureau à distance.

**Tableau 17-19.** Paramètres de stratégie de groupe de dossiers temporaires

| Paramètre | Description |
|---|---|
| `Do not delete temp folder upon exit` | Spécifie si les services Bureau à distance conservent les dossiers temporaires par session d'un utilisateur à la fermeture de la session.<br>Vous pouvez utiliser ce paramètre pour conserver les dossier temporaires spécifiques à la session d'un utilisateur, même si celui-ci ferme une session. Par défaut, les services Bureau à distance suppriment les dossiers temporaires d'un utilisateur quand celui-ci se déconnecte.<br>Si l'état est défini sur Activé, les dossiers temporaires par session de l'utilisateur sont conservés lorsque celui ferme une session.<br>Si l'état est défini sur Désactivé, les dossiers temporaires sont supprimés lorsqu'un utilisateur se déconnecte, même si l'administrateur spécifie autre chose dans l'outil Configuration de l'hôte de session Bureau à distance.<br>Si l'état est défini sur Non configuré, les services Bureau à distance suppriment les dossiers temporaires de l'ordinateur distant à la fermeture de la session, sauf si l'administrateur du serveur a spécifié autre chose.<br>**Remarque** Ce paramètre n'est appliqué que si les dossiers temporaires par session sont utilisés sur le serveur. Cela signifie que si vous activez le paramètre « Ne pas utiliser les dossiers temporaires par session », celui-ci n'est pas appliqué. |
| `Do not use temporary folders per session` | Ce paramètre vous permet d'empêcher les services Bureau à distance de créer des dossiers temporaires spécifiques à la session.<br>Vous pouvez utiliser ce paramètre de stratégie pour désactiver la création de dossiers temporaires distincts sur un ordinateur distant pour chaque session. Par défaut, les services Bureau à distance créent un dossier temporaire distinct pour chaque session active qu'un utilisateur conserve sur un ordinateur distant. Ces dossiers temporaires sont créés sur l'ordinateur distant dans un dossier Temp situé dans le dossier du profil de l'utilisateur et portent le nom de `sessionid`.<br>Si vous activez ce paramètre de stratégie, les dossiers temporaires par session ne sont pas créés. À la place, les dossiers temporaires de toutes les sessions d'un utilisateur sur l'ordinateur distant sont stockés dans un dossier Temp commun dans le dossier du profil de l'utilisateur sur l'ordinateur distant.<br>Si vous désactivez ce paramètre de stratégie, les dossiers temporaires par session sont toujours créés, même si vous spécifiez autre chose dans l'outil Configuration de l'hôte de session Bureau à distance.<br>Si vous ne configurez pas ce paramètre de stratégie, les dossiers temporaires par session sont toujours créés, sauf si vous spécifiez autre chose dans l'outil Configuration de l'hôte de session Bureau à distance. |

## Configuration de l'impression basée sur l'emplacement

La fonction d'impression basée sur l'emplacement mappe les imprimantes physiquement proches des systèmes client vers des postes de travail View, ce qui permet aux utilisateurs d'imprimer sur leurs imprimantes locales et en réseau depuis leurs postes de travail View.

L'impression basée sur l'emplacement permet aux services informatiques de mapper des postes de travail View vers l'imprimante la plus proche du périphérique client de point de terminaison. Par exemple, lorsqu'un médecin passe de chambre en chambre dans un hôpital, chaque fois qu'il imprime un document, le travail d'impression est envoyé à l'imprimante la plus proche.

La fonctionnalité d'impression basée sur l'emplacement est disponible pour Windows, Mac OS X, Linux, et pour les périphériques clients mobiles.

Dans Horizon 6.0.1 et version ultérieure, l'impression basée sur l'emplacement est prise en charge sur les applications et les postes de travail distants suivants :

- Postes de travail qui sont déployés sur des machines mono-utilisateur, notamment les machines postes de travail Windows et Windows Server
- Postes de travail qui sont déployées sur des hôtes RDS, où les hôtes RDS sont des machines virtuelles
- applications hébergées ;
- Applications hébergées qui sont lancées à partir d'Horizon Client à l'intérieur de postes de travail distants

Dans Horizon 6.0 et version antérieure, l'impression basée sur l'emplacement est prise en charge sur les postes de travail qui sont déployés sur des machines postes de travail Windows mono-utilisateur.

Pour utiliser la fonctionnalité d'impression basée sur l'emplacement, vous devez installer l'option de configuration Impression virtuelle avec Horizon Agent et les pilotes d'imprimante correspondants sur le poste de travail.

Vous réglez l'impression basée sur l'emplacement en configurant le paramètre de stratégie de groupe Active Directory `AutoConnect Map Additional Printers for VMware View`, situé dans l'Éditeur d'objets de stratégie de groupe de Microsoft dans le dossier **Paramètres du logiciel** sous **Configuration ordinateur**.

---

**Remarque** `AutoConnect Map Additional Printers for VMware View` est une stratégie spécifique à l'ordinateur. Les stratégies spécifiques à l'ordinateur s'appliquent à tous les postes de travail View, quelle que soit la personne se connectant au poste de travail.

---

`AutoConnect Map Additional Printers for VMware View` est un tableau de traduction de noms. Vous utilisez chaque ligne du tableau pour identifier une imprimante spécifique et définir un ensemble de règles de traduction pour cette imprimante. Les règles de traduction déterminent si l'imprimante est mappée vers le poste de travail View pour un système client particulier.

Lorsqu'un utilisateur se connecte à un poste de travail View, View compare le système client avec les règles de traduction associées à chaque imprimante du tableau. Si le système client satisfait toutes les règles de traduction définies pour l'imprimante, ou si une imprimante n'a pas de règle de traduction associée, View mappe l'imprimante vers le poste de travail View au cours de la session de l'utilisateur.

Vous pouvez définir des règles de traduction basées sur l'adresse IP, le nom et l'adresse MAC du système client, et sur le nom et le groupe de l'utilisateur. Vous pouvez spécifier une règle de traduction, ou une combinaison de plusieurs règles de traduction, pour une imprimante spécifique.

Les informations utilisées pour mapper l'imprimante vers le poste de travail View sont stockées dans une entrée de registre sur le poste de travail View dans `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\thinprint\tpautoconnect`.

## Paramètres d'imprimante pour impression basée sur l'emplacement

Dans Horizon 6.0.2 et versions ultérieures, les réglages d'imprimante des imprimantes basées sur l'emplacement sont conservés après la déconnexion des utilisateurs de leur poste de travail. Par exemple, un utilisateur peut choisir d'utiliser une imprimante basée sur l'emplacement en mode monochrome. Après que l'utilisateur se déconnecte et reconnecte au poste de travail, l'imprimante basée sur l'emplacement continue de fonctionner en mode monochrome.

Pour enregistrer les paramètres de l'imprimante à travers les sessions dans une application hébergée, l'utilisateur doit sélectionner une imprimante basée sur l'emplacement dans la boîte de dialogue d'impression de l'application, cliquer avec le bouton droit sur l'imprimante sélectionnée, puis sélectionner **Préférences d'impression**. Les paramètres de l'imprimante ne sont pas enregistrés si l'utilisateur sélectionne une imprimante et clique sur le bouton **Préférences** dans la boîte de dialogue d'impression de l'application.

Les paramètres persistants d'imprimantes basées sur l'emplacement ne sont pas pris en charge si les paramètres sont enregistrés dans l'espace privé du pilote plutôt que dans sa partie étendue DEVMODE, comme le recommande Microsoft. Pour prendre en charge les paramètres persistants, déployez les imprimantes dont les paramètres sont enregistrés dans la partie DEVMODE du pilote de l'imprimante.

## Enregistrer le fichier DLL de la stratégie de groupe de l'impression basée sur l'emplacement

Avant de pouvoir configurer le paramètre de stratégie de groupe pour l'impression basée sur l'emplacement, vous devez enregistrer le fichier DLL `TPVMGPoACmap.dll`.

Les versions 32 bits et 64 bits de `TPVMGPoACmap.dll` sont disponibles dans un fichier `.zip` groupé nommé `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip`, où *x.x.x* est la version et *yyyyyyy* le numéro de build. Vous pouvez télécharger le fichier sur le site de téléchargement de VMware Horizon 6 à l'adresse http://www.vmware.com/go/downloadview.

Les versions de View antérieures fournissent les versions 32 bits et 64 bits de `TPVMGPoACmap.dll` dans le répertoire *`install_directory`*`\VMware\VMware View\Server\extras\GroupPolicyFiles\ThinPrint` sur votre hôte du Serveur de connexion View.

### Procédure

1 Copiez la version appropriée de `TPVMGPoACmap.dll` sur votre serveur Active Directory ou sur l'ordinateur de domaine que vous utilisez pour configurer des stratégies de groupe.

2 Utilisez l'utilitaire `regsvr32` pour enregistrer le fichier `TPVMGPoACmap.dll`.

   Par exemple : `regsvr32 "C:\TPVMGPoACmap.dll"`

### Suivant

Configurez le paramètre de stratégie de groupe pour l'impression basée sur l'emplacement.

## Configurer la stratégie de groupe de l'impression basée sur l'emplacement

Pour régler l'impression basée sur l'emplacement, vous configurez le paramètre de stratégie de groupe `AutoConnect Map Additional Printers for VMware View`. Le paramètre de stratégie de groupe est un tableau de traduction de noms qui mappe des imprimantes vers des postes de travail View.

### Prérequis

- Vérifiez que les composants logiciels enfichables Microsoft MMC et que l'Éditeur d'objets de stratégie de groupe sont disponibles sur votre serveur Active Directory ou sur l'ordinateur de domaine que vous utilisez pour configurer des stratégies de groupe.

- Enregistrez le fichier DLL `TPVMGPoACmap.dll` sur votre serveur Active Directory ou sur l'ordinateur de domaine que vous utilisez pour configurer des stratégies de groupe. Reportez-vous à la section « Enregistrer le fichier DLL de la stratégie de groupe de l'impression basée sur l'emplacement », page 344.
- Familiarisez-vous avec la syntaxe du paramètre de stratégie de groupe `AutoConnect Map Additional Printers for VMware View`. Reportez-vous à la section « Syntaxe de paramètre de stratégie de groupe de l'impression basée sur l'emplacement », page 346.
- Créez un GPO pour le paramètre de stratégie de groupe basé sur l'emplacement et liez-le à l'UO qui contient vos postes de travail View. Reportez-vous à « Créer des GPO pour les stratégies de groupe View », page 348 pour obtenir un exemple de création de GPO pour des stratégies de groupe View.
- Vérifiez que l'option de configuration Impression virtuelle a été installée avec Horizon Agent sur vos postes de travail. Pour cela, vérifiez si les services TP AutoConnect et TP VC Gateway sont installés sur le système d'exploitation du poste de travail.
- Comme les travaux d'impression sont envoyés directement du poste de travail View vers l'imprimante, vérifiez que les pilotes d'imprimante requis sont installés sur vos postes de travail.

### Procédure

1 Sur le serveur Active Directory, modifiez les GPO.

| Version d'AD | Chemin de navigation |
|---|---|
| **Windows 2003** | a Sélectionnez **Démarrer > Tous les programmes > Outils d'administration > Utilisateurs et ordinateurs Active Directory**.<br>b Cliquez avec le bouton droit sur l'UO qui contient vos postes de travail View et sélectionnez **Propriétés**.<br>c Sous l'onglet **Stratégie de groupe**, cliquez sur **Ouvrir** pour ouvrir le plug-in Gestion de stratégie de groupe.<br>d Dans le volet de droite, cliquez avec le bouton droit sur le GPO que vous avez créé pour le paramètre de stratégie de groupe d'impression basée sur l'emplacement et sélectionnez **Modifier**. |
| **Windows 2008** | a Sélectionnez **Démarrer > Outils d'administration > Gestion de stratégie de groupe**.<br>b Développez votre domaine, cliquez avec le bouton droit sur le GPO que vous avez créé pour le paramètre de stratégie de groupe d'impression basée sur l'emplacement et sélectionnez **Modifier**. |

La fenêtre de l'Éditeur d'objets de stratégie de groupe apparaît.

2 Développez **Configuration ordinateur**, ouvrez le dossier **Paramètres du logiciel** et sélectionnez **Imprimantes supplémentaires de mappage de connexion automatique pour VMware View**.

3 Dans le volet Règle, double-cliquez sur **Configurer des imprimantes supplémentaires de mappage de connexion automatique**.

La fenêtre AutoConnect Map Additional Printers for VMware View (Imprimantes supplémentaires de mappage de connexion automatique pour VMware View) apparaît.

4 Sélectionnez **Activé** pour activer le paramètre de stratégie de groupe.

Les titres et les boutons du tableau de traduction apparaissent dans la fenêtre de stratégie de groupe.

**Important** Cliquer sur **Désactivé** supprime toutes les entrées du tableau. Par précaution, enregistrez votre configuration pour pouvoir l'importer ultérieurement.

5 Ajoutez les imprimantes que vous voulez mapper vers des postes de travail View et définissez leurs règles de traduction associées.

6 Cliquez sur **OK** pour enregistrer vos modifications.

## Syntaxe de paramètre de stratégie de groupe de l'impression basée sur l'emplacement

Vous utilisez le paramètre de stratégie de groupe `AutoConnect Map Additional Printers for VMware View` pour mapper des imprimantes à des postes de travail distants.

`AutoConnect Map Additional Printers for VMware View` est une table de traductions de noms qui identifie des imprimantes et définit les règles de traduction associées. Tableau 17-20 décrit la syntaxe de la table de traductions.

L'impression basée sur l'emplacement mappe les imprimantes locales à des postes de travail distants, mais ne prend pas en charge le mappage d'imprimantes réseau qui sont configurées à l'aide de chemins UNC.

**Tableau 17-20.** Colonnes et valeurs contenues dans le tableau de traduction

| Colonne | Description |
|---|---|
| `IP Range` | Règle de traduction spécifiant une plage d'adresses IP pour des systèmes client.<br>Pour spécifier des adresses IP dans une plage spécifique, utilisez la notation suivante :<br>***ip_address–ip_address***<br>Par exemple : **`10.112.116.0–10.112.119.255`**<br>Pour spécifier toutes les adresses IP dans un sous-réseau spécifique, utilisez la notation suivante :<br>*ip_address/subnet_mask_bits*<br>Par exemple : **`10.112.4.0/22`**<br>Cette notation spécifie les adresses IPv4 utilisables comprises entre 10.112.4.1 et 10.112.7.254.<br>Saisissez un astérisque pour inclure toutes les adresses IP. |
| `Client Name` | Règle de traduction spécifiant un nom d'ordinateur.<br>Par exemple : **`Ordinateur de Marie`**<br>Saisissez un astérisque pour inclure tous les noms d'ordinateur. |
| `Mac Address` | Règle de traduction spécifiant une adresse MAC. Dans l'éditeur de GPO, vous devez voir le même format que celui utilisé par le système client. Par exemple :<br>■ Les clients Windows utilisent des traits d'union : **`01–23–45–67–89–ab`**<br>■ Les clients Linux utilisent des deux-points : **`01:23:45:67:89:ab`**<br>Saisissez un astérisque pour inclure toutes les adresses MAC. |
| `User/Group` | Règle de traduction spécifiant un nom d'utilisateur ou de groupe.<br>Pour spécifier un utilisateur ou un groupe particulier, utilisez la notation suivante :<br>*\\domain\user_or_group*<br>Par exemple : **`\\mondomaine\Marie`**<br>Le nom de domaine complet n'est pas une notation prise en charge pour le nom de domaine. Tapez un astérisque pour inclure tous les noms d'utilisateurs ou de groupes. |
| `Printer Name` | Nom de l'imprimante lorsqu'elle est mappée au poste de travail distant.<br>Par exemple : **`PRINTER–2–CLR`**<br>Le nom mappé n'a pas à correspondre au nom de l'imprimante sur le système client.<br>L'imprimante doit être locale par rapport au périphérique client. Le mappage d'une imprimante réseau dans un chemin UNC n'est pas pris en charge. |

**Tableau 17-20.** Colonnes et valeurs contenues dans le tableau de traduction (suite)

| Colonne | Description |
|---|---|
| `Printer Driver` | Nom du pilote qu'utilise l'imprimante.<br>Par exemple : **`HP Color LaserJet 4700 PS`**<br>**Important** Comme les travaux d'impression sont envoyés directement du poste de travail vers l'imprimante, le pilote d'imprimante doit être installé sur le poste de travail. |
| `IP Port/ThinPrint Port` | Pour les imprimantes en réseau, adresses IP de l'imprimante avec le préfixe **`IP_`**.<br>Par exemple : **`IP_10.114.24.1`**<br>Le port par défaut est 9100. Vous pouvez spécifier un port différent du port par défaut en ajoutant le numéro de port à l'adresse IP.<br>Par exemple : **`IP_10.114.24.1:9104`** |
| `Default` | Indique si l'imprimante est l'imprimante par défaut. |

Vous utilisez les boutons qui apparaissent au-dessus des titres de colonne pour ajouter, supprimer et déplacer des lignes et pour enregistrer et importer des entrées de tableau. Chaque bouton a un raccourci clavier équivalent. Passez la souris sur chaque bouton pour en voir une description et son raccourci clavier. Par exemple, pour insérer une ligne à la fin du tableau, cliquez sur le premier bouton du tableau ou appuyez sur Alt+A. Cliquez sur les deux derniers boutons pour importer et enregistrer des entrées de tableau.

Tableau 17-21 montre un exemple de deux lignes de tableau de traduction.

**Tableau 17-21.** Exemple de paramètre de stratégie de groupe de l'impression basée sur l'emplacement

| Plage IP | Nom du client | Adresse Mac | Utilisateur/ Groupe | Nom de l'imprimante | Pilote d'imprimante | IP Port/ThinPrint Port (Port IP/Port ThinPrint) | Valeur par défaut |
|---|---|---|---|---|---|---|---|
| * | * | * | * | PRINTER-1-CLR | HP Color LaserJet 4700 PS | IP_10.114.24.1 | |
| 10.112.116.140-10.112.116.145 | * | * | * | PRINTER-2-CLR | HP Color LaserJet 4700 PS | IP_10.114.24.2 | X |

L'imprimante réseau spécifiée sur la première ligne sera mappée à un poste de travail distant de n'importe quel système client, car des astérisques figurent dans toutes les colonnes de la règle de traduction. L'imprimante réseau spécifiée sur la deuxième ligne sera mappée à un poste de travail distant uniquement si l'adresse IP du système client est comprise dans la plage 10.112.116.140 à 10.112.116.145.

# Exemple de stratégie de groupe Active Directory

L'une des méthodes de mise en œuvre des stratégies de groupe Active Directory dans View consiste à créer une unité d'organisation (UO) pour les machines View qui fournissent des sessions de postes de travail distants et à lier un ou plusieurs objets de stratégie de groupe (GPO) à cette UO. Vous pouvez utiliser ces GPO pour appliquer des paramètres de stratégie de groupe à vos machines View.

Vous pouvez lier les GPO directement à un domaine si les paramètres de stratégie s'appliquent à tous les ordinateurs du domaine. Pour la plupart des déploiements, nous recommandons toutefois de lier des GPO à des UO individuelles, afin d'éviter le traitement de la stratégie sur tous les ordinateurs du domaine.

Vous pouvez configurer des stratégies sur votre serveur Active Directory ou sur n'importe quel ordinateur de votre domaine. Cet exemple montre comment configurer des stratégies directement sur votre serveur Active Directory.

**Remarque** Chaque environnement View étant différent, il vous faudra peut-être effectuer différentes étapes pour répondre aux besoins spécifiques de votre organisation.

## Créer une unité d'organisation (UO) pour des machines View

Pour appliquer des stratégies de groupe aux machines View qui fournissent des sessions de poste de travail distant sans affecter d'autres ordinateurs Windows du même domaine Active Directory, vous devez créer une UO propre à vos machines View. Vous pouvez créer une UO pour l'ensemble de votre déploiement de View ou des UO distinctes pour des machines mono-utilisateur et des hôtes RDS.

### Procédure

1. Sur votre serveur Active Directory, sélectionnez **Démarrer > Tous les programmes > Outils d'administration > Utilisateurs et ordinateurs Active Directory**.
2. Cliquez avec le bouton droit sur le domaine qui contient vos machines View et sélectionnez **Nouveau > Unité d'organisation**.
3. Saisissez un nom pour l'UO et cliquez sur **OK**.

   La nouvelle UO apparaît dans le volet de gauche.
4. Pour ajouter des machines View à la nouvelle UO :
   a. Cliquez sur **Ordinateurs** dans le volet de gauche.

      Tous les objets ordinateur dans le domaine apparaissent dans le volet de droite.
   b. Cliquez avec le bouton droit sur le nom de l'objet ordinateur qui représente la machine View dans le volet de droite et sélectionnez **Déplacer**.
   c. Sélectionnez l'UO et cliquez sur **OK**.

      La machine View s'affiche dans le volet de droite lorsque vous sélectionnez l'UO.

### Suivant

Créez des GPO pour les stratégies de groupe View.

## Créer des GPO pour les stratégies de groupe View

Créez des GPO contenant des stratégies de groupe pour des composants View et l'impression basée sur l'emplacement et liez-les à l'unité d'organisation de vos machines View.

### Prérequis

- Créez une unité d'organisation pour vos machines View.
- Vérifiez que la fonctionnalité Gestion de stratégie de groupe est disponible sur votre serveur Active Directory.

### Procédure

1. Sur le serveur Active Directory, ouvrez la Console de gestion de stratégie de groupe.

| Version d'AD | Chemin de navigation |
|---|---|
| **Windows 2012** | Sélectionnez **Server Manager > Tools > Group Policy Management**. |
| **Windows 2008** | Sélectionnez **Start > Administrative Tools > Group Policy Management**. |
| **Windows 2003** | a. Sélectionnez **Démarrer > Tous les programmes > Outils d'administration > Utilisateurs et ordinateurs Active Directory**.<br>b. Cliquez avec le bouton droit sur l'unité d'organisation qui contient vos machines View et sélectionnez **Propriétés**.<br>c. Sous l'onglet **Stratégie de groupe**, cliquez sur **Ouvrir** pour ouvrir le plug-in Gestion de stratégie de groupe. |

2 Développez votre domaine, cliquez avec le bouton droit sur l'unité d'organisation qui contient vos machines View et sélectionnez **Créer un objet GPO dans ce domaine, et le lier ici**.

   Dans Windows 2003 Active Directory, cette option se nomme **Créer et lier un objet GPO ici**.

3 Saisissez un nom pour le GPO et cliquez sur **OK**.

   Le nouveau GPO apparaît sous l'UO dans le volet de gauche.

4 (Facultatif) Pour appliquer le GPO uniquement à des postes de travail View spécifiques de l'unité d'organisation :

   a Sélectionnez le GPO dans le volet de gauche.

   b Sélectionnez **Filtrage de sécurité > Ajouter**.

   c Entrez les noms d'ordinateur des machines View et cliquez sur **OK**.

      Les machines View s'affichent dans le volet Filtrage de sécurité. Les paramètres du GPO ne s'appliquent qu'à ces machines.

### Suivant

Ajoutez les modèles d'administration View au GPO pour des stratégies de groupe.

## Ajouter des modèles d'administration View à un GPO

Pour appliquer des paramètres de stratégie de groupe de composant View à vos postes de travail et applications distants, ajoutez leurs fichiers de modèle d'administration à des GPO.

### Prérequis

- Créez des GPO pour les paramètres de stratégie de groupe du composant View et liez-les à l'UO qui contient vos machines View.
- Vérifiez que la fonctionnalité Gestion de stratégie de groupe est disponible sur votre serveur Active Directory.

  La procédure d'ouverture de la Console de gestion de stratégie de groupe varie entre les versions Windows 2012, Windows 2008 et Windows 2003 d'Active Directory. Reportez-vous à la section « Créer des GPO pour les stratégies de groupe View », page 348.

### Procédure

1 Téléchargez le fichier View GPO Bundle `.zip` sur le site de téléchargement de VMware à l'adresse https://my.vmware.com/web/vmware/downloads.

   Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut GPO Bundle.

   Le fichier se nomme `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip`, où *x.x.x* est la version et *yyyyyyy* le numéro de build. Tous les fichiers ADM et ADMX qui fournissent des paramètres de stratégie de groupe pour View sont disponibles dans ce fichier.

2 Copiez le fichier sur votre serveur Active Directory et décompressez-le.

3 Sur le serveur Active Directory, ouvrez la Console de gestion de stratégie de groupe.

4 Développez votre domaine, cliquez avec le bouton droit sur le GPO que vous avez créé pour les paramètres de stratégie de groupe et sélectionnez **Modifier**.

5 Dans l'Éditeur de gestion de stratégie de groupe, cliquez avec le bouton droit sur le dossier **Configuration de l'ordinateur > Règles > Modèles administratifs : Définitions de stratégies** et sélectionnez **Ajouter/supprimer les modèles**.

6 Cliquez sur **Ajouter**, recherchez le fichier de modèle d'administration et cliquez sur **Ouvrir**.

7 Cliquez sur **Fermer** pour appliquer les paramètres de stratégie dans le fichier de modèle d'administration au GPO.

   Dans Active Directory de Windows Server 2012 ou 2008, le nom du modèle s'affiche dans le volet de gauche sous **Modèles d'administration > Modèles d'administration classiques (ADM)**. Dans Active Directory de Windows Server 2003, le modèle s'affiche sous **Modèles d'administration**.

8 Configurez les paramètres de stratégie de groupe.

### Suivant

Activez le traitement en boucle pour vos machines View.

## Activer le traitement en boucle des postes de travail distants

Pour appliquer des paramètres de Configuration d'utilisateur qui s'appliquent généralement à un ordinateur à tous les utilisateurs qui ouvrent une session sur cet ordinateur, activez le traitement en boucle.

### Prérequis

- Créez des GPO pour les paramètres de stratégie de groupe du composant View et liez-les à l'UO qui contient vos machines View.
- Vérifiez que la fonctionnalité Gestion de stratégie de groupe est disponible sur votre serveur Active Directory.

  La procédure d'ouverture de la Console de gestion de stratégie de groupe varie entre les versions Windows 2012, Windows 2008 et Windows 2003 d'Active Directory. Reportez-vous à la section « Créer des GPO pour les stratégies de groupe View », page 348.

### Procédure

1 Sur le serveur Active Directory, ouvrez la Console de gestion de stratégie de groupe.

2 Développez votre domaine, cliquez avec le bouton droit sur le GPO que vous avez créé pour les paramètres de stratégie de groupe et sélectionnez **Modifier**.

3 Dans l'Éditeur de gestion de stratégie de groupe, accédez à **Configuration de l'ordinateur > Stratégies > Modèles administratifs : définitions de stratégies > Système > Stratégie de groupe**.

4 Dans le volet de droite, double-cliquez sur **Mode de traitement en boucle de la stratégie de groupe d'utilisateurs**.

5 Sélectionnez **Activé**, puis sélectionnez un mode de traitement en boucle dans le menu déroulant **Mode**.

| Option | Action |
|---|---|
| **Merge (Fusionner)** | Les paramètres de règle utilisateur appliqués sont la combinaison de ceux inclus dans les GPO ordinateur et utilisateur. En cas de conflit, les GPO ordinateur sont prioritaires. |
| **Replace (Remplacer)** | La règle utilisateur est définie entièrement depuis les GPO associés à l'ordinateur. Tous les GPO associés à l'utilisateur sont ignorés. |

6 Cliquez sur **OK** pour enregistrer vos modifications.

# Configuration de profils d'utilisateur avec View Persona Management 18

Avec View Persona Management, vous pouvez configurer des profils utilisateur qui sont dynamiquement synchronisés avec un référentiel de profils distant. Cette fonctionnalité permet aux utilisateurs d'accéder à une expérience de poste de travail personnalisée lorsqu'ils se connectent à un poste de travail. View Persona Management développe cette fonctionnalité et améliore les performances des profils itinérants Windows, mais ne nécessite pas de profils itinérants Windows pour fonctionner.

Vous pouvez configurer des paramètres de stratégie de groupe pour activer View Persona Management et contrôler divers aspects de votre déploiement de View Persona Management.

Pour activer et utiliser View Persona Management, vous devez disposer de la licence VMware Horizon appropriée. Reportez-vous au Contrat de l'utilisateur final (CLUF) de VMware à l'adresse http://www.vmware.com/download/eula .

Ce chapitre aborde les rubriques suivantes :



## Fourniture de personas d'utilisateur dans View

Avec la fonctionnalité View Persona Management, le profil distant d'un utilisateur est dynamiquement téléchargé lorsque l'utilisateur se connecte sur un poste de travail View. Vous pouvez configurer View pour stocker des profils utilisateur dans un référentiel centralisé sécurisé. View télécharge les informations persona lorsque l'utilisateur en a besoin.

View Persona Management est une solution de remplacement aux profils itinérants de Windows. View Persona Management développe les fonctionnalités et améliore les performances par rapport aux profils itinérants Windows.

Vous pouvez configurer et gérer des personas sans quitter View. Vous n'avez pas besoin de configurer les profils itinérants Windows. Si vous disposez d'une configuration de profils itinérants Windows, vous pouvez utiliser votre configuration de référentiel existante avec View.

Un profil d'utilisateur est indépendant du poste de travail View. Lorsqu'un utilisateur se connecte à un poste de travail, le même profil s'affiche.

Par exemple, un utilisateur peut se connecter à un poste de travail de clone lié à attribution flottante et modifier l'arrière-plan du poste de travail et les paramètres de Microsoft Word. Lorsque l'utilisateur démarre la session suivante, la machine virtuelle est différente, mais l'utilisateur voit les mêmes paramètres.

Un profil d'utilisateur comprend diverses informations générées par l'utilisateur :

- Paramètres de données et de postes de travail propres à l'utilisateur
- Données et paramètres d'application
- Entrées du Registre Windows configurées par des applications d'utilisateur

En outre, si vous provisionnez des applications ThinApp sur des postes de travail, les données du sandbox ThinApp peuvent être stockées dans le profil d'utilisateur et suivre ce dernier.

View Persona Management minimise le temps requis pour se connecter et se déconnecter des postes de travail. Les temps de connexion et de déconnexion peuvent constituer un problème avec les profils itinérants Windows.

- Pendant la connexion, View télécharge uniquement les fichiers dont Windows a besoin, par exemple les fichiers de Registre de l'utilisateur. D'autres fichiers sont copiés sur le poste de travail local lorsque l'utilisateur ou une application les ouvre à partir du dossier de profil local.
- View copie régulièrement les modifications récentes du profil local dans le référentiel distant, l'intervalle entre chaque copie étant généralement de quelques minutes. La valeur par défaut est toutes les 10 minutes. Vous pouvez spécifier la fréquence de téléchargement du profil local.
- Lors de la déconnexion, seuls les fichiers qui ont été mis à jour depuis la dernière réplication sont copiés dans le référentiel distant.

## Utilisation de View Persona Management avec des systèmes autonomes

Vous pouvez installer une version autonome de View Persona Management sur des ordinateurs physiques et des machines virtuelles qui ne sont pas gérés par View. Avec ce logiciel, vous pouvez gérer des profils d'utilisateur sur des postes de travail View et des systèmes autonomes.

Le logiciel View Persona Management autonome fonctionne avec les systèmes d'exploitation Windows 7, Windows 8, Windows 10, Windows Server 2008 R2 et Windows Server 2012 R2.

Vous pouvez utiliser le logiciel View Persona Management autonome pour réaliser les objectifs suivants :

- Partager des profils d'utilisateur sur des systèmes autonomes et des postes de travail View

  Vos utilisateurs peuvent continuer à utiliser des systèmes autonomes ainsi que des postes de travail View avec View Persona Management. Si vous utilisez les mêmes paramètres de stratégie de groupe View Persona Management pour contrôler des postes de travail View et des systèmes physiques, les utilisateurs peuvent recevoir leurs profils actualisés à chaque fois qu'ils ouvrent une session, qu'ils utilisent leurs ordinateurs hérités ou des postes de travail View.

  **Remarque** View Persona Management ne prend pas en charge les sessions actives simultanées. Un utilisateur doit fermer sa session avant d'en ouvrir une autre.

- Migrer des profils d'utilisateur entre des systèmes physiques et des postes de travail View

  Si vous prévoyez de requalifier des ordinateurs physiques hérités à utiliser dans un déploiement de View, vous pouvez installer View Persona Management autonome sur les systèmes hérités avant de restaurer les postes de travail View pour vos utilisateurs. Lorsque les utilisateurs ouvrent une session sur leurs systèmes hérités, leurs profils sont stockés sur le référentiel de profils distant View. Lorsque les utilisateurs ouvrent une session sur leurs postes de travail View pour la première fois, leurs profils existants sont téléchargés sur leurs postes de travail View.

- Effectuer une migration par étape entre des systèmes physiques et des postes de travail View

Si vous migrez votre déploiement par étape, les utilisateurs qui n'ont pas encore accès à des postes de travail View peuvent utiliser View Persona Management autonome. À mesure que chaque jeu de postes de travail View est déployé, les utilisateurs peuvent accéder à leurs profils sur leurs postes de travail View et les systèmes hérités peuvent être supprimés progressivement. Ce scénario est un hybride des scénarios précédents.

- Prendre en charge des profils actualisés lorsque les utilisateurs ferment leur session

  Les utilisateurs d'ordinateurs portables autonomes peuvent se déconnecter du réseau. Lorsqu'un utilisateur se reconnecte, View Persona Management charge les dernières modifications dans le profil local de l'utilisateur vers le référentiel de profils distant.

  **Remarque** Pour qu'un utilisateur puisse se déconnecter, le profil d'utilisateur doit être complètement téléchargé sur le système local.

## Migration de profils d'utilisateur avec View Persona Management

Avec View Persona Management, vous pouvez migrer des profils d'utilisateur existants dans plusieurs paramètres vers des postes de travail View. Lorsque les utilisateurs ouvrent une session sur leurs postes de travail View après une migration de profil, ils voient les paramètres et données personnels qu'ils ont utilisés sur leurs systèmes hérités.

En migrant des profils d'utilisateur, vous pouvez atteindre les objectifs de migration de poste de travail suivants :

- Vous pouvez mettre à niveau des postes de travail View Windows 7, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 R2 vers des postes de travail View Windows 10.
- Vous pouvez mettre à niveau les systèmes de vos utilisateurs de Windows XP hérité vers Windows 7, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 R2 et migrer vos utilisateurs d'ordinateurs physiques vers View pour la première fois.
- Vous pouvez mettre à niveau des postes de travail View Windows XP hérités vers des postes de travail View Windows 7, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 R2.
- Vous pouvez effectuer une migration entre des ordinateurs physiques et des postes de travail View sans mettre à niveau les systèmes d'exploitation.

Pour réaliser ces scénarios, View Persona Management fournit un utilitaire de migration de profil et un programme d'installation View Persona Management autonome pour les machines physiques ou virtuelles sur lesquelles View Agent 5.*x* n'est pas installé.

**Important** View Agent 6.1 et les versions ultérieures ne prennent pas en charge les postes de travail Windows XP et Windows Vista. View Agent 6.0.2 est la dernière version de View qui prend en charge ces systèmes d'exploitation. Les clients qui disposent d'un contrat de support étendu avec Microsoft pour Windows XP et Vista, ainsi qu'un contrat de support étendu avec VMware pour ces systèmes d'exploitation invités, peuvent déployer l'instance de View Agent 6.0.2 de leurs postes de travail Windows XP et Vista avec le Serveur de connexion View 6.1.

Avec l'utilitaire de migration de profil d'utilisateur de View, vous pouvez effectuer une tâche importante dans une migration à partir d'un déploiement de poste de travail Windows XP hérité qui continuera à être prise en charge dans de futures versions de View.

Le Tableau 18-1 montre différents scénarios de migration et présente les tâches que vous devez effectuer dans chaque scénario.

**Tableau 18-1.** Scénarios de migration de profil d'utilisateur

| S'il s'agit de votre déploiement d'origine... | Et s'il s'agit de votre déploiement de destination... | Effectuez les tâches suivantes : |
|---|---|---|
| Postes de travail View Windows 7, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 R2 | Postes de travail View Windows 10 | 1 Configurez les postes de travail View Windows 10 avec View Persona Management pour vos utilisateurs. Reportez-vous à la section « Configuration d'un déploiement de View Persona Management », page 356.<br>**Remarque** Ne restaurez pas les postes de travail View Windows 10 pour vos utilisateurs avant d'avoir effectué l'étape 2.<br>2 Exécutez l'utilitaire de migration de profil View V2 à V5.<br>■ Pour les profils source, spécifiez le référentiel de profils distant pour les postes de travail View Windows 7, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 R2 existants.<br>■ Pour les profils de destination, spécifiez le référentiel de profils distant que vous avez configuré pour les postes de travail View Windows 10.<br>Pour plus d'informations, reportez-vous au document *Migration des profils d'utilisateur.View*<br>3 Autorisez vos utilisateurs à ouvrir une session sur leurs postes de travail View Windows 10. |
| Ordinateurs physiques Windows XP | Postes de travail View Windows 7, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 R2 | 1 Configurez les postes de travail View Windows 7, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 R2 avec View Persona Management pour vos utilisateurs. Reportez-vous à la section « Configuration d'un déploiement de View Persona Management », page 356.<br>**Remarque** Ne déployez pas les postes de travail View Windows 7, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 R2 pour vos utilisateurs avant d'avoir effectué l'étape 2.<br>2 Exécutez l'utilitaire de migration de profil View V1 à V2.<br>■ Pour les profils source, spécifiez les profils locaux sur les ordinateurs physiques Windows XP.<br>■ Pour les profils de destination, spécifiez le référentiel de profils distant que vous avez configuré pour le déploiement de View.<br>Pour plus d'informations, reportez-vous au document *Migration des profils d'utilisateur.View*<br>3 Autorisez vos utilisateurs à ouvrir une session sur leurs postes de travail View Windows 7, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 R2. |

**Tableau 18-1.** Scénarios de migration de profil d'utilisateur (suite)

| S'il s'agit de votre déploiement d'origine... | Et s'il s'agit de votre déploiement de destination... | Effectuez les tâches suivantes : |
|---|---|---|
| Ordinateurs physiques ou machines virtuelles Windows XP qui utilisent une solution de profil d'utilisateur itinérant. Par exemple, votre déploiement peut utiliser l'une des solutions suivantes :<br>■ View Persona Management<br>■ RTO Virtual Profiles<br>■ profils itinérants de Windows<br>Dans ce scénario, les profils d'utilisateur d'origine doivent être conservés dans un référentiel de profils distant. | Postes de travail View Windows 7, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 R2 | 1 Configurez les postes de travail View Windows 7, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 R2 avec View Persona Management pour vos utilisateurs. Reportez-vous à la section « Configuration d'un déploiement de View Persona Management », page 356.<br>**Remarque** Ne déployez pas les postes de travail View Windows 7, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 R2 pour vos utilisateurs avant d'avoir effectué l'étape 2.<br>2 Exécutez l'utilitaire de migration de profil View V1 à V2.<br>■ Pour les profils source, spécifiez le référentiel de profils distant pour les systèmes Windows XP.<br>■ Pour les profils de destination, spécifiez le référentiel de profils distant que vous avez configuré pour le déploiement de View.<br>Pour plus d'informations, reportez-vous au document *Migration des profils d'utilisateur.View*<br>3 Autorisez vos utilisateurs à ouvrir une session sur leurs postes de travail View Windows 7, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 R2. |
| Ordinateurs physiques ou machines virtuelles Windows 7, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 R2.<br>View Agent 5.*x* ne peut pas être installé sur les systèmes hérités. | Postes de travail View Windows 7, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 R2 | 1 Configurez les postes de travail View Windows 7, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 R2 avec View Persona Management pour vos utilisateurs. Reportez-vous à la section « Configuration d'un déploiement de View Persona Management », page 356.<br>2 Installez le logiciel View Persona Management autonome sur les systèmes Windows 7, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 R2. Reportez-vous à la section « Installer View Persona Management autonome », page 360.<br>3 Configurez les systèmes Windows 7, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 R2 hérités pour utiliser le même référentiel de profils distants que les postes de travail View. Reportez-vous à la section « Configurer un référentiel de profils d'utilisateur », page 357.<br>L'approche la plus facile consiste à utiliser les mêmes paramètres de stratégie de groupe View Persona Management dans Active Directory pour contrôler les systèmes hérités |

**Tableau 18-1.** Scénarios de migration de profil d'utilisateur (suite)

| S'il s'agit de votre déploiement d'origine... | Et s'il s'agit de votre déploiement de destination... | Effectuez les tâches suivantes : |
|---|---|---|
| | | et les postes de travail View. Reportez-vous à la section « Ajouter le fichier de modèle d'administration de View Persona Management », page 361.<br>4 Déployez vos postes de travail View Windows 7, Windows 8, Windows Server 2008 R2 ou Windows Server 2012 R2 pour vos utilisateurs. |

# Persona Management et profils itinérants de Windows

Lorsque Persona Management est activé, vous ne pouvez pas modifier les personas des utilisateurs de View en utilisant les fonctions des profils itinérants de Windows.

Par exemple, si vous ouvrez une session sur le système d'exploitation client d'un poste de travail, allez à l'onglet **Avancé** dans la boîte de dialogue Propriétés système et modifiez les paramètres Profils d'utilisateur de **Profil itinérant** à **Profil local**. View Persona Management continue de synchroniser le persona de l'utilisateur entre le poste de travail local et le référentiel de persona distant.

Toutefois, vous pouvez spécifier des fichiers et des dossiers dans les personas des utilisateurs qui sont gérés par la fonctionnalité de profils itinérants de Windows plutôt que par View Persona Management. Vous utilisez la stratégie **Synchronisation de profils itinérants de Windows** pour spécifier ces fichiers et dossiers.

# Configuration d'un déploiement de View Persona Management

Pour configurer View Persona Management, vous définissez un référentiel distant qui stocke des profils d'utilisateur, installez Horizon Agent avec l'option de configuration **View Persona Management** sur des machines virtuelles qui livrent des sessions de poste de travail distant, ajoutez et configurez les paramètres de stratégie de groupe View Persona Management, et déployez des pools de postes de travail.

Vous pouvez également configurer View Persona Management pour un déploiement autre que View. Vous installez la version autonome de View Persona Management sur des ordinateurs portables, postes de travail ou machines virtuelles autres que View de vos utilisateurs. Vous devez également définir un référentiel distant et configurer les paramètres de stratégie de groupe de View Persona Management.

## Présentation de la configuration d'un déploiement de View Persona Management

Pour configurer un déploiement de postes de travail View ou des ordinateurs autonomes avec View Persona Management, vous devez effectuer plusieurs tâches de haut niveau.

Nous vous recommandons d'effectuer les tâches dans l'ordre indiqué ci-dessous, même s'il est possible de les effectuer dans un autre ordre. Par exemple, vous pouvez configurer ou reconfigurer des paramètres de stratégie de groupe dans Active Directory après avoir déployé des pools de postes de travail.

1. Configurez un référentiel distant pour stocker des profils d'utilisateur.

   Vous pouvez configurer un partage réseau ou utiliser le chemin d'un profil d'utilisateur Active Directory existant que vous avez configuré pour des profils itinérants Windows.

2. Installez Horizon Agent avec l'option d'installation **View Persona Management** sur les machines virtuelles que vous utilisez pour créer des pools de postes de travail.

   Pour configurer View Persona Management pour des ordinateurs portables, des ordinateurs de bureau ou des machines virtuelles autres que View, installez le logiciel View Persona Management autonome sur chaque ordinateur de votre déploiement ciblé.

3 Ajoutez le fichier de modèle d'administration (ADM) de View Persona Management à votre serveur Active Directory ou à la configuration Stratégie d'ordinateur local sur la machine virtuelle parente.

   Pour configurer View Persona Management pour l'intégralité de votre déploiement de View ou d'ordinateurs autres que View, ajoutez le fichier de modèle d'administration à Active Directory.

   Pour configurer View Persona Management pour un pool de postes de travail, utilisez les méthodes suivantes :

   - Ajoutez le fichier de modèle d'administration à la machine virtuelle que vous utilisez pour créer le pool.
   - Ajoutez le fichier de modèle d'administration à Active Directory et appliquez les paramètres de stratégie de groupe à l'UO qui contient les machines du pool.

4 Activez View Persona Management en activant le paramètre de stratégie de groupe **Gérer un persona d'utilisateur**.

5 Si vous avez configuré un partage réseau pour le référentiel de profils distants, activez le paramètre de stratégie de groupe **Emplacement du référentiel de persona** et spécifiez le chemin du partage réseau.

6 (Facultatif) Configurez d'autres paramètres de stratégie de groupe dans Active Directory ou dans la configuration de Stratégie d'ordinateur local.

7 Créez des pools de postes de travail à partir des machines virtuelles sur lesquelles vous avez installé Horizon Agent avec l'option d'installation **View Persona Management**.

## Configurer un référentiel de profils d'utilisateur

Vous pouvez configurer un référentiel distant pour stocker les données et les paramètres des utilisateurs, les données spécifiques des applications et d'autres informations générés par l'utilisateur dans les profils utilisateurs. Si des profils itinérants Windows sont configurés dans votre déploiement, vous pouvez utiliser un chemin de profil d'utilisateur Active Directory à la place.

**Remarque** Vous pouvez configurer View Persona Management sans avoir à configurer les profils itinérants Windows.

### Prérequis

- Familiarisez-vous avez les autorisations d'accès minimales requises pour configurer un dossier partagé. Reportez-vous à la section « Définition d'autorisations d'accès sur des dossiers partagés pour View Persona Management », page 358.
- Familiarisez-vous avez les instructions pour la création d'un référentiel de profils utilisateurs. Reportez-vous à la section « Création d'un partage de réseau pour View Persona Management », page 359

### Procédure

1 Déterminez si vous souhaitez utiliser un chemin de profils d'utilisateur Active Directory existant ou configurer un référentiel de profils utilisateurs sur un réseau partagé.

| Option | Action |
|---|---|
| **Utiliser un chemin de profil d'utilisateur Active Directory existant** | Si vous disposez de profils itinérants Windows existants, vous pouvez utiliser le chemin de profil d'utilisateur Active Directory qui prend en charge les profils itinérants. Vous pouvez ignorer les étapes suivantes de cette procédure. |
| **Configurer un partage réseau pour stocker un référentiel de profils utilisateurs** | Si vous ne disposez pas d'une configuration de profils itinérants Windows, vous devez configurer un partage réseau pour le référentiel de profils utilisateurs. Suivez les dernières étapes de cette procédure. |

2 Créez un dossier partagé sur un ordinateur auquel vos utilisateurs peuvent accéder à partir du système d'exploitation invité de leur poste de travail.

   Si `%username%` ne fait pas partie du chemin de dossier que vous configurez, View Persona Management ajoute `%username%.%userdomain%` au chemin.

   Par exemple : `\\server.domain.com\VPRepository\%username%.%userdomain%`

3 Définissez les autorisations d'accès des dossiers partagés contenant les profils utilisateurs.

**Avertissement** Vérifiez que les autorisations d'accès sont correctement configurées. Une configuration incorrecte des autorisations d'accès du dossier partagé est la cause la plus fréquente des problèmes liés à View Persona Management.

## Définition d'autorisations d'accès sur des dossiers partagés pour View Persona Management

Les profils itinérants View Persona Management et Windows nécessitent un niveau d'autorisation minimal spécifique sur le référentiel de profils utilisateurs. View Persona Management nécessite également que le groupe de sécurité des utilisateurs ayant placé des données dans le dossier partagé dispose d'attributs de lecture sur le partage.

Définissez les autorisations d'accès nécessaires sur votre référentiel de profils utilisateurs et votre partage de dossiers redirigés.

**Tableau 18-2.** Autorisations NTFS minimales requises pour le référentiel de profils utilisateurs et le partage de dossiers redirigés

| Compte d'utilisateur | Autorisations minimales requises |
|---|---|
| Propriétaire créateur | Contrôle complet, Sous-dossiers et fichiers uniquement |
| Administrateur | aucune. Activez plutôt le paramètre de stratégie de groupe Windows, **Ajouter le groupe de sécurité Administrateurs aux profils d'utilisateur itinérant**. Dans l'Éditeur d'objets de stratégie de groupe, ce paramètre de stratégie est situé dans **Configuration ordinateur\Modèles administratifs\Système\Profils d'utilisateur**. |
| Groupe de sécurité pour les utilisateurs ayant besoin de partager des données | Afficher un dossier/Lire des données, Créer des dossiers/Ajouter des données, Lire des attributs - Ce dossier uniquement |
| Tout le monde | Aucune autorisation |
| Système local | Contrôle complet, Ce dossier, Sous-dossiers et fichiers |

**Tableau 18-3.** Autorisations de niveau de partage (SMB) nécessaires pour le référentiel de profils utilisateurs et le partage de dossiers redirigés

| Compte d'utilisateur | Autorisations par défaut | Autorisations minimales requises |
|---|---|---|
| Tout le monde | Lecture seule | Aucune autorisation |
| Groupe de sécurité pour les utilisateurs ayant besoin de partager des données | S/O | Contrôle complet |

Pour plus d'informations sur la sécurité des profils utilisateurs itinérants, reportez-vous à la rubrique Microsoft TechNet, *Recommandations de sécurité pour les dossiers partagés de profils utilisateurs itinérants*. http://technet.microsoft.com/en-us/library/cc757013(WS.10).aspx

### Création d'un partage de réseau pour View Persona Management

Vous devez suivre certaines recommandations lorsque vous créez un dossier partagé à utiliser en tant que référentiel de profils.

- Si vous utilisez des postes de travail Windows 8 et que votre partage réseau utilise un système de fichiers OneFS sur un périphérique NAS EMC Isilon, la version du système de fichiers OneFS doit être 6.5.5.11 ou supérieure.
- Vous pouvez créer le dossier partagé sur un serveur, un périphérique NAS (Network Attached Storage) ou un serveur réseau.
- Le dossier partagé n'a pas à être dans le même domaine que Serveur de connexion View.
- Le dossier partagé doit se trouver dans la même forêt Active Directory que celle des utilisateurs qui stockent des profils dans le dossier partagé.
- Vous devez utiliser un lecteur partagé suffisamment volumineux pour stocker des informations de profil d'utilisateur pour vos utilisateurs. Pour prendre en charge un déploiement volumineux de View, vous pouvez configurer des référentiels séparés pour différents pools de postes de travail.

  Si des utilisateurs sont autorisés à accéder à plusieurs pools, les pools qui partagent des utilisateurs doivent être configurés avec le même référentiel de profils. Si vous autorisez un utilisateur à accéder à deux pools avec deux référentiels de profils différents, l'utilisateur ne peut pas accéder à la même version du profil depuis des postes de travail dans chaque pool.
- Vous devez créer le chemin de profil complet sous lequel les dossiers de profils d'utilisateur seront créés. Si une partie du chemin n'existe pas, Windows crée les dossiers manquants lorsque le premier utilisateur ouvre une session, puis affecte des restrictions de sécurité de l'utilisateur à ces dossiers. Windows affecte les mêmes restrictions de sécurité à tous les dossiers qu'il crée dans ce chemin.

  Par exemple, pour `user1`, vous pouvez configurer le chemin View Persona Management `\\server\VPRepository\profiles\user1`. Si vous créez le partage de réseau `\\\\server\\VPRepository`, et si le dossier `profiles` n'existe pas, Windows crée le chemin `\\profiles\\user1` lorsque `user1` ouvre une session. Windows limite l'accès aux dossiers `\\profiles\\user1` au compte `user1`. Si un autre utilisateur ouvre une session avec un chemin de profil dans `\\server\VPRepository\profiles`, le deuxième utilisateur ne peut pas accéder au référentiel et la réplication du profil de l'utilisateur échoue.

## Installer Horizon Agent avec l'option View Persona Management

Pour utiliser View Persona Management avec des postes de travail View, vous devez installer Horizon Agent avec l'option d'installation **View Persona Management** sur les machines virtuelles que vous utilisez pour créer des pools de postes de travail.

Pour un pool automatisé, vous installez Horizon Agent avec l'option d'installation **View Persona Management** sur la machine virtuelle que vous utilisez en tant que parent ou modèle. Lorsque vous créez un pool de postes de travail à partir de la machine virtuelle, le logiciel View Persona Management est déployé sur vos postes de travail View.

Dans le cas d'un pool manuel, vous devez installer Horizon Agent avec l'option d'installation **View Persona Management** sur chaque machine virtuelle utilisée en tant que poste de travail dans le pool. Utilisez Active Directory pour configurer des stratégies de groupe View Persona Management pour un pool manuel. L'autre solution consiste à ajouter le fichier de modèle d'administration et à configurer des stratégies de groupe sur chaque machine individuelle.

### Prérequis

- Vérifiez que vous effectuez l'installation sur une machine virtuelle Windows 7, Windows 8, Windows 10, Windows Server 2008 R2 ou Windows Server 2012 R2. View Persona Management ne fonctionne pas sur des hôtes Microsoft RDS.

  L'installation d'Horizon Agent avec l'option d'installation **View Persona Management** ne fonctionne pas sur les ordinateurs physiques. Vous pouvez installer le logiciel View Persona Management autonome sur des ordinateurs physiques. Reportez-vous à la section « Installer View Persona Management autonome », page 360.

- Vérifiez que vous pouvez ouvrir une session en tant qu'administrateur sur la machine virtuelle.
- Vérifiez que le service natif RTO Virtual Profiles 2.0 n'est pas installé sur la machine virtuelle. Si un service natif RTO Virtual Profile 2.0 est présent, désinstallez-le avant d'installer Horizon Agent avec l'option d'installation **View Persona Management**.
- Familiarisez-vous avec l'installation d'Horizon Agent. Reportez-vous à la section « Installer Horizon Agent sur une machine virtuelle », page 33 ou « Installer Horizon Agent sur une machine non gérée », page 20.

### Procédure

- Lorsque vous installez Horizon Agent sur une machine virtuelle, sélectionnez l'option d'installation **View Persona Management**.

### Suivant

Ajoutez le fichier de modèle d'administration de View Persona Management à votre serveur Active Directory ou à la configuration Stratégie Ordinateur local sur la machine virtuelle elle-même. Reportez-vous à la section « Ajouter le fichier de modèle d'administration de View Persona Management », page 361.

## Installer View Persona Management autonome

Pour utiliser View Persona Management avec des ordinateurs physiques ou des machines virtuelles non View, installez la version autonome de View Persona Management. Vous pouvez exécuter une installation interactive ou une installation silencieuse à partir de la ligne de commande.

Installez le logiciel View Persona Management autonome sur chaque machine virtuelle ou ordinateur individuel dans votre déploiement ciblé.

### Prérequis

- Vérifiez que vous effectuez l'installation sur un ordinateur physique ou une machine virtuelle Windows 7, Windows 8, Windows 10, Windows Server 2008 R2 ou Windows Server 2012 R2. View Persona Management ne fonctionne pas sur des serveurs Windows Server ou sur des hôtes Microsoft RDS. Vérifiez que le système répond à la configuration requise décrite dans la section « Systèmes d'exploitation pris en charge pour View Persona Management autonome » du document *Installation de View*.
- Vérifiez que vous pouvez ouvrir une session en tant qu'administrateur sur le système.
- Vérifiez que View Agent 5.*x* ou supérieur n'est pas installé sur l'ordinateur.
- Vérifiez que le service natif RTO Virtual Profiles 2.0 n'est pas installé sur la machine virtuelle.
- Si vous prévoyez d'effectuer une installation silencieuse, familiarisez-vous avec les options de ligne de commande du programme d'installation MSI. Reportez-vous à la section « Options de la ligne de commande Microsoft Windows Installer », page 39.

### Procédure

1 Téléchargez le fichier du programme d'installation View Persona Management autonome sur la page de produits VMware à l'adresse http://www.vmware.com/products/.

Le nom de fichier du programme d'installation est `VMware-personamanagement-y.y.y-xxxxxx.exe` ou `VMware-personamanagement-x86_64-y.y.y-xxxxxx.exe`, où *y.y.y* est le numéro de version et *xxxxxx* le numéro de build.

2 Exécutez le programme d'installation interactivement ou effectuez une installation silencieuse.

| Option | Description |
|---|---|
| **Installation interactive** | a Pour démarrer le programme d'installation, double-cliquez sur le fichier du programme d'installation.<br>b Acceptez les termes de licence VMware.<br>c Cliquez sur **Installer**.<br>Par défaut, View Persona Management est installé dans le répertoire `C:\Program Files\VMware\VMware View Persona Management`.<br>d Cliquez sur **Terminer**. |
| **Installation silencieuse** | Ouvrez une invite de commande Windows sur la machine et tapez la commande d'installation sur une ligne.<br>Par exemple : `VMware-personamanagement-y.y.y-xxxxxx.exe /s /v"/qn /l*v ""c:\persona.log"" ALLUSERS=1"`<br>**Important** Vous devez inclure la propriété `ALLUSERS=1` dans la ligne de commande. |

3 Redémarrez votre système pour que les modifications de l'installation prennent effet.

### Suivant

Ajoutez le fichier de modèle d'administration de View Persona Management à votre configuration Active Directory ou de stratégie de groupe local.

## Ajouter le fichier de modèle d'administration de View Persona Management

Le fichier de modèle d'administration de View Persona Management contient des paramètres de stratégie de groupe qui vous permettent de configurer View Persona Management. Avant de pouvoir configurer les stratégies, vous devez ajouter le fichier de modèle d'administration aux systèmes locaux ou au serveur Active Directory.

Pour configurer View Persona Management sur un seul système, vous pouvez ajouter les paramètres de stratégie de groupe à la configuration Stratégie Ordinateur local sur ce système local.

Pour configurer View Persona Management pour un pool de postes de travail, vous pouvez ajouter les paramètres de stratégie de groupe à la configuration de la stratégie Ordinateur local sur la machine virtuelle que vous utilisez comme parent ou modèle de déploiement pour le pool de postes de travail.

Pour configurer View Persona Management au niveau du domaine et appliquer la configuration à plusieurs machines View ou à l'ensemble de votre déploiement, vous pouvez ajouter les paramètres de stratégie de groupe aux objets de stratégie de groupe (GPO) sur votre serveur Active Directory. Dans Active Directory, vous pouvez créer une unité d'organisation pour les machines View utilisant View Persona Management, créer un ou plusieurs GPO et les lier à l'unité d'organisation. Pour configurer des stratégies View Persona Management distinctes pour différents types d'utilisateurs, vous pouvez créer des unités d'organisation pour des ensembles particuliers de machines View et appliquer différents GPO aux unités d'organisation.

Par exemple, vous pouvez créer une unité d'organisation pour les machines View avec View Persona Management et une autre unité d'organisation pour les ordinateurs physiques sur lesquels le logiciel autonome View Persona Management est installé.

Pour voir un exemple d'implémentation de stratégies de groupe Active Directory dans View, reportez-vous à « Exemple de stratégie de groupe Active Directory », page 347.

## Ajouter le modèle d'administration de Persona Management à un système unique

Pour configurer View Persona Management pour un seul pool de postes de travail, vous devez ajouter le fichier de modèle d'administration de Persona Management à la stratégie de l'ordinateur local sur la machine virtuelle que vous utilisez pour créer le pool. Pour configurer View Persona Management sur un seul système, vous devez ajouter le fichier de modèle d'administration Persona Management à ce système.

### Prérequis

- Vérifiez qu'Horizon Agent est installé avec l'option de configuration de View Persona Management sur le système. Reportez-vous à la section « Installer Horizon Agent avec l'option View Persona Management », page 359.
- Vérifiez que vous pouvez ouvrir une session en tant qu'administrateur sur le système.

### Procédure

1. Téléchargez le fichier View GPO Bundle `.zip` sur le site de téléchargement de VMware à l'adresse https://my.vmware.com/web/vmware/downloads.

   Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut GPO Bundle.

   Le fichier se nomme `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip`, où *x.x.x* est la version et *yyyyyyy* le numéro de build. Tous les fichiers ADM et ADMX qui fournissent des paramètres de stratégie de groupe pour View sont disponibles dans ce fichier.
2. Décompressez le fichier et copiez le fichier d'administration, `ViewPM.adm`, sur le système local.
3. Sur le système local, cliquez sur **Démarrer > Exécuter**.
4. Saisissez **`gpedit.msc`** et cliquez sur **OK**.
5. Dans la fenêtre Stratégie Ordinateur local, allez à **Configuration ordinateur** et cliquez avec le bouton droit sur **Modèles d'administration**.

   **Remarque** Ne sélectionnez pas **Modèles d'administration** sous **Configuration utilisateur**.
6. Cliquez sur **Ajout/Suppression de modèles** et cliquez sur **Ajouter**.
7. Accédez au répertoire contenant le fichier `ViewPM.adm`.
8. Sélectionnez le fichier `ViewPM.adm` et cliquez sur **Ajouter**.
9. Fermer la fenêtre Add/Remove Templates (Ajout/Suppression de modèles).

Les paramètres de stratégie de groupe de View Persona Management sont ajoutés à la configuration de la stratégie Ordinateur local sur le système local. Vous devez utiliser `gpedit.msc` pour afficher cette configuration.

### Suivant

Configurez les paramètres de stratégie de groupe de View Persona Management sur le système local. Reportez-vous à la section « Configurer des stratégies View Persona Management », page 364.

## Ajouter le modèle d'administration de Persona Management à Active Directory

Pour configurer View Persona Management pour votre déploiement, vous pouvez ajouter le fichier de modèle d'administration ADM de Persona Management à un objet de stratégie de groupe (GPO) dans votre serveur Active Directory.

### Prérequis

- Créez des objets de stratégie de groupe pour votre déploiement View Persona Management et liez-les à l'UO qui contient les machines View qui utilisent View Persona Management. Reportez-vous à la section « Exemple de stratégie de groupe Active Directory », page 347.
- Vérifiez que les composants logiciels enfichables Microsoft MMC (Microsoft Management Console) et l'Éditeur d'objets de stratégie de groupe sont disponibles sur votre serveur Active Directory.
- Vérifiez qu'Horizon Agent est installé avec l'option de configuration de View Persona Management sur un système auquel votre serveur Active Directory a accès. Reportez-vous à la section « Installer Horizon Agent avec l'option View Persona Management », page 359.

### Procédure

1. Téléchargez le fichier View GPO Bundle `.zip` sur le site de téléchargement de VMware à l'adresse https://my.vmware.com/web/vmware/downloads.

   Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut GPO Bundle.

   Le fichier se nomme `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip`, où *x.x.x* est la version et *yyyyyyy* le numéro de build. Tous les fichiers ADM et ADMX qui fournissent des paramètres de stratégie de groupe pour View sont disponibles dans ce fichier.
2. Décompressez le fichier et copiez le fichier de modèle d'administration ADM de View Persona Management, `ViewPM.adm`, sur votre serveur Active Directory.
3. Sur votre serveur Active Directory, ouvrez la Console de gestion des stratégies de groupe.

   Par exemple, ouvrez la boîte de dialogue Exécuter, tapez **`gpmc.msc`**, puis cliquez sur **OK**.
4. Dans le volet de gauche, sélectionnez le domaine ou l'UO qui contient vos machines View.
5. Dans le volet de droite, cliquez avec le bouton droit sur le GPO que vous avez créé pour les paramètres de stratégie de groupe et sélectionnez **Modifier**.

   La fenêtre de l'Éditeur d'objets de stratégie de groupe apparaît.
6. Dans l'Éditeur d'objets de stratégie de groupe, cliquez avec le bouton droit sur **Modèles d'administration** sous **Configuration de l'ordinateur** et sélectionnez **Ajout/Suppression de modèles**.
7. Cliquez sur **Ajouter**, accédez au fichier `ViewPM.adm` et cliquez sur **Ouvrir**.
8. Cliquez sur **Fermer** pour appliquer les paramètres de stratégie dans le fichier de modèle d'administration au GPO.

   Le nom du modèle apparaît dans le volet gauche sous **Modèles d'administration**.

### Suivant

Configurez les paramètres de stratégie de groupe View Persona Management sur le serveur Active Directory.

## Configurer des stratégies View Persona Management

Pour utiliser View Persona Management, vous devez activer le paramètre de stratégie de groupe **Gérer un persona d'utilisateur**, ce qui active le logiciel View Persona Management. Pour configurer un référentiel de profils d'utilisateur sans utiliser de chemin de profil d'utilisateur Active Directory, vous devez configurer le paramètre de stratégie de groupe **Emplacement du référentiel de persona**.

Vous pouvez configurer les paramètres de stratégie de groupe facultatifs pour configurer d'autres aspects de votre déploiement de View Persona Management.

Si des profils itinérants de Windows sont déjà configurés dans votre déploiement, vous pouvez utiliser un chemin de profil d'utilisateur Active Directory existant. Vous pouvez laisser le paramètre **Emplacement du référentiel de persona** désactivé ou non configuré.

### Prérequis

- Familiarisez-vous avec les paramètres de stratégie de groupe **Gérer un persona d'utilisateur** et **Emplacement du référentiel de persona**. Reportez-vous à la section « Paramètres de stratégie de groupe d'itinérance et de synchronisation », page 371.
- Si vous configurez des stratégies de groupe sur un système local, familiarisez-vous avec l'ouverture de la fenêtre Group Policy (Stratégie de groupe). Reportez-vous aux étapes Étape 3 et Étape 4 de la section « Ajouter le modèle d'administration de Persona Management à un système unique », page 362.
- Si vous configurez des stratégies de groupe sur votre serveur Active Directory, familiarisez-vous avec le démarrage de l'Éditeur d'objets de stratégie de groupe. Reportez-vous aux étapes Étape 3 à Étape 5 de la section « Ajouter le modèle d'administration de Persona Management à Active Directory », page 363.

### Procédure

1 Ouvrez la fenêtre Group Policy (Stratégie de groupe).

| Option | Description |
|---|---|
| **Local system (Système local)** | Ouvrez la fenêtre Local Computer Policy (Stratégie Ordinateur local). |
| **Serveur Active Directory** | Ouvrez la fenêtre Group Policy Object Editor (Éditeur d'objets de stratégie de groupe). |

2 Développez le dossier **Configuration ordinateur** et allez dans le dossier **Gestion de persona**.

| Option | Description |
|---|---|
| **Windows 7 et versions ultérieures ou Windows Server 2008 et versions ultérieures** | Développez les dossiers suivants : **Modèles d'administration**, **Modèles d'administration classiques (ADM)**, **Configuration de VMware View Agent**, **Gestion de persona** |
| **Windows Server 2003** | Développez les dossiers suivants : **Modèles d'administration**, **Configuration de VMware View Agent**, **Gestion de persona** |

3 Ouvrez le dossier **Itinérance et synchronisation**.

4 Double-cliquez sur **Gérer un persona d'utilisateur** et cliquez sur **Activé**.

Ce paramètre active View Persona Management. Lorsque ce paramètre est désactivé ou n'est pas configuré, View Persona Management ne fonctionne pas.

5 Saisissez l'intervalle de chargement du profil, en minutes, et cliquez sur **OK**.

L'intervalle de chargement du profil détermine la fréquence à laquelle View Persona Management copie des modifications de profil d'utilisateur dans le référentiel distant. L'intervalle de chargement par défaut est 10 minutes.

6 Double-cliquez sur **Emplacement du référentiel de persona** et cliquez sur **Activé**.

Si vous possédez un déploiement de profils itinérants de Windows existant, vous pouvez utiliser un chemin de profil d'utilisateur Active Directory pour le référentiel de profils distant. Vous n'avez pas à configurer un **Emplacement du référentiel de persona**.

7 Saisissez le chemin d'accès UNC vers un partage de serveur de fichiers de réseau qui stocke les profils d'utilisateur.

Par exemple : `\\server.domain.com\UserProfilesRepository\%username%`

Le partage de réseau doit être accessible pour les machines virtuelles dans votre déploiement.

Si vous prévoyez d'utiliser un chemin de profil d'utilisateur Active Directory, vous n'avez pas à spécifier un chemin d'accès UNC.

8 Si un chemin de profil d'utilisateur Active Directory est configuré dans votre déploiement, déterminez si vous voulez utiliser ou remplacer ce chemin.

| Option | Action |
|---|---|
| **Utiliser le partage de réseau.** | Cochez la case **Remplacer le chemin de profil d'utilisateur Active Directory s'il est configuré**. |
| **Utiliser un chemin de profil d'utilisateur Active Directory, s'il en existe un.** | Ne cochez pas la case **Remplacer le chemin de profil d'utilisateur Active Directory s'il est configuré**. |

9 Cliquez sur **OK**.

10 (Facultatif) Configurez d'autres paramètres de stratégie de groupe View Persona Management.

## Créer des pools de postes de travail qui utilisent Persona Management

Pour utiliser View Persona Management avec des postes de travail View, vous devez créer des pools de postes de travail avec un agent View Persona Management installé sur chaque machine.

Vous ne pouvez pas utiliser View Persona Management sur des pools de postes de travail RDS qui s'exécutent sur des hôtes RDS (Remote Desktop Services).

### Prérequis

- Vérifiez qu'Horizon Agent avec l'option d'installation **View Persona Management** est installé sur la machine virtuelle que vous utilisez pour créer le pool de postes de travail. Reportez-vous à la section « Installer Horizon Agent avec l'option View Persona Management », page 359.
- Si vous prévoyez de configurer des stratégies View Persona Management pour ce pool de postes de travail uniquement, vérifiez que vous avez ajouté le fichier de modèle d'administration de View Persona Management à la machine virtuelle et configuré des paramètres de stratégie de groupe dans la configuration Stratégie Ordinateur local. Reportez-vous aux sections « Ajouter le modèle d'administration de Persona Management à un système unique », page 362 et « Configurer des stratégies View Persona Management », page 364.

### Procédure

- Générez un snapshot ou un modèle depuis la machine virtuelle et créez un pool de postes de travail automatisé.

  Vous pouvez configurer View Persona Management avec des pools qui contiennent des machines virtuelles complètes ou des clones liés. Les pools peuvent utiliser des affectations dédiées ou flottantes.

- (Facultatif) Pour utiliser View Persona Management avec des pools de postes de travail manuels, sélectionnez les machines sur lesquelles Horizon Agent est installé avec l'option **View Persona Management**.

**Remarque** Après avoir déployé View Persona Management sur vos pools de postes de travail View, si vous supprimez l'option d'installation **View Persona Management** sur les machines View ou désinstallez Horizon Agent complètement, les profils d'utilisateur local sont supprimés des machines d'utilisateurs qui ne sont pas actuellement connectés. Pour les utilisateurs actuellement connectés, les profils d'utilisateur sont téléchargés depuis le référentiel de profils distant lors de la désinstallation.

# Meilleures pratiques pour la configuration d'un déploiement de View Persona Management

Vous devez suivre des meilleures pratiques pour la configuration de View Persona Management afin d'accroître l'expérience de vos utilisateurs sur les postes de travail, améliorer les performances du poste de travail et vous assurer que View Persona Management fonctionne efficacement avec d'autres fonctions de View.

## Choisir de supprimer des profils d'utilisateur locaux à la fermeture de session

Par défaut, View Persona Management ne supprime pas les profils d'utilisateur des machines locales lorsque des utilisateurs ferment une session. La stratégie **Supprimer le persona local à la fermeture de session** est désactivée. Dans de nombreux cas, le paramètre par défaut est une meilleure pratique car il réduit les opérations d'E/S et évite le comportement redondant.

Par exemple, laissez cette stratégie désactivée si vous déployez des pools à attribution flottante, puis actualisez ou supprimez les machines à la fermeture de la session. Le profil local est supprimé lorsque la machine virtuelle est actualisée ou supprimée. Dans un pool automatisé d'affectation flottante, des machines virtuelles complètes peuvent être supprimées après la fermeture de session. Dans un pool de clone lié d'affectation flottante, les clones peuvent être actualisés ou supprimés à la fermeture de session.

Si vous déployez des pools à attribution dédiée, vous pouvez laisser la stratégie désactivée, car les utilisateurs reviennent aux mêmes machines à chaque session. Avec la stratégie désactivée, lorsqu'un utilisateur ouvre une session, View Persona Management n'a pas à télécharger les fichiers présents dans le profil local. Si vous configurez des pools de clone lié d'affectation dédiée avec des disques persistants, laissez la stratégie désactivée pour éviter de supprimer des données d'utilisateur des disques persistants.

Dans certains cas, vous voulez peut-être activer la stratégie **Supprimer le persona local à la fermeture de session**.

## Gestion des déploiements incluant View Persona Management et des profils itinérants de Windows

Dans des déploiements dans lesquels des profils itinérants de Windows sont configurés, et où les utilisateurs accèdent à des postes de travail View avec View Persona Management et à des postes de travail standard avec des profils itinérants de Windows, la meilleure pratique consiste à utiliser des profils différents pour les deux environnements de postes de travail. Si un poste de travail View et l'ordinateur client à partir duquel le poste de travail est lancé se trouvent dans le même domaine, et si vous utilisez un GPO Active Directory pour configurer à la fois des profils itinérants Windows et View Persona Management, activez la stratégie **Emplacement du référentiel de persona** et sélectionnez **Remplacer le chemin de profil d'utilisateur Active Directory s'il est configuré**.

Cette approche évite à des profils itinérants de Windows de remplacer un profil View Persona Management lorsque l'utilisateur ferme une session sur l'ordinateur client.

Si des utilisateurs prévoient de partager des données entre des profils itinérants de Windows existants et des profils View Persona Management, vous pouvez configurer la redirection de dossiers Windows.

## Configuration de chemins d'accès pour des dossiers redirigés

Lorsque vous utilisez le paramètre de stratégie de groupe **Redirection de dossiers**, configurez le chemin de dossier pour inclure `%username%`, mais assurez-vous que le dernier sous-dossier dans le chemin utilise le nom du dossier redirigé, tel que `My Videos`. Le dernier dossier dans le chemin est affiché sous la forme du nom de dossier sur le poste de travail de l'utilisateur.

Par exemple, si vous configurez un chemin tel que `\\myserver\videos\%username%\My Videos`, le nom de dossier qui apparaît sur le poste de travail de l'utilisateur est `My Videos`.

Si `%username%` est le dernier sous-dossier dans le chemin, le nom de l'utilisateur apparaît sous la forme du nom de dossier. Par exemple, au lieu de voir un dossier `My Videos` sur le poste de travail, l'utilisateur `JDoe` voit un dossier avec le nom `JDoe` et ne peut pas identifier facilement le dossier.

## Utilisation du journal des événements Windows pour contrôler le déploiement de View Persona Management

Pour vous aider à gérer votre déploiement, View Persona Management fournit des messages de journal et une taille de profil améliorés, ainsi que le suivi du nombre de fichiers et de dossiers. View Persona Management utilise le nombre de fichiers et de dossiers afin de recommander des dossiers pour la redirection dans le journal d'événements Windows et fournit des statistiques pour ces dossiers. Par exemple, lorsqu'un utilisateur se connecte, le journal des événements Windows peut afficher les suggestions suivantes pour rediriger les dossiers :

```
Profile path: \\server.domain.com\persona\user1V2
...
Folders to redirect:
\\server.domain.com\persona\user1V2  Reason: Folder size larger than 1GB
\\server.domain.com\persona\user1V2\Documents  Reason: More than 10000 files and folders
```

## Meilleures pratiques supplémentaires

Vous pouvez également suivre ces recommandations :

- Par défaut, de nombreux antivirus n'analysent pas les fichiers hors ligne. Par exemple, lorsqu'un utilisateur ouvre une session sur un poste de travail, ces antivirus n'analysent pas les fichiers de profil d'utilisateur qui ne sont pas spécifiés dans le paramètre de stratégie de groupe **Fichiers et dossiers à précharger** ou **Synchronisation de profils itinérants de Windows**. Pour de nombreux déploiements, le comportement par défaut est la meilleure pratique car elle réduit l'E/S requise pour télécharger des fichiers lors d'analyses à la demande.

  Si vous voulez récupérer des fichiers du référentiel distant et activer l'analyse des fichiers hors ligne, consultez la documentation de votre antivirus.

- Il vous est fortement recommandé d'utiliser des pratiques standard pour sauvegarder des partages réseau sur lesquels View Persona Management stocke le référentiel de profils.

  **Remarque** N'utilisez pas de logiciel de sauvegarde tel que MozyPro ou les services de sauvegarde Windows Volume avec View Persona Management pour sauvegarder des profils d'utilisateur sur des postes de travail View.

  View Persona Management s'assure que les profils d'utilisateur sont sauvegardés sur le référentiel de profils distant, ce qui évite d'utiliser des outils supplémentaires pour sauvegarder les données d'utilisateur sur les postes de travail. Dans certains cas, des outils tels que MozyPro ou les services de sauvegarde Windows Volume peuvent interférer avec View Persona Management et entraîner la perte ou la corruption de données.

- Vous pouvez définir des stratégies View Persona Management pour améliorer les performances lorsque des utilisateurs démarrent des applications ThinApp. Reportez-vous à la section « Configuration de profils d'utilisateur pour inclure des dossiers de sandbox ThinApp », page 368.
- Si vos utilisateurs génèrent des données de persona substantielles, et si vous prévoyez d'utiliser l'actualisation et la recomposition pour gérer des postes de travail de clone lié d'affectation dédiée, configurez votre pool de postes de travail afin d'utiliser des disques persistants de View Composer séparés. Les disques persistants peuvent améliorer les performances de View Persona Management. Reportez-vous à la section « Configuration de disques persistants de View Composer avec View Persona Management », page 369.
- Si vous configurez View Persona Management pour des ordinateurs portables autonomes, assurez-vous que les profils sont toujours synchronisés lorsque l'utilisateur ferme la session. Reportez-vous à la section « Gérer les profils d'utilisateur sur les ordinateurs portables autonomes », page 369.
- N'utilisez pas la mise en cache côté client Windows avec View Persona Management. Le système de mise en cache côté client Windows est un mécanisme qui prend en charge la fonctionnalité Fichiers hors connexion de Windows. Si ce système est en vigueur sur le système local, les fonctionnalités de View Persona Management comme la redirection de dossier, le remplissage des fichiers hors connexion à la connexion, le téléchargement en arrière-plan et la réplication de fichiers de profil local sur le référentiel du profil distant ne fonctionnent pas correctement.

  Nous vous recommandons de désactiver la fonctionnalité Fichiers hors connexion de Windows avant de commencer à utiliser View Persona Management. Si vous rencontrez des difficultés avec View Persona Management parce que la mise en cache côté client Windows est en vigueur sur vos postes de travail, vous pouvez les résoudre en synchronisant les données du profil qui résident actuellement dans la base de données de mise en cache côté client et en désactivant la fonctionnalité Fichiers hors connexion de Windows. Pour obtenir des instructions, consultez l'article 2016416 de la base de connaissances : Les fonctions de View Persona Management ne fonctionnent pas lorsque la mise en cache sur le client Windows est activée.

## Configuration de profils d'utilisateur pour inclure des dossiers de sandbox ThinApp

View Persona Management conserve les paramètres d'utilisateur associés à des applications ThinApp en incluant des dossiers de sandbox ThinApp dans les profils d'utilisateur. Vous pouvez définir des stratégies View Persona Management pour améliorer les performances lorsque des utilisateurs démarrent des applications ThinApp.

View Persona Management précharge des dossiers et des fichiers de sandbox ThinApp dans le profil d'utilisateur local lorsqu'un utilisateur ouvre une session. Les dossiers de sandbox ThinApp sont créés avant qu'un utilisateur puisse terminer l'ouverture de session. Pour améliorer les performances, View Persona Management ne télécharge pas les données de sandbox ThinApp lors de l'ouverture de session, bien que les fichiers soient créés sur le poste de travail local avec les mêmes attributs et tailles de base que les fichiers de sandbox ThinApp dans le profil distant de l'utilisateur.

Comme meilleure pratique, il vous est conseillé de télécharger les données de sandbox ThinApp réelles en arrière-plan. Activez le paramètre de stratégie de groupe **Dossiers à télécharger en arrière-plan** et ajoutez les dossiers de sandbox ThinApp. Reportez-vous à la section « Paramètres de stratégie de groupe d'itinérance et de synchronisation », page 371.

Les fichiers de sandbox ThinApp réels peuvent être volumineux. Avec le paramètre **Dossiers à télécharger en arrière-plan**, les utilisateurs n'ont pas à attendre que des fichiers volumineux se téléchargent lorsqu'ils démarrent une application. De plus, les utilisateurs n'ont pas à attendre que les fichiers se préchargent lorsqu'ils ouvrent une session, comme ils le devraient si vous utilisez le paramètre **Fichiers et dossiers à précharger** avec des fichiers volumineux.

## Configuration de disques persistants de View Composer avec View Persona Management

Avec des disques persistants de View Composer, vous pouvez conserver des données et des paramètres d'utilisateur tout en gérant des disques du système d'exploitation de clone lié avec des opérations d'actualisation, de recomposition et de rééquilibrage. La configuration de disques persistants peut améliorer les performances de View Persona Management lorsque les utilisateurs génèrent une grande quantité d'informations de persona. Vous pouvez configurer des disques persistants uniquement avec des postes de travail de clone lié d'affectation dédiée.

View Persona Management conserve chaque profil d'utilisateur sur un référentiel distant configuré sur un partage de réseau. Une fois qu'un utilisateur ouvre une session sur un poste de travail, les fichiers de persona sont téléchargés dynamiquement lorsque l'utilisateur en a besoin.

Si vous configurez des disques persistants avec View Persona Management, vous pouvez actualiser et recomposer les disques du système d'exploitation de clone lié et conserver une copie locale de chaque profil d'utilisateur sur les disques persistants.

Les disques persistants peuvent agir comme un cache pour les profils d'utilisateur. Lorsqu'un utilisateur requiert des fichiers de persona, View Persona Management n'a pas besoin de télécharger les données qui sont les mêmes sur le disque persistant local et sur le référentiel distant. Seules les données de persona non synchronisées doivent être téléchargées.

Si vous configurez des disques persistants, n'activez pas la stratégie **Supprimer le persona local à la fermeture de session**. L'activation de cette stratégie supprime les données d'utilisateur des disques persistants lorsque des utilisateurs ferment une session.

## Gérer les profils d'utilisateur sur les ordinateurs portables autonomes

Si vous installez View Persona Management sur des ordinateurs portables autonomes (non-View), veillez à maintenir les profils d'utilisateur synchronisés lorsque les utilisateurs mettent leurs ordinateurs portables autonomes hors ligne.

Pour que l'ordinateur portable autonome d'un utilisateur ait un profil local à jour, vous pouvez configurer le paramètre de stratégie de groupe View Persona Management `Enable background download for laptops`. Ce paramètre télécharge l'ensemble du profil d'utilisateur vers l'ordinateur portable autonome en arrière-plan.

Comme meilleure pratique, notifiez les utilisateurs pour que leurs profils d'utilisateur soient complètement téléchargés avant qu'ils se déconnectent du réseau. Demandez aux utilisateurs d'attendre l'affichage de l'avis `Background download complete` sur leur écran avant de se déconnecter.

Pour afficher l'avis `Background download complete` sur les ordinateurs portables des utilisateurs, définissez le paramètre de stratégie de groupe View Persona Management, `Show critical errors to users via tray icon alerts`.

Si l'utilisateur se déconnecte du réseau avant la fin du téléchargement de profil, le profil local et le profil distant risquent de ne plus être synchronisés. Lorsque l'utilisateur est hors ligne, il pourrait mettre à jour un fichier local qui n'a pas été complètement téléchargé. Lorsque l'utilisateur se reconnecte au réseau, le profil local est envoyé en remplaçant le profil distant. Les données qui se trouvaient dans le profil distant d'origine sont perdues.

Voici un exemple d'étapes à suivre.

### Prérequis

Vérifiez que View Persona Management est configuré pour les ordinateurs portables autonomes des utilisateurs. Reportez-vous à la section « Configuration d'un déploiement de View Persona Management », page 356.

### Procédure

1 Dans l'UO Active Directory qui contrôle les ordinateurs portables autonomes, activez le paramètre `Enable background download for laptops`.

   Dans l'Éditeur d'objets de stratégie de groupe, développez les dossiers suivants : **Configuration ordinateur**, **Modèles d'administration**, **Modèles d'administration classiques (ADM)** > **Configuration de VMware View Agent** > **Gestion de persona**, **Itinérance et synchronisation**

   Le dossier **Modèles d'administration classiques (ADM)** s'affiche uniquement dans Windows 7 (et versions ultérieures) et Windows Server 2008 (et versions ultérieures).

2 Pour les ordinateurs portables autonomes, vous devez utiliser une méthode non-View pour notifier les utilisateurs lorsqu'ils ouvrent une session.

   Par exemple, vous pouvez diffuser le message suivant :
   **`Vos données personnelles sont téléchargées dynamiquement vers votre ordinateur portable après l'ouverture d'une session. Attendez la fin du téléchargement de vos données personnelles avant de déconnecter votre ordinateur portable du réseau. Un avis de fin de téléchargement en arrière-plan s'affichera lorsque le téléchargement de vos données personnelles sera terminé.`**

## Paramètres de stratégie de groupe View Persona Management

Le fichier de modèle d'administration de View Persona Management contient des paramètres de stratégie de groupe que vous ajoutez à la configuration Stratégie de groupe sur des systèmes individuels ou sur un serveur Active Directory. Vous devez configurer les paramètres de stratégie de groupe pour configurer et contrôler plusieurs aspects de View Persona Management.

Le fichier de modèle d'administration ADM se nomme `ViewPM.adm`.

Ce fichier ADM est disponible dans un fichier groupé `.zip` nommé `VMware-Horizon-Extras-Bundle-`*`x.x.x`*`-`*`yyyyyyy`*`.zip`, que vous pouvez télécharger sur le site de téléchargement de VMware à l'adresse https://my.vmware.com/web/vmware/downloads. Sous Desktop & End-User Computing, sélectionnez le téléchargement de VMware Horizon 7, qui inclut le fichier groupé `.zip`.

Une fois que vous avez ajouté le fichier `ViewPM.adm` à votre configuration Stratégie de groupe, les paramètres de règle se trouvent dans le dossier **Gestion de persona** dans la fenêtre Stratégie de groupe.

**Tableau 18-4.** Emplacement des paramètres de View Persona Management dans la fenêtre Stratégie de groupe

| Système d'exploitation | Emplacement |
|---|---|
| Windows 7 et versions ultérieures ou Windows Server 2008 et versions ultérieures | **Computer Configuration (Configuration ordinateur)** > **Administrative Templates (Modèles administratifs)** > **Classic Administrative Templates (ADM) (Modèles d'administration classiques)** > **VMware View Agent Configuration (Configuration de VMware View Agent)** > **Persona Management** |
| Windows Server 2003 | **Computer Configuration (Configuration ordinateur)** > **Administrative Templates (Modèles administratifs)** > **VMware View Agent Configuration (Configuration de VMware View Agent)** > **Persona Management** |

Les paramètres de stratégie de groupe sont contenus dans ces dossiers :

- Itinérance et synchronisation (Roaming & Synchronization)
- Redirection de dossiers
- Desktop UI (Interface utilisateur de poste de travail)
- Journalisation

## Paramètres de stratégie de groupe d'itinérance et de synchronisation

Les paramètres de stratégie de groupe d'itinérance et de synchronisation activent et désactivent View Persona Management, définissent l'emplacement du référentiel de profils distant, déterminent quels dossiers et quels fichiers appartiennent au profil d'utilisateurs, et contrôlent la façon dont sont synchronisés les dossiers et les fichiers.

| Paramètre de stratégie de groupe | Description |
|---|---|
| Gérer un persona d'utilisateur | Détermine si vous voulez gérer des profils d'utilisateur dynamiquement avec View Persona Management ou avec des profils itinérants de Windows. Ce paramètre active et désactive View Persona Management.<br>Lorsque ce paramètre est activé, View Persona Management gère des profils d'utilisateur.<br>Lorsque le paramètre est activé, vous pouvez spécifier un intervalle de chargement du profil en minutes. Cette valeur détermine la fréquence de copie des modifications du profil d'utilisateur dans le référentiel distant. La valeur par défaut est 10 minutes.<br>Lorsque ce paramètre est désactivé ou n'est pas configuré, les profils d'utilisateur sont gérés par Windows. |
| Emplacement du référentiel de persona | Spécifie l'emplacement du référentiel de profils d'utilisateur. Ce paramètre détermine également si vous voulez utiliser un partage de réseau spécifié dans View Persona Management ou un chemin d'accès configuré dans Active Directory afin de prendre en charge des profils itinérants de Windows.<br>Lorsque ce paramètre est activé, vous pouvez utiliser **Partager un chemin d'accès** pour déterminer l'emplacement du référentiel de profils d'utilisateur.<br>Dans la zone de texte **Partager un chemin d'accès**, vous spécifiez un chemin d'accès UNC vers un partage de réseau accessible aux postes de travail View Persona Management. Ce paramètre permet à View Persona Management de contrôler l'emplacement du référentiel de profils d'utilisateur.<br>Par exemple : `\\server.domain.com\VPRepository`<br>Si `%username%` ne fait pas partie du chemin de dossier que vous configurez, View Persona Management ajoute `%username%.%userdomain%` au chemin.<br>Par exemple : `\\server.domain.com\VPRepository\%username%.%userdomain%`<br>Si vous spécifiez un emplacement dans **Partager un chemin d'accès**, vous n'avez pas à régler des profils itinérants dans Windows ou à configurer un chemin de profil d'utilisateur dans Active Directory pour prendre en charge des profils itinérants de Windows.<br>Pour plus d'informations sur la configuration d'un partage de réseau UNC pour View Persona Management, reportez-vous à la section « Configurer un référentiel de profils d'utilisateur », page 357.<br>Par défaut, le chemin de profil d'utilisateur Active Directory est utilisé.<br>En particulier, lorsque **Partager un chemin d'accès** est laissé vide, le chemin de profil d'utilisateur Active Directory est utilisé. Le champ **Partager un Partager un chemin d'accès** est vide et inactif lorsque ce paramètre est désactivé ou n'est pas configuré. Vous pouvez également laisser le chemin vide lorsque ce paramètre est activé.<br>Lorsque ce paramètre est activé, vous pouvez cocher la case **Remplacer le chemin de profil d'utilisateur Active Directory s'il est configuré** pour vous assurer que View Persona Management utilise le chemin spécifié dans **Partager un chemin d'accès**. Par défaut, cette case est décochée, et View Persona Management utilise le chemin de profil d'utilisateur Active Directory lorsque les deux emplacements sont configurés. |

| Paramètre de stratégie de groupe | Description |
|---|---|
| Supprimer le persona local à la fermeture de session | Supprime de la machine virtuelle le profil de chaque utilisateur stocké localement lorsque celui-ci ferme une session.<br>Vous pouvez également cocher une case pour supprimer les dossiers de paramètres locaux de chaque utilisateur lorsque le profil d'utilisateur est supprimé. Si vous cochez cette case, le dossier `AppData\Local` est supprimé.<br>Pour voir des recommandations sur l'utilisation de ce paramètre, reportez-vous à la section « Meilleures pratiques pour la configuration d'un déploiement de View Persona Management », page 366.<br>Lorsque ce paramètre est désactivé ou n'est pas configuré, les profils d'utilisateur stockés localement, y compris les dossiers de paramètres locaux, ne sont pas supprimés lorsque les utilisateurs ferment une session. |
| Déplacer des dossiers de paramètres locaux | Déplace les dossiers de paramètres locaux avec le reste de chaque profil d'utilisateur.<br>Cette stratégie affecte le dossier `AppData\Local`.<br>Par défaut, les paramètres locaux ne sont pas déplacés. |
| Fichiers et dossiers à précharger | Spécifie une liste de fichiers et de dossiers téléchargés vers le profil d'utilisateur local quand l'utilisateur ouvre une session. Les modifications dans les fichiers sont copiées sur le référentiel distant au moment où elles se produisent.<br>Dans certaines situations, vous voulez peut-être précharger des fichiers et des dossiers spécifiques dans le profil d'utilisateur stocké localement. Utilisez ce paramètre pour spécifier ces fichiers et dossiers.<br>Spécifiez des chemins liés à la racine du profil local. Ne spécifiez pas de lecteur dans un nom de chemin d'accès.<br>Par exemple : `Application Data\Microsoft\Certificates`<br>Après le préchargement des fichiers et des dossiers spécifiés, View Persona Management gère les fichiers et les dossiers comme il gère d'autres données de profil. Lorsqu'un utilisateur met à jour des fichiers et des dossiers préchargés, View Persona Management copie les données mises à jour vers le référentiel de profils distant au cours de la session, au prochain intervalle de chargement du profil. |
| Fichiers et dossiers à précharger (exceptions) | Empêche le préchargement des fichiers et des dossiers spécifiés.<br>Les chemins de dossier sélectionnés doivent résider dans les dossiers que vous spécifiez dans le paramètre **Fichiers et dossiers à précharger**.<br>Spécifiez des chemins liés à la racine du profil local. Ne spécifiez pas de lecteur dans un nom de chemin d'accès. |
| Synchronisation de profils itinérants de Windows | Spécifie une liste de fichiers et de dossiers gérés par des profils itinérants de Windows standard. Les fichiers et les dossiers sont récupérés depuis le référentiel distant quand l'utilisateur ouvre une session. Les fichiers ne sont pas copiés sur le référentiel distant jusqu'à ce que l'utilisateur ferme une session.<br>Pour les fichiers et les dossiers spécifiés, View Persona Management ignore l'intervalle de réplication des profils configuré par le **Intervalle de chargement du profil** dans le paramètre **Gérer un persona d'utilisateur**.<br>Spécifiez des chemins liés à la racine du profil local. Ne spécifiez pas de lecteur dans un nom de chemin d'accès. |
| Synchronisation de profils itinérants de Windows (exceptions) | Les fichiers et les dossiers sélectionnés sont des exceptions aux chemins spécifiés dans le paramètre **Synchronisation de profils itinérants de Windows**.<br>Les chemins de dossier sélectionnés doivent résider dans les dossiers que vous spécifiez dans le paramètre **Synchronisation de profils itinérants de Windows**.<br>Spécifiez des chemins liés à la racine du profil local. Ne spécifiez pas de lecteur dans un nom de chemin d'accès. |

| Paramètre de stratégie de groupe | Description |
|---|---|
| Fichiers et dossiers exclus du déplacement | Spécifie une liste de fichiers et de dossiers qui ne sont pas déplacés avec le reste du profil d'utilisateur. Les fichiers et les dossiers spécifiés n'existent que sur le système local.<br>Certaines situations requièrent que des fichiers et des dossiers spécifiques résident uniquement dans le profil d'utilisateur stocké localement. Par exemple, vous pouvez exclure les fichiers temporaires et mis en cache du déplacement. Ces fichiers n'ont pas à être répliqués dans le référentiel distant.<br>Spécifiez des chemins liés à la racine du profil local. Ne spécifiez pas de lecteur dans un nom de chemin d'accès.<br>Par défaut, le dossier temp du profil d'utilisateur, le dossier du cache d'application ThinApp et les dossiers du cache pour Internet Explorer, Firefox, Chrome et Opera sont exclus du déplacement. |
| Fichiers et dossiers exclus du déplacement (exceptions) | Les fichiers et les dossiers sélectionnés sont des exceptions aux chemins spécifiés dans le paramètre **Fichiers et dossiers exclus du déplacement**.<br>Les chemins de dossier sélectionnés doivent résider dans les dossiers que vous spécifiez dans le paramètre **Fichiers et dossiers exclus du déplacement**.<br>Spécifiez des chemins liés à la racine du profil local. Ne spécifiez pas de lecteur dans un nom de chemin d'accès. |
| Activer le téléchargement en arrière-plan pour les ordinateurs portables | Télécharge tous les fichiers dans le profil d'utilisateur lorsqu'un utilisateur ouvre une session sur un ordinateur portable sur lequel le logiciel View Persona Management est installé. Les fichiers sont téléchargés en arrière-plan.<br>Lorsque l'opération est terminée, une notification contextuelle s'affiche sur l'écran de l'utilisateur : `Téléchargement en arrière-plan terminé`. Pour autoriser cette notification à apparaître sur l'ordinateur portable de l'utilisateur, vous devez activer le paramètre `Afficher des erreurs critiques aux utilisateurs via des alertes d'icône de la barre d'état`.<br>**Remarque** Si vous activez ce paramètre, il vous est recommandé d'en informer vos utilisateurs pour s'assurer que le profil est complètement téléchargé avant que les utilisateurs se déconnectent du réseau.<br>Si un utilisateur met un ordinateur portable autonome hors ligne avant la fin du téléchargement de profil, l'utilisateur peut ne pas avoir accès aux fichiers de profils locaux. Lorsque l'utilisateur est hors ligne, il ne peut pas ouvrir un fichier local qui n'a pas été complètement téléchargé.<br>Reportez-vous à la section « Gérer les profils d'utilisateur sur les ordinateurs portables autonomes », page 369. |
| Dossiers à télécharger en arrière-plan | Les dossiers sélectionnés sont téléchargés dans l'arrière-plan lorsqu'un utilisateur ouvre une session sur le poste de travail.<br>Dans certains cas, vous pouvez optimiser View Persona Management en téléchargeant le contenu de dossiers spécifiques dans l'arrière-plan. Avec ce paramètre, les utilisateurs n'ont pas à attendre que des fichiers volumineux se téléchargent lorsqu'ils démarrent une application. Les utilisateurs n'ont pas non plus besoin d'attendre la fin du préchargement des fichiers lorsqu'ils ouvrent une session, ce qui est le cas si vous utilisez le paramètre **Fichiers et dossiers à précharger** avec des fichiers très volumineux.<br>Par exemple, vous pouvez inclure des dossiers de sandbox ThinApp de VMware dans le paramètre **Dossiers à télécharger en arrière-plan**. Le téléchargement en arrière-plan n'affecte pas les performances lorsqu'un utilisateur ouvre une session ou utilise d'autres applications sur le poste de travail. Lorsque l'utilisateur démarre l'application ThinApp, les fichiers de sandbox ThinApp requis sont susceptibles d'être téléchargés depuis le référentiel distant, ce qui améliore l'heure de démarrage de l'application.<br>Spécifiez des chemins liés à la racine du profil local. Ne spécifiez pas de lecteur dans un nom de chemin d'accès. |
| Dossiers à télécharger en arrière-plan (exceptions) | Les dossiers sélectionnés sont des exceptions aux chemins spécifiés dans le paramètre **Dossiers à télécharger en arrière-plan**.<br>Les chemins de dossier sélectionnés doivent résider dans les dossiers que vous spécifiez dans le paramètre **Dossiers à télécharger en arrière-plan**.<br>Spécifiez des chemins liés à la racine du profil local. Ne spécifiez pas de lecteur dans un nom de chemin d'accès. |

| Paramètre de stratégie de groupe | Description |
|---|---|
| Processus exclus | L'E/S des processus spécifiés est ignorée par View Persona Management.<br>Vous pouvez avoir à ajouter certaines applications antivirus à la liste **Processus exclus** pour éviter tout problème de performance. Si une application antivirus ne dispose pas d'une fonction pour désactiver la récupération des fichiers hors ligne lors de ses analyses à la demande, le paramètre **Processus exclus** empêche l'application de récupérer les fichiers inutilement. Toutefois, View Persona Management ne réplique pas les modifications apportées aux fichiers et paramètres dans les profils des utilisateurs qui sont réalisés par des processus exclus.<br>Pour ajouter des processus à la liste **Processus exclus**, activez ce paramètre, cliquez sur **Afficher**, tapez le nom du processus et cliquez sur **OK**. Par exemple : **`process.exe`**. |
| Nettoyer des fichiers CLFS | Supprime les fichiers générés par le service Common Log File System (CLFS) pour `ntuser.dat` et `usrclass.dat` du profil itinérant à l'ouverture de session.<br>Activez ce paramètre uniquement si vous devez réparer des profils d'utilisateur qui rencontrent un problème avec ces fichiers. Sinon, laissez ce paramètre désactivé ou non configuré. |

## Paramètres de stratégie de groupe de redirection de dossiers

Avec des paramètres de stratégie de groupe de redirection de dossiers, vous pouvez rediriger des dossiers de profils d'utilisateur vers un partage de réseau. Lorsqu'un dossier est redirigé, toutes les données sont stockées directement sur le partage de réseau lors de la session utilisateur.

Vous pouvez utiliser ces paramètres pour rediriger des dossiers qui doivent être hautement disponibles. View Persona Management copie des mises à jour depuis le profil d'utilisateur local vers le profil distant au maximum une fois par minute, en fonction de la valeur que vous définissez pour l'intervalle de chargement du profil. Toutefois, si une panne réseau ou un échec sur le système local se produit, les mises à jour d'un utilisateur depuis la dernière réplication peuvent ne pas être enregistrées dans le profil distant. Dans les cas où les utilisateurs ne peuvent pas se permettre de perdre temporairement quelques minutes de leur travail récent, vous pouvez rediriger les dossiers qui stockent ces données critiques.

Les règles et recommandations suivantes s'appliquent à la redirection de dossiers :

- Lorsque vous activez ce paramètre pour un dossier, vous devez saisir le chemin d'accès UNC du partage de réseau vers lequel le dossier est redirigé.
- Si `%username%` ne fait pas partie du chemin de dossier que vous configurez, View Persona Management ajoute `%username%` au chemin d'accès UNC.
- Il vous est recommandé de configurer le chemin de dossier pour inclure `%username%`, mais assurez-vous que le dernier sous-dossier dans le chemin utilise le nom du dossier redirigé, tel que `My Videos`. Le dernier dossier dans le chemin est affiché sous la forme du nom de dossier sur le poste de travail de l'utilisateur. Pour plus d'informations, reportez-vous à « Configuration de chemins d'accès pour des dossiers redirigés », page 367.
- Vous configurez un paramètre séparé pour chaque dossier. Vous pouvez sélectionner des dossiers particuliers pour la redirection et en laisser d'autres sur le poste de travail View local. Vous pouvez également rediriger différents dossiers vers différents chemins d'accès UNC.
- Si un paramètre de redirection de dossiers est désactivé ou n'est pas configuré, le dossier est stocké sur le poste de travail View local et géré en fonction des paramètres de stratégie de groupe de View Persona Management.
- Si View Persona Management et des profils itinérants de Windows sont configurés pour rediriger le même dossier, la redirection de dossiers de View Persona Management est prioritaire sur les profils itinérants de Windows.

- La redirection de dossiers s'applique uniquement aux applications qui utilisent les API de shell Windows afin de rediriger des chemins de dossier communs. Par exemple, si une application écrit un fichier dans `%USERPROFILE%\AppData\Roaming`, le fichier est écrit dans le profil local et n'est pas redirigé vers l'emplacement réseau.
- Par défaut, la redirection du dossier Windows accorde aux utilisateurs des droits exclusifs sur les dossiers redirigés. Pour accorder aux administrateurs du domaine l'accès aux dossiers nouvellement redirigés, vous pouvez utiliser un paramètre de stratégie de groupe View Persona Management.

  La redirection des dossiers Windows comporte une case à cocher appelée **Accorder à l'utilisateur des droits exclusifs {nom de dossier} in italics** qui accorde à l'utilisateur spécifié des droits exclusifs sur le dossier redirigé. Par mesure de sécurité, cette case est cochée par défaut. Lorsque cette case est cochée, les administrateurs n'ont pas accès au dossier redirigé. Si un administrateur tente de forcer la modification des droits d'accès au dossier redirigé d'un utilisateur, View Persona Management ne fonctionne plus pour cet utilisateur.

  Vous pouvez rendre les dossiers nouvellement redirigés accessibles aux administrateurs du domaine à l'aide du paramètre de stratégie de groupe **Ajouter le groupe d'administrateurs aux dossiers redirigés**. Ce paramètre vous permet d'accorder au groupe d'administrateurs de domaine le contrôle total sur chaque dossier redirigé. Reportez-vous à la section Tableau 18-5.

  Pour les dossiers redirigés existants, consultez « Octroi d'un accès à des dossiers redirigés existants à des administrateurs de domaine », page 376.

Vous pouvez spécifier des chemins de dossier qui sont exclus de la redirection de dossier. Reportez-vous à la section Tableau 18-5.

**Avertissement** View ne prend pas en charge l'activation de la redirection de dossier vers un dossier qui se trouve déjà dans un profil géré par View Persona Management. Cette configuration peut provoquer des échecs dans View Persona Management et entraîner la perte de données utilisateur.

Par exemple, si le dossier racine dans le référentiel de profils distant est `\\Server\%username%\`, et si vous redirigez des dossiers vers `\\Server\%username%\Desktop`, ces paramètres peuvent provoquer l'échec de la redirection de dossier dans View Persona Management et la perte du contenu qui se trouvait précédemment dans le dossier `\\Server\%username%\Desktop`.

Vous pouvez rediriger les dossiers suivants vers un partage de réseau :

- Données d'application (itinérantes)
- Contacts
- Cookies
- Poste de travail
- Téléchargements
- Favoris
- Historique
- Liens
- Mes documents
- Ma musique
- Mes images
- Mes vidéos
- Voisinage réseau
- Voisinage imprimante

- Éléments récents
- Jeux sauvegardés
- Recherches
- Menu Démarrer
- Éléments de démarrage
- Modèles
- Fichiers Internet temporaires

**Tableau 18-5.** Paramètres de stratégie de groupe qui contrôlent la redirection de dossier

| Paramètre de stratégie de groupe | Description |
|---|---|
| Ajouter le groupe d'administrateurs aux dossiers redirigés | Détermine si le groupe d'administrateurs doit être ajouté à chaque dossier redirigé. Les utilisateurs disposent de droits exclusifs sur les dossiers redirigés par défaut. Lorsque vous activez ce paramètre, les administrateurs peuvent également accéder aux dossiers redirigés.<br>Par défaut, ce paramètre n'est pas configuré. |
| Fichiers et dossiers exclus de la redirection de dossier | Les chemins de fichier et de dossier sélectionnés ne sont pas redirigés vers un partage de réseau.<br>Dans certains scénarios, des fichiers et des dossiers spécifiques doivent rester dans le profil d'utilisateur local.<br>Pour ajouter un chemin de dossier à la liste **Fichiers et dossiers exclus de la redirection de dossier**, activez ce paramètre, cliquez sur **Afficher**, tapez le nom du chemin et cliquez sur **OK**.<br>Spécifiez des chemins de dossier liés à la racine du profil local de l'utilisateur. Par exemple : **`Poste de travail\Nouveau dossier`**. |
| Fichiers et dossiers exclus de la redirection de dossier (exceptions) | Les chemins de fichier et de dossier sélectionnés sont des exceptions aux chemins spécifiés dans le paramètre **Fichiers et dossiers exclus de la redirection de dossier**.<br>Pour ajouter un chemin de dossier à la liste **Fichiers et dossiers exclus de la redirection de dossier (exceptions)**, activez ce paramètre, cliquez sur **Afficher**, tapez le nom du chemin et cliquez sur **OK**.<br>Spécifiez les chemins de dossier qui résident dans un dossier spécifié dans le paramètre **Dossiers exclus de la redirection de dossier** et qui sont liés à la racine du profil local de l'utilisateur. Par exemple : **`Poste de travail\Nouveau dossier\Dossier unique`**. |

## Octroi d'un accès à des dossiers redirigés existants à des administrateurs de domaine

Par défaut, la redirection du dossier Windows accorde aux utilisateurs des droits exclusifs sur les dossiers redirigés. Pour accorder aux administrateurs de domaine un accès à des dossiers redirigés existants, vous devez employer l'utilitaire `icacls`.

Si vous configurez de nouveaux dossiers redirigés en vue d'une utilisation avec View Persona Management, vous pouvez rendre les nouveaux dossiers redirigés accessibles aux administrateurs de domaine en utilisant le paramètre de stratégie de groupe **Ajouter le groupe d'administrateurs aux dossiers redirigés**. Reportez-vous à la section Tableau 18-5.

### Procédure

1 Attribuez à l'administrateur la propriété des fichiers et des dossiers.

```
icacls "\\file-server\persona-share\*" /setowner "domain\admin" /T /C /L /Q
```

Par exemple : `icacls "\\myserver-123abc\folders\*" /setowner "mycompanydomain\vcadmin" /T /C /L /Q`

2 Modifiez les listes de contrôle d'accès pour les fichiers et les dossiers.

```
icacls "\\file-server\persona-share\*" /grant "admin-group":F /T /C /L /Q
```

Par exemple : `icacls "\\myserver-123abc\folders\*" /grant "Domain-Admins":F /T /C /L /Q`

3 Pour chaque dossier d'utilisateur, réattribuez la propriété, de l'administrateur à l'utilisateur correspondant.

```
icacls "\\file-server\persona-share\*" /setowner "domain\folder-owner" /T /C /L /Q
```

Par exemple : `icacls "\\myserver-123abc\folders\*" /setowner "mycompanydomain\user1" /T /C /L /Q`

## Paramètres de stratégie de groupe d'interface utilisateur de poste de travail

Les paramètres de stratégie de groupe d'interface utilisateur de poste de travail contrôlent les paramètres de View Persona Management que les utilisateurs voient sur leurs postes de travail.

| Paramètre de stratégie de groupe | Description |
|---|---|
| Hide local offline file icon (Masquer les icônes des fichiers hors ligne locaux) | Détermine si l'icône hors ligne est masquée lorsqu'un utilisateur voit les fichiers stockés localement qui appartiennent au profil d'utilisateur. L'activation de ce paramètre masque l'icône hors ligne dans Windows Explorer et dans la plupart des boîtes de dialogue de Windows.<br>Par défaut, l'icône hors ligne est masquée. |
| Show progress when downloading large files (Afficher la progression lors du téléchargement de fichiers volumineux) | Détermine si une fenêtre de progression s'affiche sur le poste de travail d'un utilisateur quand le client récupère des fichiers volumineux depuis le référentiel distant.<br>Quand ce paramètre est activé, vous pouvez spécifier la taille de fichier minimale, en mégaoctets, pour commencer à afficher la fenêtre de progression. La fenêtre s'affiche lorsque View Persona Management détermine que la quantité spécifiée de données sera récupérée depuis le référentiel distant. Cette valeur représente l'ensemble des fichiers récupérés en même temps.<br>Par exemple, si la valeur du paramètre est 50 Mo et qu'un fichier de 40 Mo est récupéré, la fenêtre ne s'affiche pas. Si un fichier de 30 Mo est récupéré et que le premier fichier est toujours en cours de téléchargement, l'ensemble du téléchargement dépasse la valeur et la fenêtre de progression s'affiche. La fenêtre apparaît lorsque le téléchargement d'un fichier démarre.<br>Par défaut, cette valeur est de 50 Mo.<br>Par défaut, cette fenêtre de progression ne s'affiche pas. |
| Show critical errors to users via tray icon alerts (Afficher des erreurs critiques aux utilisateurs via des alertes d'icône de la barre d'état) | Affiche des alertes d'icône d'erreur critique dans la barre d'état du poste de travail lorsque des échecs de réplication ou de connectivité réseau se produisent.<br>Par défaut, ces alertes d'icône sont masquées. |

## Paramètres de stratégie de groupe de journalisation

Les paramètres de stratégie de groupe de journalisation déterminent le nom, l'emplacement et le comportement des fichiers journaux de View Persona Management.

La configuration de journalisation de View Persona Management est simplifiée dans Horizon 6 version 6.1 et versions ultérieures. Pour utiliser les paramètres de journalisation mis à jour, vous devez mettre à niveau le fichier ADM de View Persona Management, `ViewPM.adm`, vers la version qui est fournie avec Horizon 6 version 6.1 avec View ou version ultérieure.

| Paramètre de stratégie de groupe | Description |
|---|---|
| Logging filename (Nom de fichier de journalisation) | Spécifie le nom de chemin complet du fichier journal de View Persona Management local.<br>Le chemin par défaut est `ProgramData\VMware\VDM\logs\`*`filename`*.<br>Le nom de fichier de journalisation par défaut est `VMWVvp.txt`. |
| Logging destination (Destination de journalisation) | Détermine si tous les messages du journal sont écrits dans le fichier journal, dans le port de débogage ou dans les deux destinations.<br>Par défaut, les messages de journalisation sont envoyés vers le fichier journal. |
| Logging flags (Indicateurs de journalisation) | Spécifie le type de messages de journalisation générés.<br>■ messages d'information de journalisation ;<br>■ messages de débogage de journalisation.<br>Lorsque ce paramètre est désactivé ou non configuré et que, par défaut lorsque le paramètre est configuré, les messages de journalisation sont définis au niveau des informations. |
| Profondeur d'historique des journaux | Détermine le nombre de fichiers journaux d'historique conservés par View Persona Management.<br>Vous pouvez conserver entre un et dix fichiers journaux d'historique au maximum.<br>Par défaut, un seul fichier journal d'historique est conservé. |
| Télécharger le journal sur le réseau | Télécharge le fichier journal de View Persona Management sur le partage réseau spécifié lorsque l'utilisateur ferme la session.<br>Lorsque ce paramètre est activé, spécifiez le chemin du partage réseau. Le chemin du partage réseau doit être un chemin UNC. View Persona Management ne crée pas le partage réseau.<br>Par défaut, le fichier journal n'est pas téléchargé sur le partage réseau. |

# Dépannage de machines et de pools de postes de travail 19

Vous avez la possibilité d'utiliser différentes procédures pour diagnostiquer et résoudre les problèmes que vous pouvez rencontrer lorsque vous créez et utilisez des machines et des pools de postes de travail.

Les utilisateurs peuvent rencontrer des difficultés lorsqu'ils utilisent Horizon Client pour accéder aux postes de travail et aux applications. Vous pouvez utiliser des procédures de dépannage pour rechercher les causes de tels problèmes et essayer de les corriger vous-même, ou vous pouvez obtenir de l'aide du support technique de VMware.

Ce chapitre aborde les rubriques suivantes :



## Afficher les machines problématiques

Vous pouvez afficher la liste des machines pour lesquelles View a détecté un fonctionnement suspect.

View Administrator affiche les machines qui présentent les problèmes suivants :

- Allumés mais ne répondent pas.
- Restent dans l'état d'approvisionnement pendant un long moment.
- Sont prêts mais signalent qu'ils n'acceptent pas les connexions.
- Apparaissent manquants sur un serveur vCenter Server.
- Ont des connexions actives sur la console, des connexions par des utilisateurs non autorisés ou des connexions non effectuées via une instance du Serveur de connexion View.

### Procédure

1. Dans View Administrator, sélectionnez **Ressources > Machines**.
2. Dans l'onglet **Machines virtuelles vCenter**, cliquez sur **Machines problématiques**.

### Suivant

La mesure à prendre dépend du problème signalé par View Administrator pour une machine.

- Si une machine de clone lié est dans un état d'erreur, le mécanisme de récupération automatique de View tente de mettre sous tension, ou d'arrêter et de redémarrer, le clone lié. Si des tentatives de récupération répétées échouent, le clone lié est supprimé. Dans certaines situations, un clone lié peut être supprimé et recréé plusieurs fois. Reportez-vous à la section « Dépannage de machines qui sont supprimées et recréées à plusieurs reprises », page 387.
- Si une machine est sous tension, mais ne répond pas, redémarrez sa machine virtuelle. Si la machine ne répond toujours pas, vérifiez que la version d'Horizon Agent est prise en charge pour le système d'exploitation de la machine. Vous pouvez utiliser la commande `vdmadmin` avec l'option `–A` pour afficher la version d'Horizon Agent. Pour plus d'informations, reportez-vous au document *Administration de View*.
- Si une machine reste dans l'état de provisionnement pendant une période prolongée, supprimez sa machine virtuelle et clonez-la de nouveau. Vérifiez que l'espace disque est suffisant pour provisionner la machine. Reportez-vous à la section « Des machines virtuelles sont bloquées dans l'état d'approvisionnement », page 385.
- Si une machine signale qu'elle est prête, mais qu'elle n'accepte pas les connexions, vérifiez la configuration du pare-feu pour vous assurer que le protocole d'affichage n'est pas bloqué. Reportez-vous à la section « Problèmes de connexion entre des machines et des instances du Serveur de connexion View », page 392.
- Si une machine semble manquante sur un serveur vCenter Server, vérifiez si sa machine virtuelle est configurée sur le serveur vCenter Server prévu ou si elle a été déplacée vers un autre serveur vCenter Server.
- Si une machine dispose d'une ouverture de session active, mais qu'elle ne figure pas sur la console, la session doit être distante. Si vous ne pouvez pas contacter les utilisateurs connectés, vous devrez peut-être redémarrer la machine virtuelle pour fermer les sessions des utilisateurs de force.

## Envoyer des messages à des utilisateurs de poste de travail

Vous devez parfois avoir à envoyer des messages à des utilisateurs dont la session est actuellement ouverte sur des postes de travail. Par exemple, si vous devez effectuer une maintenance sur une machine, vous pouvez demander aux utilisateurs de fermer provisoirement leur session ou les prévenir d'une prochaine interruption de service. Vous pouvez envoyer un message à plusieurs utilisateurs.

### Procédure

1. Dans View Administrator, cliquez sur **Catalogue > Pools de postes de travail**.
2. Double-cliquez sur un pool et cliquez sur l'onglet **Sessions**.
3. Sélectionnez une ou plusieurs machines et cliquez sur **Envoyer un message**.
4. Saisissez le message, sélectionnez le type de message et cliquez sur **OK**.

   Un message peut être du type **Infos**, **Avertissement** ou **Erreur**.

Le message est envoyé à toutes les machines sélectionnées dans les sessions actives.

# Problèmes lors du provisionnement ou de la recréation d'un pool de postes de travail

Vous pouvez utiliser plusieurs procédures pour le diagnostic et la résolution de problèmes liés au provisionnement ou à la recréation de pools de postes de travail.

## Échec du provisionnement de clone instantané ou de l'image de transfert

L'image en attente d'un pool de postes de travail de clone instantané est dans un état d'échec.

### Problème

Lors de la création d'un pool ou d'une opération d'image de transfert, le message d'erreur `Fault type is SERVER_FAULT_FATAL – Runtime error: Method called after shutdown was initiated (Type d'erreur SERVER_FAULT_FATAL – Erreur d'exécution : méthode appelée après l'amorce de l'arrêt)` s'affiche.

### Cause

Cela peut se produire occasionnellement lorsqu'un Serveur de connexion réplica est démarré alors qu'un autre Serveur de connexion effectue des opérations d'image.

### Solution

- Si l'erreur se produit lors de la création d'un pool, activez le provisionnement s'il est désactivé. S'il est activé, désactivez-le, puis activez-le.
- Si l'erreur se produit lors d'une opération d'image de transfert, initiez une autre opération d'image de transfert avec la même image.

## Échec de la publication de l'image de clone instantané

View Administrator indique qu'une publication d'image a échoué.

### Problème

Après avoir créé un pool de postes de travail de clone instantané ou initié une image de transfert, vous vérifiez l'état de l'opération et View Administrator indique que la publication d'image a échoué.

### Solution

- Réactivez le provisionnement, s'il est désactivé. S'il est activé, désactivez-le, puis activez-le. Cela force View à déclencher une nouvelle opération de publication initiale.
- S'il s'avère que l'image actuelle contient des problèmes, initiez une autre opération d'image de transfert avec une image différente.

### Suivant

Si la publication d'image échoue à plusieurs reprises, attendez 30 minutes et réessayez.

## Récupération d'erreur sans fin lors du provisionnement de clone instantané

La récupération d'erreur entre dans une boucle sans fin lors du provisionnement d'un pool de postes de travail de clone instantané.

### Problème

Lors du provisionnement, les clones instantanés peuvent entrer dans un état d'erreur avec le message « Aucune connexion réseau entre Agent et le Serveur de connexion ». Le mécanisme de récupération d'erreur automatique supprime et recrée les clones, qui passent dans le même état d'erreur, et le processus se répète indéfiniment.

### Cause

Parmi les causes possibles, on compte une erreur réseau permanente ou un chemin incorrect vers le script post-personnalisation.

### Solution

- Résolvez l'erreur dans le réseau ou dans le chemin vers le script post-personnalisation.

## Impossible de supprimer des clones instantanés orphelins

Très rarement, lors du provisionnement, un clone instantané passe dans un état d'erreur et vous ne pouvez pas supprimer le pool de postes de travail de View Administrator.

### Problème

Pour supprimer le pool, View envoie des demandes à vCenter Server pour désactiver les clones. Toutefois, les demandes échouent pour les clones orphelins. Cela se traduit par le fait que View ne peut pas supprimer le pool.

### Solution

1. Dans vCenter Server, désinscrivez les clones orphelins.
2. Dans View Administrator, supprimez les clones.

## La création de pool échoue si des spécifications de personnalisation sont introuvables

Si vous essayez de créer un pool de postes de travail, l'opération échoue si les spécifications de personnalisation sont introuvables.

### Problème

Vous ne pouvez pas créer de pool de postes de travail et vous voyez le message suivant dans la base de données des événements.

```
Provisioning error occurred for Machine <varname>Machine_Name</varname>: Customization failed
for Machine (Une erreur d'approvisionnement s'est produite pour la machine
<varname>Machine_Name</varname> : échec de la personnalisation pour la machine)
```

### Cause

La cause la plus probable de ce problème est que vous disposez d'autorisations insuffisantes pour accéder aux spécifications de personnalisation ou pour créer un pool. Une autre cause possible est que la spécification de personnalisation a été renommée ou supprimée.

### Solution

- Vérifiez que vous disposez d'autorisations suffisantes pour accéder aux spécifications de personnalisation et pour créer un pool.
- Si la spécification de personnalisation n'existe plus car elle a été renommée ou supprimée, choisissez une spécification différente.

## La création de pool échoue à cause d'un problème d'autorisations

Vous ne pouvez pas créer de pool de postes de travail s'il y a un problème d'autorisations avec un hôte ESX/ESXi, un cluster ESX/ESXi ou le datacenter.

### Problème

Vous ne pouvez pas créer de pool de postes de travail dans View Administrator car les modèles, l'hôte ESX/ESXi, le cluster ESX/ESXi ou le datacenter ne sont pas accessibles.

### Cause

Ce problème a plusieurs causes possibles.

- Vous ne disposez pas des autorisations correctes pour créer un pool.
- Vous ne disposez pas des autorisations correctes pour accéder aux modèles.
- Vous ne disposez pas des autorisations correctes pour accéder à l'hôte ESX/ESXi, au cluster ESX/ESXi ou au datacenter.

### Solution

- Si l'écran Template Selection (Sélection de modèle) n'indique aucun modèle disponible, vérifiez que vous disposez d'autorisations suffisantes pour accéder aux modèles.
- Vérifiez que vous disposez d'autorisations suffisantes pour accéder à l'hôte ESX/ESXi, au cluster ESX/ESXi ou au datacenter.
- Vérifiez que vous disposez d'autorisations suffisantes pour créer un pool.

## L'approvisionnement de pool échoue à cause d'un problème de configuration

Si un modèle n'est pas disponible ou qu'une image de machine virtuelle a été déplacée ou supprimée, l'approvisionnement d'un pool de postes de travail peut échouer.

### Problème

Un pool de postes de travail n'est pas approvisionné et vous voyez le message suivant dans la base de données des événements.

```
Provisioning error occurred on Pool <varname>Desktop_ID</varname> because of a configuration
problem (Une erreur d'approvisionnement s'est produite sur le pool <varname>Desktop_ID</varname>
à cause d'un problème de configuration)
```

### Cause

Ce problème a plusieurs causes possibles.

- Un modèle n'est pas accessible.
- Le nom d'un modèle a été modifié dans vCenter.
- Un modèle a été déplacé vers un dossier différent dans vCenter.
- Une image de machine virtuelle a été déplacée entre des hôtes ESX/ESXi ou elle a été supprimée.

### Solution

- Vérifiez que le modèle est accessible.
- Vérifiez que le nom et le dossier corrects sont spécifiés pour le modèle.
- Si une image de machine virtuelle a été déplacée entre des hôtes ESX/ESXi, déplacez la machine virtuelle vers le bon dossier vCenter.

- Si une image de machine virtuelle a été supprimée, supprimez l'entrée pour la machine virtuelle dans View Administrator et recréez ou restaurez l'image.

## L'approvisionnement de pool échoue à cause d'une instance du Serveur de connexion View incapable de se connecter à vCenter

Si un serveur de connexion ne peut pas se connecter à vCenter, l'approvisionnement d'un pool de postes de travail peut échouer.

### Problème

L'approvisionnement d'un pool de postes de travail échoue et vous voyez l'un des messages d'erreur suivants dans la base de données des événements.

- `Cannot log in to vCenter at address VC_Address (Impossible d'ouvrir une session sur vCenter à l'adresse VC_Address)`
- `The status of vCenter at address VC_Address is unknown (L'état de vCenter à l'adresse VC_Address est inconnu)`

### Cause

L'instance du Serveur de connexion View ne peut pas se connecter à vCenter pour l'une des raisons suivantes.

- Le service Web sur le serveur vCenter Server s'est arrêté.
- Il existe des problèmes de réseau entre l'hôte du Serveur de connexion View et le serveur vCenter Server.
- Les numéros de port et les informations d'ouverture de session pour vCenter ou View Composer ont été modifiés.

### Solution

- Vérifiez que le service Web s'exécute sur le serveur vCenter.
- Vérifiez qu'il n'y a pas de problème de réseau entre l'hôte du Serveur de connexion View et le serveur vCenter.
- Dans View Administrator, vérifiez les numéros de port et les informations d'ouverture de session qui sont configurés pour vCenter et View Composer.

## L'approvisionnement de pool échoue à cause de problèmes liés au magasin de données

Si un magasin de données n'a plus d'espace disque ou que vous n'avez pas l'autorisation d'accéder au magasin de données, l'approvisionnement d'un pool de postes de travail peut échouer.

### Problème

L'approvisionnement d'un pool de postes de travail échoue et vous voyez l'un des messages d'erreur suivants dans la base de données des événements.

- `Provisioning error occurred for Machine Machine_Name: Cloning failed for Machine (Une erreur d'approvisionnement s'est produite pour la machine Machine_Name : échec du clonage pour la machine)`
- `Provisioning error occurred on Pool Desktop_ID because available free disk space is reserved for linked clones (Une erreur d'approvisionnement s'est produite sur le pool Desktop_ID car l'espace disque libre est réservé aux clones liés)`

- `Provisioning error occurred on Pool Desktop_ID because of a resource problem (Une erreur d'approvisionnement s'est produite sur le pool Desktop_ID à cause d'un problème de ressource)`

### Cause

Vous n'avez pas l'autorisation d'accéder au magasin de données sélectionné ou le magasin de données utilisé pour le pool n'a plus d'espace disque.

### Solution

- Vérifiez que vous disposez d'autorisations suffisantes pour accéder au magasin de données sélectionné.
- Vérifiez si le disque sur lequel le magasin de données est configuré est plein.
- Si le disque est plein ou si l'espace est réservé, libérez de l'espace sur le disque, rééquilibrez les magasins de données disponibles ou migrez le magasin de données vers un disque plus volumineux.

## L'approvisionnement de pool échoue car vCenter Server est surchargé

Si vCenter Server est surchargé par des demandes, l'approvisionnement d'un pool de postes de travail peut échouer.

### Problème

L'approvisionnement d'un pool de postes de travail échoue et vous voyez le message d'erreur suivant dans la base de données des événements.

```
Une erreur d'approvisionnement s'est produite sur le pool <varname
id="varname_76C2270646664C0B89AC2F37A5F3F201">Desktop_ID</varname> en raison de l'expiration
d'un délai d'attente lors d'une personnalisation
```

### Cause

vCenter est surchargé par des demandes.

### Solution

- Dans View Administrator, réduisez le nombre maximal d'opérations d'approvisionnement et d'alimentation simultanées pour vCenter Server.
- Configurez des instances de vCenter Server supplémentaires.

  Pour plus d'informations sur la configuration de vCenter Server, reportez-vous au document *Installation de View*.

## Des machines virtuelles sont bloquées dans l'état d'approvisionnement

Après leur clonage, des machines virtuelles sont bloquées dans l'état Provisioning (Approvisionnement).

### Problème

Des machines virtuelles sont bloquées dans l'état Provisioning (Approvisionnement).

### Cause

La cause la plus probable de ce problème est que vous avez redémarré l'instance du Serveur de connexion View au cours d'une opération de clonage.

### Solution

- Supprimez les machines virtuelles et clonez-les de nouveau.

## Des machines virtuelles sont bloquées dans l'état de personnalisation

Après leur clonage, des machines virtuelles sont bloquées dans l'état Customizing (Personnalisation).

### Problème

Des machines virtuelles sont bloquées dans l'état Customizing (Personnalisation).

### Cause

La cause la plus probable de ce problème est qu'il n'y a pas suffisamment d'espace disque pour démarrer la machine virtuelle. Une machine virtuelle doit démarrer avant que la personnalisation puisse avoir lieu.

### Solution

- Supprimez la machine virtuelle pour restaurer d'une personnalisation bloquée.
- Si le disque est plein, libérez de l'espace sur le disque ou migrez le magasin de données vers un disque plus volumineux.

## Retrait des clones liés orphelins ou supprimés

Sous certaines conditions, les données de clone lié dans View, View Composer et vCenter Server peuvent être désynchronisées, et vous risquez de ne pas pouvoir provisionner ni supprimer des machines de clone lié.

### Problème

- Vous ne pouvez pas approvisionner un pool de postes de travail de clone lié.
- Le provisionnement de machines de clones liés échoue et l'erreur suivante se produit : `Une machine virtuelle comportant une spécification d'entrée existe déjà`
- Dans View Administrator, les machines de clone lié sont bloquées dans un état `Deleting`. Vous ne pouvez pas redémarrer la commande Supprimer dans View Administrator, car les machines sont déjà dans l'état `Deleting`.

### Cause

Ce problème se produit si la base de données View Composer contient des informations sur les clones liés qui sont incohérentes avec les informations dans View LDAP, Active Directory ou vCenter Server. Plusieurs situations peuvent provoquer cette incohérence :

- Le nom de la machine virtuelle de clone lié est modifié manuellement dans vCenter Server après la création du pool, ce qui entraîne View Composer et vCenter Server à se reporter à la même machine virtuelle avec des noms différents.
- Un échec de stockage ou une opération manuelle provoque la suppression de la machine virtuelle de vCenter Server. Les données de la machine virtuelle de clone lié existent toujours dans la base de données View Composer, View LDAP et Active Directory.
- Pendant qu'un pool est supprimé de View Administrator, un échec de réseau ou autre laisse la machine virtuelle dans vCenter Server.

### Solution

Si la machine virtuelle a été renommée dans vSphere Client après l'approvisionnement du pool de postes de travail, essayez de renommer la machine virtuelle avec le nom qui était utilisé lorsqu'elle a été déployée dans View.

Si d'autres informations sur la base de données sont incohérentes, utilisez la commande `SviConfig RemoveSviClone` pour supprimer ces éléments :

- Les entrées de base de données de clone lié de la base de données View Composer
- Le compte de machine de clone lié d'Active Directory
- La machine virtuelle de clone lié de vCenter Server

L'utilitaire `SviConfig` partage le même emplacement que l'application View Composer. Le chemin d'accès par défaut est `C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe`.

---

**Important** Seuls les administrateurs de View Composer expérimentés doivent employer l'utilitaire `SviConfig`. Cet utilitaire est conçu pour résoudre des problèmes liés au service View Composer.

---

Procédez comme suit :

1. Vérifiez que le service View Composer est en cours d'exécution.
2. À partir d'une invite de commande Windows sur l'ordinateur View Composer, exécutez la commande `SviConfig RemoveSviClone` au format suivant :

   ```
   sviconfig -operation=removesviclone
             -VmName=virtual machine name
             [-AdminUser=local administrator username]
             -AdminPassword=local administrator password
             [-ServerUrl=View Composer server URL]
   ```

   Par exemple :

   ```
   sviconfig -operation=removesviclone -vmname=MyLinkedClone
    -adminuser=Admin -adminpassword=Pass -serverurl=ViewComposerURL
   ```

   Les paramètres `VmName` et `AdminPassword` sont requis. La valeur par défaut du paramètre `AdminUser` est `Administrator`. La valeur par défaut du paramètre `ServerURL` est `https://localhost:18443/SviService/v2_0`

Pour plus d'informations sur la suppression des informations de machines virtuelles de View LDAP, consultez l'article 2015112 de la base de connaissances VMware : *Manually deleting linked clones or stale virtual desktop entries from the View Composer database in VMware View Manager and VMware Horizon View (Suppression manuelle de clones liés ou d'entrées de postes de travail virtuels périmées de la base de données View Composer dans VMware View Manager et VMware Horizon View)*.

## Dépannage de machines qui sont supprimées et recréées à plusieurs reprises

View peut supprimer et recréer à plusieurs reprises des machines de clone lié et de clone complet dont l'état est Erreur.

### Problème

Une machine de clone lié ou de clone complet est créée dans l'état Erreur, supprimée, puis recréée dans l'état Erreur. Ce cycle se répète sans cesse.

### Cause

Lorsqu'un pool de postes de travail important est approvisionné, une ou plusieurs machines virtuelles peuvent finir avec un état d'erreur. Le mécanisme de récupération automatique de View tente de mettre sous tension la machine virtuelle en échec. Si la machine virtuelle ne se met pas sous tension après un certain nombre de tentatives, View la supprime.

Conformément aux spécifications de dimensionnement de pool, View crée un nouvelle machine virtuelle, généralement avec le même nom de machine que celle d'origine. Si la nouvelle machine virtuelle est approvisionnée avec la même erreur, elle est supprimée et le cycle se répète.

La récupération automatique s'effectue sur des machines de clone lié et de clone complet.

Si les tentatives de récupération automatique échouent pour une machine virtuelle, View supprime celle-ci uniquement s'il s'agit d'une machine flottante ou d'une machine dédiée qui n'est pas attribuée à un utilisateur. De plus, View ne supprime pas des machines virtuelles lorsque le provisionnement de pool est désactivé.

### Solution

Examinez la machine virtuelle parente ou le modèle qui a été utilisé pour créer le pool de postes de travail. Recherchez les erreurs dans la machine virtuelle ou le système d'exploitation client qui peuvent causer l'erreur dans la machine virtuelle.

Pour les clones liés, résolvez les erreurs dans la machine virtuelle parente et prenez un nouveau snapshot.

- Si de nombreux postes de travail se trouvent dans l'état Erreur, utilisez le nouveau snapshot ou modèle pour recréer le pool.
- Si la plupart des machines sont saines, sélectionnez le pool de postes de travail dans View Administrator, cliquez sur **Modifier**, sélectionnez l'onglet Paramètres de vCenter, sélectionnez le nouveau snapshot comme image de base par défaut et enregistrez vos modifications.

  Les nouvelles machines de clone lié sont créées à l'aide du nouveau snapshot.

Pour les clones complets, résolvez les erreurs dans la machine virtuelle, générez un nouveau modèle et recréez le pool.

## Résolution de problèmes de personnalisation de QuickPrep

Un script de personnalisation QuickPrep de View Composer peut échouer pour plusieurs raisons.

### Problème

Un script de post-synchronisation ou de désactivation QuickPrep ne s'exécute pas. Dans certains cas, un script peut s'exécuter correctement sur certains clones liés et échouer sur d'autres.

### Cause

Quelques causes communes existes pour les problèmes de script QuickPrep :

- Le script expire.
- Le chemin du script fait référence à un script qui requiert un interprète.
- Le compte sous lequel le script s'exécute ne dispose pas d'autorisations suffisantes pour exécuter une tâche de script.

### Solution

- Examinez le journal du script de personnalisation.

  Les informations de personnalisation QuickPrep sont inscrites dans un fichier journal dans le répertoire `temp` de Windows :

  ```
  C:\Windows\Temp\vmware-viewcomposer-ga-new.log
  ```

- Déterminez si le script est expiré.

  View Composer termine un script de personnalisation qui dure plus de 20 secondes. Le fichier journal affiche un message indiquant que le script a démarré et un autre message indiquant l'expiration :

  ```
  2010-02-21 21:05:47,687 [1500] INFO Ready -
  [Ready.cpp, 102] Running the PostSync script: cmd /c
  C:\temp\build\composer.bat
  2010-02-21 21:06:07,348 [1500] FATAL Guest -
  [Guest.cpp, 428] script cmd /c
  C:\temp\build\composer.bat timed out
  ```

  Pour résoudre un problème d'expiration, augmentez la limite d'expiration pour le script et exécutez-le de nouveau.

- Déterminez si le chemin du script est valide.

  Si vous utilisez un langage de script qui a besoin d'un interprète pour exécuter le script, le chemin du script doit démarrer par le binaire de l'interprète.

  Par exemple, si vous spécifiez le chemin d'accès `C:\script\myvb.vbs` en tant que script de personnalisation QuickPrep, View Composer Agent ne peut pas exécuter le script. Vous devez spécifier un chemin qui démarre par le chemin du binaire de l'interprète :

  ```
  C:\windows\system32\cscript.exe c:\script\myvb.vbs
  ```

- Déterminez si le compte sous lequel le script s'exécute dispose d'autorisations appropriées pour effectuer des tâches de script.

  QuickPrep exécute les scripts sous le compte dans lequel le service VMware View Composer Guest Agent Server est configuré pour être exécuté. Par défaut, ce compte est `système local`.

  Ne modifiez pas ce compte d'ouverture de session. Si vous le faites, les clones liés ne démarrent pas.

## Recherche et suppression de la protection des réplicas View Composer inutilisés

Dans certains cas, les réplicas View Composer peuvent rester dans vCenter Server lorsqu'ils n'ont plus de clones liés associés.

### Problème

Un réplica inutilisé reste dans un dossier vCenter Server. Vous ne pouvez pas supprimer le réplica en utilisant vSphere Client.

### Cause

Les indisponibilités de réseau au cours des opérations View Composer ou de la suppression des clones liés associés directement depuis vSphere sans utiliser les commandes View appropriées, peut laisser un réplica inutilisé dans vCenter Server.

Les réplicas sont des entités protégées dans vCenter Server. Ils ne peuvent pas être supprimés avec les commandes de gestion ordinaires de vCenter Server ou de vSphere Client.

### Solution

Utilisez la commande `SviConfig FindUnusedReplica` pour rechercher le réplica dans un dossier donné. Vous pouvez utiliser le paramètre `-Move` pour transférer le réplica vers un autre dossier. Le paramètre `-Move` lève la protection d'un réplica inutilisé avant de le déplacer.

---

**Important** Seuls les administrateurs de View Composer expérimentés doivent employer l'utilitaire `SviConfig`. Cet utilitaire est conçu pour résoudre des problèmes liés au service View Composer.

---

L'utilitaire `SviConfig` partage le même emplacement que l'application View Composer. Le chemin d'accès par défaut est `C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe`.

Avant de commencer, vérifiez qu'aucun clone lié n'est associé au réplica.

Familiarisez-vous avec les paramètres `SviConfig FindUnusedReplica` :

- `DsnName`. DSN qui doit être utilisé pour se connecter à la base de données.
- `UserName`. Nom d'utilisateur utilisé pour se connecter à la base de données. Si ce paramètre n'est pas spécifié, l'authentification Windows est utilisée.
- `Password (Mot de passe)`. Mot de passe de l'utilisateur qui se connecte à la base de données. Si ce paramètre n'est pas spécifié et si l'authentification Windows n'est pas utilisée, vous êtes invité à entrer le mot de passe ultérieurement.
- `ReplicaFolder`. Nom du dossier de réplica. Utilisez une chaîne vide pour le dossier racine. La valeur par défaut est `VMwareViewComposerReplicaFolder`.
- `UnusedReplicaFolder`. Nom du dossier devant contenir tous les réplicas inutilisés. La valeur par défaut est `UnusedViewComposerReplicaFolder`. Utilisez ce paramètre pour définir le dossier de destination lorsque vous utilisez le paramètre `Move`.
- `OutputDir`. Nom du répertoire de sortie dans lequel la liste des réplicas inutilisés stockés dans le fichier `unused-replica-*.txt` est générée. La valeur par défaut est le répertoire de travail en cours.
- `Move`. Détermine s'il est nécessaire de lever la protection des machines virtuelles de réplica inutilisés et de les transférer vers un dossier défini. Le paramètre `UnusedReplicaFolder` spécifie le dossier de destination. La valeur par défaut du paramètre `Move` est `false`.

Les paramètres `DsnName`, `Username` et `Password` sont obligatoires. `DsnName` ne peut pas être une chaîne vide.

Procédez comme suit :

1. Arrêtez le service View Composer.
2. À partir d'une invite de commande Windows sur l'ordinateur View Composer, exécutez la commande `SviConfig FindUnusedReplica` au format suivant :

   ```
   sviconfig -operation=findunusedreplica
             -DsnName=name of the DSN
             -Username=Database administrator username
             -Password=Database administrator password
             [-ReplicaFolder=Replica folder name]
             [-UnusedReplicaFolder=Unused replica folder name.]
             [-OutputDir=Output file directory]
             [-Move=true or false]
   ```

   Par exemple :

   ```
   sviconfig -operation=FindUnusedReplica -DsnName=SVI
      -Username=SVIUser -Password=1234 -Move=True
   ```

3. Redémarrez le service View Composer.
4. (Facultatif) Une fois le réplica transféré vers le nouveau dossier, supprimez la machine virtuelle de réplica de vCenter Server.

## Erreurs d'approvisionnement de View Composer

Si une erreur se produit lorsque View Composer provisionne ou recompose des machines de clone lié, un code d'erreur indique la cause de l'échec. Le code d'erreur s'affiche dans la colonne d'état de la machine dans View Administrator.

Tableau 19-1 décrit les codes d'erreur d'approvisionnement de View Composer.

Ce tableau répertorie les erreurs associées à View Composer et à la personnalisation de QuickPrep. D'autres erreurs peuvent se produire dans le Serveur de connexion View et dans d'autres composants de View pouvant interférer avec le provisionnement de machine.

**Tableau 19-1.** Erreurs d'approvisionnement de View Composer

| Erreur | Description |
|---|---|
| 0 | La règle a été appliquée correctement.<br>**Remarque** Le code de résultat 0 n'apparaît pas dans View Administrator. La machine de clone lié passe à l'état Prêt, sauf si une erreur View se produit en dehors du domaine de View Composer. Ce code de résultat est inclus pour couvrir tous les cas de figure. |
| 1 | Échec de définition du nom de l'ordinateur. |
| 2 | Échec de redirection des profils d'utilisateur vers le disque persistant de View Composer. |
| 3 | Échec de définition du mot de passe du compte de domaine de l'ordinateur. |
| 4 | Échec de sauvegarde des clés de profil d'un utilisateur. La prochaine fois que l'utilisateur se connectera à cette machine de clone lié après l'opération de recomposition, le système d'exploitation créera un répertoire de profil pour l'utilisateur. Lors de la création d'un nouveau profil, l'utilisateur ne peut pas voir les anciennes données de profil. |
| 5 | Échec de restauration du profil d'un utilisateur. L'utilisateur ne doit pas se connecter à la machine dans cet état, car l'état du profil est indéfini. |
| 6 | Erreurs non couvertes par d'autres codes d'erreur. Les fichiers journaux d'agent de View Composer dans le système d'exploitation client peuvent fournir plus d'informations sur les causes de ces erreurs.<br>Par exemple, un délai d'expiration de Windows Plug-and-Play (PnP) peut générer ce code d'erreur. Dans cette situation, View Composer expire après avoir attendu que le service PnP installe de nouveaux volumes pour la machine virtuelle de clone lié.<br>PnP monte jusqu'à trois disques, en fonction de la configuration du pool :<br>■ Disque persistant de View Composer<br>■ Disque non persistant pour rediriger des fichiers temporaires et d'échange du système d'exploitation client<br>■ Disque interne qui stocke des données de configuration QuickPrep et d'autres données liées au système d'exploitation. Ce disque est toujours configuré avec un clone lié.<br>Le délai d'expiration est de 10 minutes. Si PnP ne termine pas le montage des disques en 10 minutes, View Composer échoue avec le code d'erreur 6. |
| 7 | Trop de disques persistants de View Composer sont attachés au clone lié. Un clone peut avoir au plus trois disques persistants de View Composer. |
| 8 | Un disque persistant ne peut pas être monté sur le magasin de données sélectionné lors de la création du pool. |
| 9 | View Composer ne peut pas rediriger des fichiers de données supprimables vers le disque non persistant. Le fichier d'échange ou les dossiers de fichiers temporaires n'étaient pas redirigés. |
| 10 | View Composer ne peut pas trouver le fichier de règle de configuration QuickPrep sur le disque interne spécifié. |
| 12 | View Composer ne peut pas trouver le disque interne qui contient le fichier de règle de configuration QuickPrep et d'autres données liées au système d'exploitation. |
| 13 | Plusieurs disques persistants sont configurés pour rediriger le profil d'utilisateur Windows. |
| 14 | View Composer n'a pas réussi à démonter le disque interne. |
| 15 | Le nom d'ordinateur que View Composer a lu depuis le fichier de règle de configuration ne correspond pas au nom du système actuel après la première mise sous tension du clone lié. |
| 16 | L'agent View Composer n'a pas démarré car la licence en volume pour le système d'exploitation client n'était pas activée. |
| 17 | L'agent View Composer n'a pas démarré. L'agent a expiré en attendant que Sysprep démarre. |
| 18 | L'agent View Composer n'a pas pu joindre la machine virtuelle de clone lié au domaine lors de la personnalisation. |

**Tableau 19-1.** Erreurs d'approvisionnement de View Composer (suite)

| Erreur | Description |
|---|---|
| 19 | L'agent View Composer n'a pas pu exécuter un script de post-synchronisation. |
| 20 | L'agent View Composer n'a pas pu gérer un événement de synchronisation de mot de passe de machine.<br>Cette erreur peut être temporaire. Si le clone lié joint le domaine, le mot de passe est correct.<br>Si le clone ne parvient pas à joindre le domaine, redémarrez l'opération que vous avez effectuée avant que l'erreur se produise. Si vous avez redémarré le clone, redémarrez-le de nouveau. Si vous avez actualisé le clone, actualisez-le de nouveau. Si le clone ne parvient toujours pas à joindre le domaine, recomposez le clone. |
| 21 | L'agent View Composer n'a pas réussi à monter le disque supprimable par le système. |
| 22 | L'agent View Composer n'a pas réussi à monter le disque persistant de View Composer. |

# Résolution des problèmes de connexion réseau

Vous pouvez utiliser diverses procédures pour le diagnostic et la résolution de problèmes liés à des connexions réseau avec des machines, des périphériques Horizon Client et des instances du Serveur de connexion View.

## Problèmes de connexion entre des machines et des instances du Serveur de connexion View

Vous pouvez rencontrer des problèmes de connexion entre des machines et des instances du Serveur de connexion View.

### Problème

Si la connectivité entre une machine et une instance du Serveur de connexion View échoue, vous voyez l'un des messages suivants dans la base de données des événements.

- `Provisioning error occurred for Machine` *`Machine_Name`*`: Customization error due to no network communication between the Horizon Agent and Connection Server (Une erreur de provisionnement s'est produite pour la machine Machine_Name : erreur de personnalisation due à une absence de communication réseau entre l'instance d'Horizon Agent et le Serveur de connexion)`
- `Provisioning error occurred on Pool` *`Desktop_ID`* `because of a networking problem with a Horizon Agent (Une erreur d'approvisionnement s'est produite sur le pool Desktop_ID à cause d'un problème de réseau avec une instance d'Horizon Agent)`
- `Unable to launch from Pool` *`Desktop_ID`* `for user` *`User_Display_Name`*`: Failed to connect to Machine` *`MachineName`* `using` *`Protocol`* `(Lancement impossible depuis le pool Desktop_ID pour l'utilisateur User_Display_Name : impossible de se connecter à la machine MachineName à l'aide de Protocol)`

### Cause

Les problèmes de connectivité entre une machine et une instance du Serveur de connexion View peuvent se produire pour différentes raisons.

- Une erreur de recherche du nom DNS de l'hôte du Serveur de connexion View sur la machine.
- Les ports pour la communication JMS, RDP ou AJP13 bloqués par des règles de pare-feu.
- L'échec du routeur JMS sur l'hôte du Serveur de connexion View.

### Solution

- À l'invite de commande sur la machine, tapez la commande `nslookup`.

  `nslookup` *`CS_FQDN`*

*CS_FQDN* est le nom de domaine complet (FQDN) de l'hôte du Serveur de connexion View. Si la commande ne parvient pas à renvoyer l'adresse IP de l'hôte du Serveur de connexion View, appliquez des techniques de dépannage de réseau générales pour corriger la configuration DNS.

- À l'invite de commande sur la machine, vérifiez que le port TCP 4001, qu'Horizon Agent utilise pour établir une communication JMS avec l'hôte du Serveur de connexion View, fonctionne en entrant la commande `telnet`.

  ```
  telnet CS_FQDN 4001
  ```

  Si la connexion `telnet` est établie, la connectivité réseau pour JMS fonctionne.

- Si un serveur de sécurité est déployé dans la zone démilitarisée, vérifiez que des règles d'exception sont configurées dans le pare-feu intérieur pour autoriser la connectivité RDP entre le serveur de sécurité et des machines virtuelles sur le port TCP 3389.
- Si des connexions sécurisées sont contournées, vérifiez que les règles de pare-feu autorisent un client à établir une connexion RDP directe avec la machine virtuelle sur le port TCP 3389, ou une connexion PCoIP directe avec la machine virtuelle sur le port TCP 4172 et le port UDP 4172.
- Vérifiez que les règles d'exception sont configurées dans le pare-feu intérieur pour autoriser des connexions entre chaque serveur de sécurité et son hôte du Serveur de connexion View associé sur le port TCP 4001 (JMS) et le port TCP 8009 (AJP13).

## Problèmes de connexion entre Horizon Client et PCoIP Secure Gateway

Vous pouvez rencontrer des problèmes de connexion entre Horizon Client et un hôte du serveur de sécurité ou du Serveur de connexion View lorsque PCoIP Secure Gateway est configuré pour authentifier des utilisateurs externes qui communiquent sur PCoIP.

### Problème

Les clients qui utilisent PCoIP ne peuvent pas se connecter à des postes de travail View ni les afficher. La connexion initiale à une instance du serveur de sécurité ou du Serveur de connexion View réussit, mais la connexion échoue lorsque l'utilisateur sélectionne un poste de travail View. Ce problème se produit lorsque PCoIP Secure Gateway est configuré sur un hôte du serveur de sécurité ou du Serveur de connexion View.

**Remarque** En général, PCoIP Secure Gateway est exploité sur un serveur de sécurité. Dans une configuration de réseau dans laquelle des clients externes se connectent directement à un hôte du Serveur de connexion View, PCoIP Secure Gateway peut également être configuré sur Serveur de connexion View.

### Cause

Des problèmes de connexion à PCoIP Secure Gateway peuvent se produire pour différentes raisons.

- Le pare-feu Windows a fermé un port requis pour PCoIP Secure Gateway.
- PCoIP Secure Gateway n'est pas activé sur l'instance du serveur de sécurité ou du Serveur de connexion View.
- Le paramètre PCoIP External URL (URL externe PCoIP) est mal configuré. Ce paramètre doit spécifier l'adresse IP externe à laquelle les clients ont accès sur Internet.
- L'URL externe PCoIP, l'URL externe du tunnel sécurisé, l'URL externe Blast ou une autre adresse est configurée pour pointer vers un hôte du serveur de sécurité ou du Serveur de connexion View différent. Lorsque vous configurez ces adresses sur un hôte du serveur de sécurité ou du Serveur de connexion View, toutes les adresses doivent permettre aux systèmes clients d'atteindre l'hôte actuel.
- Le client se connecte via un proxy Web externe qui a fermé un port requis pour PCoIP Secure Gateway. Par exemple, un proxy Web sur le réseau d'un hôtel ou une connexion publique sans fil peut bloquer les ports requis.

- La version de l'instance du Serveur de connexion View couplée avec le serveur de sécurité sur lequel PCoIP Secure Gateway est configuré est View 4.5 ou antérieure. La version du serveur de sécurité et de l'instance du Serveur de connexion View couplée doit être View 4.6 ou supérieure.

### Solution

- Vérifiez que les ports réseau suivants sont ouverts sur le pare-feu pour l'hôte du serveur de sécurité ou du Serveur de connexion View.

| Port | Description |
|---|---|
| TCP 4172 | À partir d'Horizon Client vers l'hôte du serveur de sécurité ou du Serveur de connexion View. |
| UDP 4172 | Entre Horizon Client et l'hôte du serveur de sécurité ou du Serveur de connexion View, dans les deux sens. |
| TCP 4172 | De l'hôte du serveur de sécurité ou du Serveur de connexion View vers le poste de travail View. |
| UDP 4172 | Entre l'hôte du serveur de sécurité ou du Serveur de connexion View et le poste de travail View, dans les deux sens. |

- Dans View Administrator, assurez-vous que le service PCoIP Secure Gateway est activé.
  a Cliquez sur **Configuration de View > Serveurs**.
  b Dans l'onglet **Serveurs de connexion**, sélectionnez l'instance du Serveur de connexion View et cliquez sur **Modifier**.
  c Cochez la case **Utiliser PCoIP Secure Gateway pour les connexions PCoIP à la machine**.

    Par défaut, PCoIP Secure Gateway est désactivé.
  d Cliquez sur **OK**.
- Dans View Administrator, assurez-vous que l'URL PCoIP externe est correctement configurée.
  a Cliquez sur **Configuration de View > Serveurs**.
  b Sélectionnez l'hôte à configurer.
    - Si vos utilisateurs se connectent à PCoIP Secure Gateway sur un serveur de sécurité, sélectionnez le serveur de sécurité dans l'onglet **Serveurs de sécurité**.
    - Si vos utilisateurs se connectent à PCoIP Secure Gateway sur une instance du Serveur de connexion View, sélectionnez cette instance dans l'onglet **Serveurs de connexion**.
  c Cliquez sur **Modifier**.
  d Dans la zone de texte **URL externe PCoIP**, assurez-vous que l'URL contient l'adresse IP externe de l'hôte du serveur de sécurité ou du Serveur de connexion View auquel les clients ont accès sur Internet.

    Spécifiez le port 4172. N'incluez pas de nom de protocole.

    Par exemple : `10.20.30.40:4172`
  e Assurez-vous que toutes les adresses de cette boîte de dialogue permettent aux systèmes clients d'atteindre cet hôte.

    Toutes les adresses de la boîte de dialogue Modifier les paramètres du serveur de sécurité doivent permettre aux systèmes clients d'atteindre cet hôte du serveur de sécurité. Toutes les adresses dans la boîte de dialogue Modifier les paramètres du Serveur de connexion View doivent permettre aux systèmes clients d'atteindre cette instance du Serveur de connexion View.
  f Cliquez sur **OK**.

  Répétez ces étapes pour chaque instance du serveur de sécurité et du Serveur de connexion View sur laquelle les utilisateurs se connectent à PCoIP Secure Gateway.

- Si l'utilisateur se connecte via un proxy Web se trouvant à l'extérieur de votre réseau, et que le proxy bloque un port requis, demandez à l'utilisateur de se connecter à partir d'un emplacement réseau différent.

## Problèmes de connexion entre des machines et des instances du Serveur de connexion View

Vous pouvez rencontrer des problèmes de connexion entre des machines et des instances du Serveur de connexion View.

### Problème

Si la connectivité entre une machine et une instance du Serveur de connexion View échoue, vous voyez l'un des messages suivants dans la base de données des événements.

- `Provisioning error occurred for Machine Machine_Name: Customization error due to no network communication between the Horizon Agent and Connection Server (Une erreur de provisionnement s'est produite pour la machine Machine_Name : erreur de personnalisation due à une absence de communication réseau entre l'instance d'Horizon Agent et le Serveur de connexion)`
- `Provisioning error occurred on Pool Desktop_ID because of a networking problem with a Horizon Agent (Une erreur d'approvisionnement s'est produite sur le pool Desktop_ID à cause d'un problème de réseau avec une instance d'Horizon Agent)`
- `Unable to launch from Pool Desktop_ID for user User_Display_Name: Failed to connect to Machine MachineName using Protocol (Lancement impossible depuis le pool Desktop_ID pour l'utilisateur User_Display_Name : impossible de se connecter à la machine MachineName à l'aide de Protocol)`

### Cause

Les problèmes de connectivité entre une machine et une instance du Serveur de connexion View peuvent se produire pour différentes raisons.

- Une erreur de recherche du nom DNS de l'hôte du Serveur de connexion View sur la machine.
- Les ports pour la communication JMS, RDP ou AJP13 bloqués par des règles de pare-feu.
- L'échec du routeur JMS sur l'hôte du Serveur de connexion View.

### Solution

- À l'invite de commande sur la machine, tapez la commande `nslookup`.

  ```
  nslookup CS_FQDN
  ```

  *CS_FQDN* est le nom de domaine complet (FQDN) de l'hôte du Serveur de connexion View. Si la commande ne parvient pas à renvoyer l'adresse IP de l'hôte du Serveur de connexion View, appliquez des techniques de dépannage de réseau générales pour corriger la configuration DNS.

- À l'invite de commande sur la machine, vérifiez que le port TCP 4001, qu'Horizon Agent utilise pour établir une communication JMS avec l'hôte du Serveur de connexion View, fonctionne en entrant la commande `telnet`.

  ```
  telnet CS_FQDN 4001
  ```

  Si la connexion `telnet` est établie, la connectivité réseau pour JMS fonctionne.

- Si un serveur de sécurité est déployé dans la zone démilitarisée, vérifiez que des règles d'exception sont configurées dans le pare-feu intérieur pour autoriser la connectivité RDP entre le serveur de sécurité et des machines virtuelles sur le port TCP 3389.

- Si des connexions sécurisées sont contournées, vérifiez que les règles de pare-feu autorisent un client à établir une connexion RDP directe avec la machine virtuelle sur le port TCP 3389, ou une connexion PCoIP directe avec la machine virtuelle sur le port TCP 4172 et le port UDP 4172.
- Vérifiez que les règles d'exception sont configurées dans le pare-feu intérieur pour autoriser des connexions entre chaque serveur de sécurité et son hôte du Serveur de connexion View associé sur le port TCP 4001 (JMS) et le port TCP 8009 (AJP13).

### Problèmes de connexion dus à l'attribution incorrecte d'adresses IP à des machines clonées

Il est possible que vous ne puissiez pas vous connecter à des machines clonées si elles ont des adresses IP statiques.

#### Problème

Vous ne pouvez pas utiliser Horizon Client pour vous connecter à des machines clonées.

#### Cause

Les machines clonées sont configurées de manière incorrecte, si bien qu'elles utilisent une adresse IP statique au lieu d'utiliser DHCP pour obtenir leur adresse IP.

#### Solution

1. Vérifiez que le modèle de pool de postes de travail sur vCenter Server est configuré pour utiliser DHCP afin d'attribuer des adresses IP aux machines.
2. Dans vSphere Web Client, clonez une machine virtuelle manuellement à partir du pool de postes de travail et vérifiez qu'elle obtient correctement son adresse IP de DHCP.

## Résolution de problèmes de redirection USB

Plusieurs problèmes peuvent se produire avec la redirection USB dans Horizon Client.

#### Problème

La redirection USB dans Horizon Client ne parvient pas à rendre disponibles des périphériques locaux sur le poste de travail distant ou certains périphériques ne semblent pas être disponibles pour la redirection dans Horizon Client.

#### Cause

Voici des causes possibles d'échec du fonctionnement correct ou prévu de la redirection USB.

- Le périphérique est un périphérique USB composite et l'un des périphériques qu'il inclut est bloqué par défaut. Par exemple, un périphérique de dictée qui inclut une souris est bloqué par défaut parce que les souris sont bloquées par défaut. Pour contourner ce problème, reportez-vous à « Configuration de paramètres de règle de fractionnement de périphérique pour des périphériques USB composites », page 258.
- La redirection USB n'est pas prise en charge sur les hôtes Windows Server 2008 RDS qui déploient des applications et des postes de travail distants. La redirection USB est prise en charge sur les hôtes RDS Windows Server 2012 avec View Agent 6.1 et versions ultérieures, mais uniquement pour les périphériques de stockage USB. La redirection USB est prise en charge sur les systèmes Windows Server 2008 R2 et Windows Server 2012 R2 utilisés comme postes de travail mono-utilisateur.
- Seuls les lecteurs flash et les disques durs USB sont pris en charge sur les postes de travail et applications RDS. Vous ne pouvez pas rediriger d'autres types de périphériques USB (par exemple, d'autres types de périphériques de stockage USB tels que les lecteurs de stockage de sécurité et les CD-ROM USB) vers un poste de travail ou une application RDS.

- Les webcams ne sont pas prises en charge pour la redirection.
- La redirection de périphériques audio USB dépend de l'état du réseau et n'est pas fiable. Certains périphériques requièrent un débit de données élevé même lorsqu'ils sont inactifs.
- La redirection USB n'est pas prise en charge pour les périphériques d'amorçage. Si vous exécutez Horizon Client sur un système Windows qui démarre à partir d'un périphérique USB, et que vous redirigez ce périphérique vers le poste de travail distant, le système d'exploitation local risque de ne plus répondre ou de devenir inutilisable. Reportez-vous à la section http://kb.vmware.com/kb/1021409.
- Par défaut, Horizon Client pour Windows ne vous permet pas de sélectionner des périphériques clavier, souris, carte à puce et sortie audio pour la redirection. Reportez-vous à la section http://kb.vmware.com/kb/1011600.
- RDP ne prend pas en charge la redirection pour les périphériques HID USB pour la session de console, ou pour les lecteurs de cartes à puce. Reportez-vous à la section http://kb.vmware.com/kb/1011600.
- Windows Mobile Device Center peut empêcher la redirection de périphériques USB pour des sessions RDP. Reportez-vous à la section http://kb.vmware.com/kb/1019205.
- Pour certains périphériques HID USB, vous devez configurer la machine virtuelle afin d'actualiser la position du pointeur de la souris. Reportez-vous à la section http://kb.vmware.com/kb/1022076.
- Pour certains périphériques audio, vous devrez éventuellement modifier les paramètres de règle ou de Registre. Reportez-vous à la section http://kb.vmware.com/kb/1023868.
- La latence réseau peut ralentir l'interaction entre périphériques ou rendre les applications figées car elles sont conçues pour interagir avec des périphériques locaux. Les disques durs USB très volumineux peuvent prendre plusieurs minutes pour apparaître dans Windows Explorer.
- Le chargement des cartes flash USB formatées avec le système de fichiers FAT32 est lent. Reportez-vous à la section http://kb.vmware.com/kb/1022836.
- Un processus ou un service sur le système local a ouvert le périphérique avant votre connexion à l'application ou au poste de travail distant.
- Un périphérique USB redirigé arrête de fonctionner si vous reconnectez une session de poste de travail ou d'application, même si le poste de travail ou l'application indique que le périphérique est disponible.
- La redirection USB est désactivée dans View Administrator.
- Des pilotes de redirection USB sont manquants ou désactivés sur le client.

### Solution

- S'il est disponible, utilisez PCoIP au lieu de RDP comme protocole.
- Si un périphérique redirigé reste indisponible ou arrête de fonctionner après une déconnexion temporaire, éjectez le périphérique, rebranchez-le et tenter de nouveau l'opération de redirection.
- Dans View Administrator, accédez à **Règles > Règles générales**, et vérifiez que l'accès USB est défini sur **Autoriser** sous Règles de View.
- Dans le journal de l'invité, recherchez des entrées de la classe `ws_vhub` et, dans le journal du client, recherchez des entrées de la classe `vmware-view-usbd`.

  Les entrées avec ces classes sont inscrites dans les journaux si un utilisateur n'est pas un administrateur, ou si les pilotes de redirection USB ne sont pas installés ou ne fonctionnent pas. Pour connaître l'emplacement de ces fichiers journaux, reportez-vous à « Utilisation de fichiers journaux pour le dépannage et pour déterminer les ID de périphérique USB », page 256.
- Ouvrez le Gestionnaire de périphériques sur l'invité, développez les contrôleurs USB (Universal Serial Bus) et réinstallez les pilotes VMware View Virtual USB Host Controller et VMware View Virtual USB Hub s'ils sont manquants ou réactivez-les s'ils sont désactivés.

# Gérer des machines et des stratégies pour des utilisateurs non autorisés

Vous pouvez afficher les machines attribuées à des utilisateurs dont le droit d'accès a été supprimé. Vous pouvez également afficher les stratégies qui ont été appliquées à des utilisateurs non autorisés.

Un utilisateur non autorisé peut avoir quitté l'entreprise définitivement ou vous pouvez avoir suspendu son compte pour une longue période de temps. Une machine est attribuée à cet utilisateur, mais il n'est plus autorisé à utiliser le pool de machines.

Vous pouvez également utiliser la commande `vdmadmin` avec l'option `-O` ou `-P` pour afficher les machines et les stratégies non attribuées. Pour plus d'informations, reportez-vous au document *Administration de View*.

### Procédure

1 Dans View Administrator, sélectionnez **Ressources > Machines**.

2 Sélectionnez **Plus de commandes > Afficher les machines non autorisées**.

3 Supprimez les attributions de machines pour les utilisateurs non autorisés.

4 Sélectionnez **Plus de commandes > Afficher les machines non autorisées** ou **Plus de commandes > Afficher les règles non autorisées** selon le cas.

5 Modifiez ou supprimez les règles qui sont appliquées à des utilisateurs non autorisés.

# Résolution des incohérences de base de données avec la commande ViewDbChk

Avec la commande `ViewDbChk`, vous pouvez résoudre les incohérences dans les bases de données qui stockent des informations sur les machines virtuelles de poste de travail dans un pool de postes de travail automatisé et des hôtes RDS dans une batterie de serveurs automatisée.

Dans un environnement View, les informations sur les machines virtuelles de poste de travail et les hôtes RDS dans une batterie de serveurs automatisée sont stockées dans les emplacements suivants :

- Base de données LDAP
- Base de données vCenter Server
- Pour les machines de clone lié View Composer uniquement : la base de données View Composer

Normalement, vous pouvez récupérer les erreurs qui se produisent lors du provisionnement ou d'autres opérations en supprimant ou en réinitialisant une machine virtuelle de poste de travail ou un hôte RDS à l'aide de View Administrator. En de rares occasions, les informations dans les différentes bases de données sur une machine en état d'erreur deviennent incohérentes et il devient impossible de récupérer l'erreur à l'aide de View Administrator. Vous pouvez voir l'un des symptômes suivants :

- L'approvisionnement échoue avec le message d'erreur `La machine virtuelle avec la spécification d'entrée existe déjà`.
- La recomposition d'un pool de postes de travail échoue avec le message d'erreur `Erreur de Desktop Composer : La machine virtuelle avec la spécification d'entrée existe déjà`.
- View Administrator indique qu'une machine de poste de travail ou un hôte RDS est bloqué dans un état Suppression.
- Vous ne pouvez pas supprimer un pool de postes de travail ou une batterie de serveurs automatisée.
- Vous ne pouvez pas supprimer une machine de poste de travail ou un hôte RDS.
- Dans l'onglet Inventaire de View Administrator, l'état d'une machine de poste de travail ou d'un hôte RDS est absent.

Lorsque des incohérences de base de données placent une machine de poste de travail ou un hôte RDS dans un état d'erreur irrécupérable ou empêchent l'aboutissement d'une tâche de View Administrator, vous pouvez utiliser la commande `ViewDbChk` pour résoudre les incohérences. La commande `ViewDbChk` a les caractéristiques suivantes :

- `ViewDbChk` est automatiquement installé lorsque vous installez le Serveur standard View ou le Serveur réplica View. L'utilitaire n'est pas installé lorsque vous installez le serveur de sécurité View.
- `ViewDbChk` est une commande que vous pouvez exécuter à partir de l'invite de commande Windows ou à partir d'un script.
- `ViewDbChk` prend en charge les batteries de serveurs automatisées et les pools de postes de travail automatisés de machines virtuelles complètes ainsi que les clones liés View Composer.
- Lorsque vous souhaitez supprimer une machine, `ViewDbChk` effectue un contrôle de la santé sur la machine et vous demande de fournir des informations supplémentaires si la machine semble saine.
- `ViewDbChk` peut supprimer des entrées LDAP erronées ou incomplètes.
- `ViewDbChk` prend en charge l'entrée et la sortie utilisant les jeux de caractères I18N.
- `ViewDbChk` ne supprime pas les données utilisateur. Pour une machine virtuelle de poste de travail complète, `ViewDbChk` supprime la machine virtuelle de l'inventaire, mais ne la supprime pas du disque. Pour une machine virtuelle de poste de travail de clone lié, `ViewDbChk` supprime la machine virtuelle et archive les disques utilisateur dans le dossier racine dans le cas de banques de données VMFS ou dans un sous-dossier nommé archiveUDD dans le cas de banques de données Virtual SAN et Virtual Volumes.
- `ViewDbChk` ne prend pas en charge les machines de poste de travail ou les hôtes RDS non gérés dans une batterie de serveurs manuelle.

## Syntaxe de ViewDbChk

```
ViewDbChk --findDesktop --desktopName <desktop pool or farm name> [--verbose]

ViewDbChk --enableDesktop --desktopName <desktop pool or farm name> [--verbose]

ViewDbChk --disableDesktop --desktopName <desktop pool or farm name> [--verbose]

ViewDbChk --findMachine --desktopName <desktop pool or farm name> --machineName <machine name>
[--verbose]

ViewDbChk --removeMachine --machineName <machine name> [--desktopName <desktop pool or farm
name>] [--force] [--noErrorCheck] [--verbose]

ViewDbChk --scanMachines [--desktopName <desktop pool or farm name>] [--limit <maximum deletes>]
[--force] [--verbose]

ViewDbChk --help [--commandName] [--verbose]
```

## Paramètres de ViewDbChk

| Paramètre | Description |
|---|---|
| --findDesktop | Recherche un pool de postes de travail ou une batterie de serveurs. |
| --enableDesktop | Active un pool de postes de travail ou une batterie de serveurs. |
| --disableDesktop | Désactive un pool de postes de travail ou une batterie de serveurs. |
| --findMachine | Recherche une machine. |

| Paramètre | Description |
|---|---|
| --removeMachine | Supprime une machine d'un pool de postes de travail ou d'une batterie de serveurs. Avant de supprimer une machine, `ViewDbChk` invite l'utilisateur à désactiver le pool de postes de travail ou la batterie de serveurs. Après la suppression de la machine, `ViewDbChk` invite l'utilisateur à réactiver le pool de postes de travail ou la batterie de serveurs. |
| --scanMachines | Recherche des machines en état error ou cloneerror ou pour lesquelles des machines virtuelles sont manquantes, répertorie les machines virtuelles problématiques groupées par pool de postes de travail ou batterie de serveurs, et offre la possibilité de supprimer les machines. Avant de supprimer une machine, `ViewDbChk` invite l'utilisateur à désactiver le pool de postes de travail ou la batterie de serveurs. Après la suppression de toutes les machines en erreur d'un pool de postes de travail ou d'une batterie de serveurs, `ViewDbChk` invite l'utilisateur à réactiver le pool de postes de travail ou la batterie de serveurs. |
| --help | Affiche la syntaxe de `ViewDbChk`. |
| --desktopName <nom de poste de travail> | Spécifie le nom du pool de postes de travail ou de la batterie de serveurs. |
| --machineName <nom de machine> | Spécifie le nom de la machine. |
| --limit <nombre maximal de suppressions> | Limite le nombre de machines que `ViewDbChk` peut supprimer. Le niveau par défaut est 1. |
| --force | Force la suppression de la machine sans confirmation de l'utilisateur. |
| --noErrorCheck | Force la suppression des machines ne présentant pas d'erreur. |
| --verbose | Active la journalisation détaillée. |

**Remarque** Tous les noms de paramètres sont sensibles à la casse.

## Exemples d'utilisation de ViewDbChk

Une machine de poste de travail nommée lc-pool2-2 est dans un état d'erreur et nous ne pouvons pas la supprimer à l'aide de View Administrator. Nous utilisons ViewDbChk pour la supprimer de l'environnement View.

```
C:\>viewdbchk --removeMachine --machineName lc-pool2-2
Looking for desktop pool "lc-pool2" in LDAP...
   Desktop Pool Name: lc-pool2
   Desktop Pool Type: AUTO_LC_TYPE
   VM Folder: /vdi/vm/lc-pool2/
   Desktop Pool Disabled: false
   Desktop Pool Provisioning Enabled: true
Looking for machine "/vdi/vm/lc-pool2/lc-pool2-2" in vCenter...
   Connecting to vCenter "https://10.133.17.3:443/sdk". This may take some time...
Checking connectivity...
   Connecting to View Composer "https://10.133.17.3:18443". This may take some time...
The desktop pool "lc-pool2" must be disabled before proceeding. Do you want to disable the
desktop pool? (yes/no):yes
Found machine "lc-pool2-2"
   VM Name: lc-pool2-2
   Creation Date: 1/25/15 1:20:26 PM PST
   MOID: vm-236
   Clone Id: b12a9ed2-8535-44ee-a9d6-6c9b5cf6f878
   VM Folder: /vdi/vm/lc-pool2/lc-pool2-2
   VM State: ERROR
Do you want to remove the desktop machine "lc-pool2-2"? (yes/no):yes
```

```
Shutting down VM "/vdi/vm/lc-pool2/lc-pool2-2"...
Archiving persistent disks...
Destroying View Composer clone "b12a9ed2-8535-44ee-a9d6-6c9b5cf6f878"...
Removing ThinApp entitlements for machine "/vdi/vm/lc-pool2/lc-pool2-2"...
Removing machine "/vdi/vm/lc-pool2/lc-pool2-2" from LDAP...
Running delete VM scripts for machine "/vdi/vm/lc-pool2/lc-pool2-2"...
Do you want to enable the desktop pool "lc-pool2"? (yes/no):yes
```

## Autres informations de dépannage

Vous pouvez trouver davantage d'informations de dépannage dans des articles de la base de connaissances VMware.

La base de connaissances VMware est mise à jour en continu avec des nouvelles informations de dépannage pour des produits VMware.

Pour plus d'informations sur le dépannage de View, reportez-vous aux articles proposés sur le site Web de la base de connaissances VMware :

http://kb.vmware.com/selfservice/microsites/microsite.do

# Index

## D

## E



## F



## G

## H



## I



## J



## L



## M

## N



## O



## P

## Q



## R

## S