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

VMware Horizon 6.0.0
VMware Horizon 6.0.1

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-001485-01

vmware®

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

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

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

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

docfeedback@vmware.com

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

Dans VMware Horizon avec View, vous pouvez créer des pools de postes de travail qui comprennent un, des centaines ou des milliers de postes de travail virtuels. Vous pouvez déployer des postes de travail qui s'exécutent sur des machines virtuelles, des machines physiques et des hôtes des services Bureau à distance Windows (RDS). Créez une machine virtuelle en tant qu'image de base de sorte que View 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

Avec View, vous pouvez créer des pools de postes de travail et d'applications afin d'accorder aux utilisateurs l'accès 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. View bénéficie des technologies Services Bureau à distance Microsoft (RDS) et VMware PCoIP (PC-over-IP) pour fournir un accès à distance de haute qualité aux utilisateurs.

Hôtes RDS

Les hôtes RDS sont des ordinateurs serveurs sur lesquels les services Bureau à distance Windows et View Agent sont installés. Ces serveurs hébergent des sessions d'application et de poste de travail auxquelles les utilisateurs peuvent accéder à distance. Pour utiliser des pools de postes de travail ou des applications RDS, vous utilisateurs finaux doivent avoir accès au logiciel Horizon Client 3.0 ou version ultérieure.

Pools de postes de travail

Il existe trois 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 Windows 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 Windows. 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

View 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 View 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.
- Si vous utilisez une machine virtuelle, spécifiez si vous voulez la mettre hors tension lorsqu'elle n'est pas utilisée et si vous voulez la supprimer.
- Spécifiez 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.

De plus, l'utilisation de pools de postes de travail a de nombreux avantages.

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 utilisateurs peuvent personnaliser leurs postes de travail, installer des applications et stocker des données.

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. Un poste de travail d'affectation flottante ressemble à un laboratoire informatique ou à un environnement de kiosque où chaque poste de travail est chargé avec les applications nécessaires et tous les postes de travail ont accès aux données nécessaires.

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

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 de clone lié et des options de récupération d'urgence et de continuité des activités plus faciles et moins coûteuses.

Images de poste de travail avec état

Ces images peuvent requérir des techniques de gestion d'image traditionnelles. 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.

Vous créez des images de poste de travail sans état en utilisant View Composer et en créant des pools d'affectation flottante de machines virtuelles de clone lié.

Vous créez des images de poste de travail avec état en créant des pools d'affectation dédiée de machines virtuelles de clone lié ou de machines virtuelles complètes. Si vous utilisez des machines virtuelles de clone lié, vous pouvez configurer des disques persistants de View Composer et la redirection de dossiers. Certains fournisseurs de stockage disposent de solutions de stockage rentables pour les images de poste de travail avec état. 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.

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.
- 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 lié View Composer pour que les postes de travail partagent la même image de base et utilisent moins d'espace de stockage dans le datacenter que des machines virtuelles complètes.
- Déterminez quelle action, le cas échéant, à effectuer lorsque des utilisateurs ferment leur session. 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.
- Le cas échéant, utilisez les banques de données Virtual SAN. Virtual SAN virtualise les disques de stockage physiques et locaux disponibles sur les hôtes ESXi dans une seule banque de données partagée par tous les hôtes dans un cluster vSphere. 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. 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 193.
- 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 sur des banques de données locales », page 205.
- 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.

Comme les utilisateurs expérimentés et les travailleurs du savoir (comptables, directeurs commerciaux, analystes en recherche marketing, etc.) doivent pouvoir créer et conserver des documents et des paramètres, vous créez des postes de travail d'affectation dédiée pour eux. 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 :

- Utilisez des pools d'affectation dédiée pour que chaque travailleur du savoir ou utilisateur expérimenté ouvre une session sur le même poste de travail à chaque fois.
- 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 ont besoin d'installer leurs propres applications, ce qui ajoute des données au disque du système d'exploitation, créez des postes de travail de machine virtuelle complète. Utilisez Mirage pour déployer et mettre à jour les applications sans remplacer les applications installées par l'utilisateur.
- 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 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.

  Configurez 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.

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 dans le 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 lié View Composer pour que les postes de travail partagent la même image de base et utilisent moins d'espace de stockage dans le datacenter que des machines virtuelles complètes.
- Établissez une règle d'actualisation pour que le poste de travail soit actualisé fréquemment, par exemple à chaque fermeture de session d'un utilisateur.
- Le cas échéant, utilisez les banques de données Virtual SAN. Virtual SAN virtualise les disques de stockage physiques et locaux disponibles sur les hôtes ESXi dans une seule banque de données partagée par tous les hôtes dans un cluster vSphere. 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. 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 193.
- 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 sur des banques de données locales », page 205.
- 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 16, « Configuration de stratégies pour des pools de postes de travail et d'applications », page 213.

- Utilisez un GPO si vous souhaitez remplacer la règle par défaut qui permet de connecter des périphériques USB locaux au poste de travail lorsque ce dernier est lancé ou lorsque des périphériques USB sont raccordés à 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 7, « Configuration des hôtes de services Bureau à distance », page 95.

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. Pour plus d'informations, reportez-vous au document *Installation de View*.

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 View Agent sur la machine non gérée. Reportez-vous à la section « Installer View Agent sur une machine non gérée », page 18.

Installer View Agent sur une machine non gérée

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

Pour installer View Agent sur plusieurs ordinateurs physiques Windows sans avoir à répondre à des invites d'assistant, vous pouvez installer View Agent en silence. Reportez-vous à la section « Installer View Agent en silence », page 34.

Prérequis

- Vérifiez que vous disposez des droits d'administration sur la machine non gérée.
- Pour utiliser une machine virtuelle Windows Server 2008 R2 non gérée en tant que poste de travail distant plutôt qu'en tant qu'hôte RDS, procédez de la manière décrite dans « Préparer Windows Server 2008 R2 pour l'utiliser en tant que poste de travail », page 29.
- Familiarisez-vous avec les options de configuration personnalisée de View Agent pour des machines non gérées. Reportez-vous à la section « Options d'installation personnalisée de View Agent pour des machines non gérées », page 20.
- Familiarisez-vous avec les ports TCP que le programme d'installation de View Agent ouvre sur le pare-feu. Pour plus d'informations, reportez-vous au document *Planification de l'architecture de View*.
- Téléchargez le fichier du programme d'installation View Agent sur la page du produit VMware sur http://www.vmware.com/products/.

Procédure

1 Pour démarrer le programme d'installation de View 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 les options d'installation personnalisée désirées.

4 Acceptez ou modifiez le dossier de destination.

5 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.

6 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**.

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 dans le programme d'installation de View Agent et terminez l'installation.

8 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 View Agent démarre sur la machine non gérée.

Si Windows Media Player n'est pas installé, le programme d'installation de View Agent n'installe pas la fonction de redirection multimédia (MMR). Si vous installez Windows Media Player après l'installation de View Agent, vous pouvez installer la fonction MMR en exécutant de nouveau le programme d'installation de View Agent et en sélectionnant l'option Repair (Réparer).

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 89.

Options d'installation personnalisée de View Agent pour des machines non gérées

Lorsque vous installez View Agent sur une machine non gérée, vous pouvez sélectionner ou désélectionner des options de configuration personnalisée. En outre, View 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.

Tableau 2-1. Options d'installation personnalisée de View Agent pour des machines non gérées

Option	Description
Redirection USB	Donne aux utilisateurs un accès à des périphériques USB connectés en local sur leurs postes de travail. L'option Redirection USB 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. **Remarque** Vous pouvez utiliser les paramètres de stratégie de groupe pour désactiver une redirection USB pour des utilisateurs spécifiques.
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.
Carte à puce PCoIP	Permet aux utilisateurs de s'authentifier avec des cartes à puce lorsqu'ils utilisent le protocole d'affichage PCoIP. L'option Carte à puce PCoIP 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.

Tableau 2-2. Fonctionnalités de View Agent installées automatiquement sur des machines non gérées

Option	Description
PCoIP Agent	Permet aux utilisateurs de se connecter au poste de travail distant à l'aide du protocole d'affichage PCoIP. La fonctionnalité PCoIP Agent est prise en charge sur les machines physiques configurées avec une carte d'hôte Teradici TERA. **Remarque** Sous Windows Vista, si vous installez le composant PCoIP Agent, la stratégie de groupe Windows **Désactiver ou activer la séquence de touches de sécurité (SAS, Secure Attention Sequence)** est activée et définie sur **Services** et **Services et applications d'ergonomie**. Si vous modifiez ce paramètre, l'authentification unique ne fonctionne pas correctement.
Redirection multimédia Wyse (MMR)	Fournit la redirection multimédia aux postes de travail et clients Windows XP et Windows Vista. 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.
Lync	Fournit la prise en charge de Microsoft Lync 2013 Client sur les postes de travail distants.

Tableau 2-2. Fonctionnalités de View Agent installées automatiquement sur des machines non gérées (suite)

Option	Description
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 audio virtuel	Fournit un pilote audio virtuel sur le poste de travail distant.

Création et préparation de machines virtuelles 3

Vous pouvez utiliser des machines virtuelles gérées par vCenter Server pour provisionner et déployer des postes de travail distants. Vous pouvez utiliser une machine virtuelle gérée par vCenter Server en tant que modèle pour un pool automatisé, en tant que parent pour un pool de clones liés ou en tant que machine dans un pool manuel. Vous devez préparer des machines virtuelles pour fournir un accès au poste de travail distant.

Ce chapitre aborde les rubriques suivantes :

Création de machines virtuelles pour un déploiement de postes de travail distants

La machine virtuelle initiale établit un profil de matériel virtuel et un système d'exploitation à utiliser pour un déploiement rapide de postes de travail distants.

1 Créer une machine virtuelle pour un déploiement de poste de travail distant page 24

Vous utilisez vSphere Client pour créer des machines virtuelles dans vCenter Server pour des postes de travail distants.

2 Installer un système d'exploitation client page 26

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 27

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 Windows Server 2008 R2 pour l'utiliser en tant que poste de travail page 29

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

Créer une machine virtuelle pour un déploiement de poste de travail distant

Vous utilisez vSphere Client pour créer des machines virtuelles dans vCenter Server pour des postes de travail distants.

Prérequis

- Chargez un fichier image ISO du système d'exploitation invité vers une banque de données sur votre serveur ESXi.
- 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 24.

Procédure

1 Dans vSphere Client, ouvrez une session sur le système vCenter Server.

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 du système d'exploitation client que vous avez téléchargé vers votre magasin de données, puis sélectionnez **Se connecter à l'activation**.

   b Si vous installez un système d'exploitation client Windows XP, ajoutez un lecteur de disquette et définissez le **Type de périphérique** sur **Périphérique client**.

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

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

Suivant

Installez un système d'exploitation client sur la machine virtuelle.

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. 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. 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. Pour la plupart des systèmes d'exploitation clients, un seul processeur est suffisant.
`Memory`	Quantité de mémoire à allouer à la machine virtuelle. Dans la plupart des cas, 512 Mo est suffisant.
`Network`	Nombre de cartes réseau dans la machine virtuelle. 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. Lorsque vous installez View Agent sur une machine virtuelle qui possède plusieurs cartes réseau, vous devez configurer le sous-réseau que View Agent utilise. Pour plus d'informations, reportez-vous à « Configurer une machine virtuelle avec plusieurs cartes réseau pour View Agent », page 40. **IMPORTANT** Pour les systèmes d'exploitation Windows 8, Windows 7, Windows Vista et Windows Server 2008 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 : ■ Pour Windows 7 SP1 : http://support.microsoft.com/kb/2550978 ■ Pour les versions Windows 7 antérieures à SP1 : http://support.microsoft.com/kb/2344941

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

Paramètre	Description et recommandations
`SCSI Controller`	Type d'adaptateur SCSI à utiliser avec la machine virtuelle. Pour les systèmes d'exploitation invités Windows 8, Windows 7 et Windows XP, vous devez spécifier l'adaptateur LSI Logic. L'adaptateur LSI Logic a des performances améliorées et fonctionne mieux avec des périphériques SCSI génériques. LSI Logic SAS est disponible uniquement pour les machines virtuelles avec la version matérielle 7 et supérieure. **Remarque** Windows XP ne comporte pas de pilote pour l'adaptateur LSI Logic. Vous devez télécharger le pilote sur le site Web de LSI Logic.
`Select a Disk`	Disque à utiliser avec la machine virtuelle. 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. 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.
- Si vous installez Windows XP et que vous avez sélectionné l'adaptateur LSI Logic pour la machine virtuelle, téléchargez le pilote du contrôleur LSI20320-R à partir du site Web LSI Logic, créez un fichier image de disquette (`.flp`) contenant le pilote et téléchargez le fichier sur une banque de données sur votre serveur.

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 Si vous installez Windows XP et que vous avez sélectionné l'adaptateur LSI Logic pour la machine virtuelle, installez le pilote LSI Logic lors du processus d'installation de Windows.

   a Appuyez sur F6 pour sélectionner des pilotes SCSI supplémentaires.

   b Saisissez `S` pour spécifier un périphérique supplémentaire.

   c Sur la barre d'outils vSphere Client, cliquez sur **Connecter la disquette** pour sélectionner le fichier image disquette (`.flp`) du pilote LSI Logic.

   d Retournez à l'écran d'installation de Windows et appuyez sur Entrée pour continuer le processus d'installation de Windows.

   e Quand le processus d'installation de Windows a terminé, déconnectez le lecteur de disquette virtuelle.

5 Si vous installez Windows 7 ou Windows 8, activez Windows en ligne.

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. Pour plus d'informations, reportez-vous au document *Installation de View*.
- 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, appelés Terminal Services sur les systèmes Windows XP, sont démarrés sur la machine virtuelle. Les services Bureau à distance sont requis pour l'installation de View 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 138.
- Vérifiez que vous disposez de droits d'administration sur le système d'exploitation client.
- Sur les systèmes d'exploitation Windows Vista, vérifiez que le service Windows Update est activé. Si vous désactivez ce service sous Windows Vista, le programme d'installation de View Agent ne parvient pas à installer le pilote USB.
- Sur les systèmes d'exploitation Windows Server 2008 R2, préparez le système d'exploitation pour l'utilisation d'un poste de travail. Reportez-vous à la section « Préparer Windows Server 2008 R2 pour l'utiliser en tant que poste de travail », page 29.
- 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 de View 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 Windows Media Player si vous utilisez MMR et des pilotes de cartes à puce si vous utilisez l'authentification par carte à puce.

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

Sur les systèmes Windows XP, installez tous les logiciels et applications tiers (sauf Microsoft .NET Framework) avant d'installer View Agent.

Important Si vous installez Microsoft .NET Framework, vous devez l'installer après View 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 Joignez la machine virtuelle au domaine Active Directory de vos postes de travail distants.

   Une machine virtuelle parente que vous utilisez pour View Composer doit appartenir au même domaine Active Directory que le domaine que les postes de travail de clone lié rejoindront ou doit être un membre du Groupe de travail local.

13 Configurez le pare-feu Windows pour autoriser des connexions Bureau à distance vers 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.

Suivant

Installez View Agent. Reportez-vous à la section « Installer View Agent sur une machine virtuelle », page 30.

Préparer Windows Server 2008 R2 pour l'utiliser en tant que poste de travail

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

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 de View Agent vous invite à confirmer que vous souhaitez installer View Agent en mode de poste de travail. Si le rôle Services Bureau à distance est présent, le programme d'installation de View Agent n'affiche pas cette invite et considère la machine Windows Server 2008 R2 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).

   Si vous n'installez pas la version SP1, une erreur se produira lorsque vous installerez View Agent.

3 Installez la fonctionnalité Expérience utilisateur de Windows Server 2008 R2.

   Si vous n'installez pas cette fonctionnalité, HTML Access ne fonctionnera pas correctement sur les postes de travail View déployés à partir d'une machine virtuelle Windows Server 2008 R2.

4 (Facultatif) Pour utiliser Windows Aero sur un poste de travail Windows Server 2008 R2, activez manuellement la fonctionnalité Expérience utilisateur et 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 Configurez View Administrator afin qu'il considère Windows Server 2008 R2 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 2008 R2 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 Server 2008 R2** et cliquez sur **OK**.

Lorsque vous activez des postes de travail Windows Server 2008 R2 dans View Administrator, celui-ci affiche toutes les machines Windows Server 2008 R2 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 View Agent sur des machines sur lesquelles d'autres composants logiciels de View sont installés.

Installer View Agent sur une machine virtuelle

Vous devez installer View Agent sur des machines virtuelles gérées par vCenter Server pour que le Serveur de connexion View puisse communiquer avec elles. Installez View Agent sur toutes les machines virtuelles que vous utilisez en tant que modèles pour les pools de postes de travail automatisés, en tant que parents pour les pools de postes de travail de clone lié et en tant que machines dans les pools de postes de travail manuels.

Pour installer View Agent sur plusieurs machines virtuelles Windows sans avoir à répondre à des invites d'assistant, vous pouvez installer View Agent en silence. Reportez-vous à la section « Installer View Agent en silence », page 34.

Le logiciel View Agent ne peut pas coexister sur la même machine virtuelle ou physique avec un autre composant logiciel de View, notamment un serveur de sécurité, le Serveur de connexion View, 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 27.
- Pour utiliser une machine virtuelle Windows Server 2008 R2 en tant que poste de travail distant (et non en tant qu'hôte RDS), procédez comme décrit dans « Préparer Windows Server 2008 R2 pour l'utiliser en tant que poste de travail », page 29.
- Téléchargez le fichier du programme d'installation View Agent sur la page du produit VMware sur http://www.vmware.com/products/.
- Vérifiez que vous disposez des droits d'administration sur la machine virtuelle.
- Familiarisez-vous avec les options d'installation personnalisée de View Agent. Reportez-vous à la section « Options d'installation personnalisée de View Agent », page 31.
- Familiarisez-vous avec les ports TCP que le programme d'installation de View Agent ouvre sur le pare-feu. Pour plus d'informations, reportez-vous au document *Planification de l'architecture de View*.
- Si vous sélectionnez l'option d'installation personnalisée de View Composer Agent, vérifiez que vous possédez une licence pour utiliser View Composer.

Procédure

1 Pour démarrer le programme d'installation de View 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 les options d'installation personnalisée désirées.

Pour déployer des postes de travail de clone lié, sélectionnez l'option **View Composer Agent**.

4 Acceptez ou modifiez le dossier de destination.

5 Suivez les invites dans le programme d'installation de View 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 de View Agent vous invite à l'activer. Si vous n'activez pas la prise en charge du Bureau à distance au cours de l'installation de View Agent, vous devez l'activer manuellement une fois l'installation terminée.

6 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.

Le service VMware Horizon View Agent démarre sur la machine virtuelle.

Si vous avez sélectionné l'option **View Composer Agent**, le service VMware Horizon View Composer Guest Agent Server démarre sur la machine virtuelle.

Si Windows Media Player n'est pas installé, le programme d'installation de View Agent n'installe pas la fonction de redirection multimédia (MMR). Si vous installez Windows Media Player après l'installation de View Agent, vous pouvez installer la fonction MMR en exécutant de nouveau le programme d'installation de View Agent et en sélectionnant l'option Repair (Réparer).

Suivant

Si la machine virtuelle contient plusieurs cartes réseau, configurez le sous-réseau que View Agent utilise. Reportez-vous à la section « Configurer une machine virtuelle avec plusieurs cartes réseau pour View Agent », page 40.

Options d'installation personnalisée de View Agent

Lorsque vous installez View Agent sur une machine virtuelle, vous pouvez sélectionner ou désélectionner des options d'installation personnalisée. En outre, View 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, reportez-vous à « Matrice de prise en charge des fonctionnalités pour View Agent » dans le document *Planification de l'architecture de View*.

Toutes les options de configuration personnalisée, à l'exception de Carte à puce PCoIP, sont sélectionnées par défaut.

Tableau 3-2. Options d'installation personnalisée de View Agent

Option	Description
Redirection USB	Donne aux utilisateurs un accès à des périphériques USB connectés en local sur leurs postes de travail. L'option Redirection USB 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. **Remarque** 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 aux postes de travail View en utilisant HTML Access. L'agent HTML Access doit être installé sur les postes de travail View pour permettre aux utilisateurs de se connecter avec HTML Access.
View Composer Agent	Permet à View Agent de s'exécuter sur les postes de travail de clone lié déployés depuis cette machine virtuelle.
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.
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. 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 : ■ Postes de travail qui sont déployés sur des machines mono-utilisateur, notamment les machines postes de travail Windows et Windows Server 2008 R2 ■ 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 virtuelle est prise en charge sur les postes de travail qui sont déployés sur des machines de poste de travail mono-utilisateur. La fonction d'impression virtuelle n'est prise en charge que lorsque vous l'installez à partir de View Agent. Elle n'est pas prise en charge si vous l'installez avec VMware Tools.
vCenter Operations Manager Agent	Fournit des informations qui permettent à vCenter Operations Manager pour View de surveiller des postes de travail View.

Tableau 3-2. Options d'installation personnalisée de View Agent (suite)

Option	Description
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.
Carte à puce PCoIP	Permet aux utilisateurs de s'authentifier avec des cartes à puce lorsqu'ils utilisent le protocole d'affichage PCoIP. Cette fonction n'est pas installée par défaut. L'option Carte à puce PCoIP 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.

Tableau 3-3. Fonctionnalités de View Agent installées automatiquement

Option	Description
PCoIP Agent	Permet aux utilisateurs de se connecter au poste de travail View à l'aide du protocole d'affichage PCoIP. L'installation de la fonctionnalité PCoIP Agent désactive le mode veille sur les postes de travail Windows 8, Windows 7, Windows Vista et Windows XP. 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. **Remarque** Sous Windows Vista, si vous installez la fonctionnalité PCoIP Agent, la stratégie de groupe Windows **Désactiver ou activer la séquence de touches de sécurité (SAS, Secure Attention Sequence)** est activée et définie sur **Services** et **Applications d'ergonomie**. Si vous modifiez ce paramètre, l'authentification unique ne fonctionne pas correctement.
Redirection multimédia Wyse (MMR)	Fournit la redirection multimédia aux postes de travail et clients Windows XP et Windows Vista. 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.
Redirection multimédia (MMR) de Windows 7	Permet d'étendre la redirection multimédia pour les postes de travail Windows 7 et postes de travail client. 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.
Lync	Fournit la prise en charge de Microsoft Lync 2013 Client sur les postes de travail View.
Impression virtuelle avec PCoIP	Fournit l'impression virtuelle sur PCoIP. Cette fonctionnalité permet aux utilisateurs d'imprimer sur n'importe quelle imprimante disponible sur leur ordinateur client Windows. Les utilisateurs n'ont pas à installer des pilotes supplémentaires sur leurs postes de travail.

Tableau 3-3. Fonctionnalités de View Agent installées automatiquement (suite)

Option	Description
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.
Pilote audio virtuel	Fournit un pilote audio virtuel sur le poste de travail distant.

Installer View Agent en silence

Vous pouvez utiliser la fonction d'installation silencieuse de MSI (Microsoft Windows Installer) pour installer View 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.

Avec l'installation silencieuse, vous pouvez déployer efficacement les composants de View dans une grande entreprise.

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 27.
- Pour utiliser Windows Server 2008 R2 en tant que poste de travail distant à session unique (et non en tant qu'hôte RDS), procédez comme décrit dans « Préparer Windows Server 2008 R2 pour l'utiliser en tant que poste de travail », page 29.
- Téléchargez le fichier du programme d'installation View Agent sur la page du produit VMware sur http://www.vmware.com/products/.

  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 d'installation personnalisée de View Agent. Reportez-vous à la section « Options d'installation personnalisée de View Agent », page 31.
- Si vous sélectionnez l'option d'installation personnalisée de View Composer Agent, vérifiez que vous possédez une licence pour utiliser View Composer.
- 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 35.
- Familiarisez-vous avec les propriétés d'installation silencieuse disponibles avec View Agent. Reportez-vous à la section « Propriétés de l'installation silencieuse pour View Agent », page 37.
- Familiarisez-vous avec les ports TCP que le programme d'installation de View 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 View 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.

Cet exemple installe View Agent dans une machine virtuelle gérée par vCenter Server. Le programme d'installation configure les options de configuration personnalisées PCoIP, View Composer Agent, Impression virtuelle, Redirection USB, HTML Access, Unity Touch, Audio-vidéo en temps réel et Redirection multimédia (MMR) Windows 7.

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

Cet exemple installe View Agent sur un ordinateur non géré et inscrit le poste de travail avec le du Serveur de connexion View spécifié, `cs1.companydomain.com`. Le programme d'installation configure les options d'installation personnalisée : authentification unique, 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,ThinPrint,USB"
```

Le service VMware Horizon View Agent démarre sur la machine virtuelle.

Si vous avez sélectionné l'option **View Composer Agent**, le service VMware Horizon View Composer Guest Agent Server démarre sur la machine virtuelle.

Si Windows Media Player n'est pas installé, le programme d'installation de View Agent n'installe pas la fonction de redirection multimédia (MMR). Si vous installez Windows Media Player après l'installation de View Agent, vous pouvez installer la fonction MMR en exécutant de nouveau le programme d'installation de View Agent et en sélectionnant l'option Repair (Réparer).

Suivant

Si la machine virtuelle contient plusieurs cartes réseau, configurez le sous-réseau que View Agent utilise. Reportez-vous à la section « Configurer une machine virtuelle avec plusieurs cartes réseau pour View Agent », page 40.

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. Par exemple : `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s` 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. Par exemple : `VMware-viewagent-y.y.y-xxxxxx.exe /s /v"command_line_options"` 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. Par exemple : `VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"command_line_options INSTALLDIR=""d:\abc\my folder"""` 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. 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. Par exemple, vous voulez peut-être installer View Agent en silence et n'utiliser que des options et des fonctions d'installation par défaut : `VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn"` 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. L'option `/qn` ou `/qb` est obligatoire pour que l'installation soit silencieuse.
`INSTALLDIR`	Spécifie un autre chemin d'installation pour le composant View. 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. Cette propriété MSI est facultative.

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

Option ou propriété MSI	Description
ADDLOCAL	Détermine les fonctionnalités spécifiques du composant à installer. Dans une installation interactive, le programme d'installation de View affiche des options d'installation personnalisée à sélectionner et installe d'autres fonctionnalités automatiquement. La propriété ADDLOCAL vous permet de spécifier ces options et fonctionnalités sur la ligne de commande. Vous pouvez utiliser ADDLOCAL pour installer de manière sélective les options et fonctionnalités d'installation individuelle. Les fonctionnalités que vous ne spécifiez pas explicitement ne sont pas installées. Tapez ADDLOCAL=ALL pour installer toutes les fonctionnalités installées automatiquement (sur les systèmes d'exploitation invités pris en charge) et toutes les options d'installation personnalisée qui sont installées par défaut. Par exemple : VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=ALL" Les options d'installation par défaut et les fonctionnalités installées automatiquement seront installées si vous n'utilisez pas la propriété ADDLOCAL. Taper ADDLOCAL=ALL sans utiliser la propriété ADDLOCAL aboutit au même résultat. Pour spécifier des options et fonctionnalités 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=*valeur*,*valeur*,*valeur*.... Contrairement à une installation interactive, cette méthode installe uniquement les fonctionnalités spécifiées. Par exemple, vous voulez peut-être installer View Agent dans un système d'exploitation client avec les fonctions View Composer Agent et PCoIP : VMware-viewagent-*y.y.y-xxxxxx*.exe /s /v"/qn ADDLOCAL=Core,SVIAgent,PCoIP" **IMPORTANT** La fonctionnalité Core est requise si vous spécifiez des fonctionnalités individuelles avec ADDLOCAL=*value*,*value*,*value*.... La propriété MSI ADDLOCAL est facultative.
REBOOT	Vous pouvez utiliser l'option REBOOT=ReallySuppress pour autoriser l'exécution de tâches de configuration système avant le redémarrage du système. Cette propriété MSI est facultative.
/l*v *log_file*	Écrit des informations de journalisation dans le fichier journal spécifié avec une sortie détaillée. Par exemple : /l*v ""%TEMP%\vmmsi.log"" Cet exemple génère un fichier journal détaillé semblable à celui généré lors d'une installation interactive. 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. L'option /l*v est facultative.

Propriétés de l'installation silencieuse pour View Agent

Vous pouvez inclure des propriétés spécifiques lorsque vous installez de façon silencieuse View Agent à partir de la ligne de commande. Vous devez utiliser la forme *Propriété=valeur* de manière que Microsoft Windows Installer (MSI) puisse interpréter les propriétés et les valeurs.

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

Tableau 3-6. Propriétés MSI pour l'installation silencieuse de View Agent

Propriété MSI	Description	Valeur par défaut
INSTALLDIR	Chemin d'accès et dossier dans lequel le logiciel View Agent est installé. Par exemple : `INSTALLDIR=""D:\abc\my folder""` Les jeux de deux guillemets doubles entourant le chemin autorisent le programme d'installation MSI à ignorer l'espace dans le chemin. Cette propriété MSI est facultative.	`%ProgramFiles %\VMware\VMware View\Agent`
RDPCHOICE	Détermine l'activation du protocole RDP (Remote Desktop Protocol) sur le poste de travail. Une valeur de 1 active RDP. Une valeur de 0 laisse le paramètre RDP désactivé. 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. 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 148. Cette propriété MSI est facultative.	
VDM_VC_MANAGED_AGENT	Détermine si vCenter Server gère la machine virtuelle sur laquelle View Agent est installé. Une valeur de 1 configure le poste de travail en tant que machine virtuelle gérée par vCenter Server. Une valeur de 0 configure le poste de travail comme étant non géré par vCenter Server. 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 de View Agent inscrit un poste de travail non géré. Cette propriété s'applique uniquement à des postes de travail non gérés. Par exemple : `VDM_SERVER_NAME=10.123.01.01` Cette propriété MSI est requise pour les postes de travail non gérés. 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. Par exemple : `VDM_SERVER_USERNAME=admin.companydomain.com` Cette propriété MSI est requise pour les postes de travail non gérés. 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. Par exemple : `VDM_SERVER_PASSWORD=secret` Cette propriété MSI est requise pour les postes de travail non gérés. N'utilisez pas cette propriété MSI pour les postes de travail de machine virtuelle gérés par vCenter Server.	Aucune

Dans une commande d'installation silencieuse, vous pouvez utiliser la propriété MSI `ADDLOCAL=` pour spécifier les fonctionnalités que le programme d'installation de View Agent configure.

Si vous spécifiez des fonctionnalités individuelles avec la propriété ADDLOCAL=, vous devez inclure la fonctionnalité Core.

Tableau 3-7 montre les fonctionnalités de View Agent que vous pouvez entrer sur la ligne de commande et qui correspondent à des options d'installation que vous pouvez sélectionner ou désélectionner lors d'une installation interactive. Pour plus de détails sur les options d'installation personnalisées, reportez-vous à « Options d'installation personnalisée de View Agent », page 31.

Lors d'une installation interactive, toutes les fonctionnalités suivantes, à l'exception de Carte à puce PCoIP, sont installées par défaut.

Tableau 3-7. Fonctions d'installation silencieuse de View Agent et options d'installation personnalisée interactive

Fonction de l'installation silencieuse	Option de l'installation personnalisée dans une installation interactive
USB	Redirection USB
HtmlAccess	Agent HTML Access
SVIAgent	View Composer Agent
RTAV	Audio/Vidéo en temps réel
ThinPrint	Impression virtuelle
V4V	vCenter Operations Manager pour View
VPA	View Persona Management
Carte à puce	Carte à puce PCoIP. Cette fonctionnalité n'est pas installée par défaut dans une installation interactive.

Tableau 3-8 montre les fonctionnalités de View Agent que vous pouvez entrer sur la ligne de commande, qui sont installées automatiquement pendant une installation interactive. Les fonctionnalités sont installées sur tous les systèmes d'exploitation invités sur lesquels elles sont prises en charge. Ces fonctionnalités ne correspondent à aucune des options d'installation présentées lors d'une installation interactive.

Tableau 3-8. Fonctionnalités d'installation silencieuse de View Agent qui sont installées automatiquement dans une installation interactive

Fonction de l'installation silencieuse	Description
Core	Fonctions Core de View Agent. Si vous spécifiez des fonctions individuelles avec la propriété ADDLOCAL=, vous devez inclure Core. Si vous spécifiez ADDLOCAL=ALL, les fonctionnalités Core sont installées.
ThinPrintPCoIP	Impression virtuelle avec PCoIP
PCoIP	Agent du protocole PCoIP
VmVideo	Pilote vidéo virtuel
VmwVaudio	Pilote audio virtuel
UnityTouch	Unity Touch
MMR	Redirection multimédia (MMR) de Windows 7

Vous installez la fonctionnalité Redirection d'URL Flash en tapant l'argument de ligne de commande FlashURLRedirection 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 ADDLOCAL=Core,PCoIP,SVIAgent,ThinPrint,USB,HtmlAccess,UnityTouch,FlashURLRedirection,RTAV,MMR"`

Configurer une machine virtuelle avec plusieurs cartes réseau pour View Agent

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

Procédure

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

  Par exemple : **`HKLM\Software\VMware, Inc.\VMware VDM\Node Manager\subnet = 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.

Optimiser les performances des systèmes d'exploitation invités pour toutes les versions de Windows

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. Ces étapes s'appliquent à tous les systèmes d'exploitation Windows. 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.

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.
- Si les utilisateurs veulent lire des vidéos en plein écran ou exécuter des applications 3D sur des postes de travail exécutés dans un environnement vSphere 5.1, suivez les instructions pour modifier le registre dans l'article 235257 de la Base de connaissances Microsoft.

  Cet article est intitulé « Le serveur n'utilise pas toute la bande passante disponible lors de la diffusion en continu de fichiers avec des vitesses de transmission supérieures à 100 Kbit/s » et se trouve à l'adresse http://support.microsoft.com/kb/235257. Redémarrez la machine virtuelle pour que le paramètre de registre modifié prenne effet.

  Sans cette optimisation, les images peuvent se figer brièvement ou les vidéos peuvent être saccadées.

  Remarque Cette optimisation permet d'améliorer les performances dans ESXi 5.x et ESXi 5.1, mais elle est requise pour ESXi 5.1.

Suivant

Pour les systèmes d'exploitation client Windows 7 et Windows 8, effectuez des tâches d'optimisation complémentaires. Reportez-vous à la section « Optimiser les performances du système d'exploitation client Windows 7 et Windows 8 », page 41.

Optimiser les performances du système d'exploitation client Windows 7 et Windows 8

Vous pouvez effectuer des étapes supplémentaires pour optimiser les performances du système d'exploitation invité Windows 7 et Windows 8 pour le déploiement de postes de travail distants. Toutes ces étapes sont facultatives.

Prérequis

- Effectuez les opérations d'optimisation du système d'exploitation client qui s'appliquent à tous les systèmes d'exploitation Windows. Reportez-vous à la section « Optimiser les performances des systèmes d'exploitation invités pour toutes les versions de Windows », page 40.
- 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 42.

Procédure

1. Désinstallez Tablet PC Components, à moins que cette fonction soit requise.
2. Désactivez IPv6, sauf si l'option est requise.
3. 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`

4 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)`**.

5 Désactivez le programme d'amélioration de l'expérience utilisateur Windows et les tâches liées du Planificateur de tâches.

6 Arrêtez le système d'exploitation client et éteignez la machine virtuelle.

7 Activez la machine virtuelle.

Suivant

Reportez-vous à « Optimisation de Windows 7 et Windows 8 pour les machines virtuelles de clone lié », page 43 pour obtenir des informations sur la désactivation de certains services et de certaines tâches Windows 7 et Windows 8 pour réduire la croissance des machines virtuelles de clone lié de 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 et Windows 8 dans des pools de postes de travail volumineux.

Procédure

1 Dans le système d'exploitation client 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** et **ProgramDataUpdater**.

7 Dans le nœud **Bibliothèque du Planificateur de tâches > Microsoft > Windows**, ouvrez le dossier **Customer Experience Improvement Program**.

8 Désactivez les tâches **Consolidateur**, **KernelCEIPTask** et **Utiliser CEIP**.

Suivant

Réalisez d'autres tâches d'optimisation de Windows 7 ou Windows 8. Reportez-vous à la section « Optimiser les performances du système d'exploitation client Windows 7 et Windows 8 », page 41.

Optimisation de Windows 7 et Windows 8 pour les machines virtuelles de clone lié

En désactivant certains services et tâches de Windows 7 ou Windows 8, vous pouvez réduire la croissance des machines virtuelles de clone lié de 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 7 et Windows 8

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

Windows 7 et Windows 8 contiennent de nouveaux services et planifient des services plus anciens à exécuter par défaut, tels que la défragmentation de disque. 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 par seconde (IOPS) sur les machines virtuelles Windows 7 ou Windows 8. La désactivation de ces services peut réduire l'IOPS et améliorer les performances sur des machines virtuelles complètes et des clones liés.

La désactivation de certains services peut également avantager des systèmes d'exploitation Windows XP et Windows Vista.

Ces meilleures pratiques pour l'optimisation de Windows 7 et Windows 8 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, la désactivation du service Windows Update est judicieuse si vous actualisez et recomposez les clones liés. Une opération d'actualisation restaure les disques du système d'exploitation sur leurs derniers snapshots, ce qui supprime toutes les mises à jour Windows automatiques depuis la prise des derniers snapshots. Une opération de recomposition recrée les disques du système d'exploitation à partir d'un nouveau snapshot pouvant contenir les mises à jour Windows actuelles, ce qui rend les mises à jour Windows automatiques redondantes.

Si vous n'utilisez pas l'actualisation et la recomposition régulièrement, vous pouvez décider de laisser le service Windows Update actif.

Présentation des services et tâches Windows 7 et Windows 8 qui entraînent la croissance de clone lié

Un certain nombre de services et de tâches de Windows 7 et Windows 8 peuvent entraîner la croissance incrémentielle des disques du systèmes d'exploitation des clones liés à intervalles réguliers, même si les machines de clone lié sont inactives. 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 IOPS sur les machines virtuelles Windows 7 et Windows 8. Vous pouvez évaluer les avantages de la désactivation de ces services sur des machines virtuelles complètes ainsi que sur des clones liés.

Avant de désactiver les services Windows 7 ou Windows 8 présentés dans Tableau 3-9, vérifiez que vous avez suivi la procédure d'optimisation de « Optimiser les performances des systèmes d'exploitation invités pour toutes les versions de Windows », page 40 et de « Optimiser les performances du système d'exploitation client Windows 7 et Windows 8 », page 41.

Tableau 3-9. Impact des services et tâches Windows 7 et Windows 8 sur la croissance du disque du système d'exploitation et l'IOPS lorsque le système d'exploitation est laissé inactif

Service ou tâche	Description	Occurrence par défaut ou démarrage	Impact sur les disques du système d'exploitation de clone lié	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. 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. Lorsque la mise en veille prolongée est déclenchée, le système écrit un fichier `hiberfil.sys` de la taille de la RAM installée.	Oui La mise en veille prolongée n'a aucun avantage dans un environnement virtuel. Pour obtenir des instructions, consultez « Désactiver la mise en veille prolongée Windows sur la machine virtuelle parente », page 54..
Défragmentation de disque planifiée Windows	La défragmentation de disque est planifiée en tant que processus d'arrière-plan.	Une fois par semaine	Élevé. Des opérations de défragmentation répétées peuvent augmenter de plusieurs Go la taille des disques du système d'exploitation de clone lié et ne rendent pas l'accès au disque plus efficace sur les clones liés.	Élevée	Oui
Service Windows Update	Détecte, télécharge et installe des mises à jour pour Windows et d'autres programmes.	Démarrage automatique	Moyen à élevé. Entraîne des écritures fréquentes sur les disques du système d'exploitation des clones liés car des vérifications de mise à jour se produisent souvent. L'impact dépend des mises à jour téléchargées.	Moyen à élevé	Oui, si vous utilisez la recomposition de View Composer pour installer des mises à jour Windows et l'actualisation pour remettre les disques du système d'exploitation à leurs snapshots d'origine.
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. 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 3-9. Impact des services et tâches Windows 7 et Windows 8 sur la croissance du disque du système d'exploitation et l'IOPS lorsque le système d'exploitation est laissé inactif (suite)

Service ou tâche	Description	Occurrence par défaut ou démarrage	Impact sur les disques du système d'exploitation de clone lié	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. Cette fonction a été présentée dans Windows XP.	Toujours activé, sauf s'il est désactivé.	Moyenne 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. Chaque fois que cette tâche s'exécute, elle génère des fichiers de sauvegarde de registre.	Moyen.	Oui. La sauvegarde du registre Windows n'est pas nécessaire. Pour restaurer des données de registre, vous pouvez utiliser l'opération d'actualisation de View Composer.
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. Capture un point de restauration système dès que le système détecte qu'il est nécessaire. Lorsque le clone lié est inactif, ce temps système est faible.	Aucun impact majeur.	Oui Bien que son impact soit faible, cette tâche est redondante si vous utilisez l'actualisation de View Composer pour rétablir des disques du système d'exploitation à leurs snapshots d'origine.

Tableau 3-9. Impact des services et tâches Windows 7 et Windows 8 sur la croissance du disque du système d'exploitation et l'IOPS lorsque le système d'exploitation est laissé inactif (suite)

Service ou tâche	Description	Occurrence par défaut ou démarrage	Impact sur les disques du système d'exploitation de clone lié	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. 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. 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 des machines virtuelles parentes Windows 7 et Windows 8

Avant de créer des clones liés, vous devez désactiver les défragmentations planifiées sur des machines virtuelles parentes Windows 7 et Windows 8. Par défaut, Windows 7 et Windows 8 planifient des défragmentations de disque une fois par semaine. Des opérations de défragmentation répétées augmentent significativement la taille des disques du système d'exploitation de clone lié et ne rendent pas l'accès au disque plus efficace sur les clones liés.

Lorsque vous créez un pool de clone lié à partir de la machine virtuelle parente, les clones liés partagent le disque du réplica. Les opérations de défragmentation suivantes n'affectent pas le disque du réplica, qui est en lecture seule. Au lieu de cela, les défragmentations développent le disque du système d'exploitation de chaque clone.

Il est recommandé de défragmenter la machine virtuelle parente une fois, avant de prendre un snapshot et de créer le pool. Les clones liés bénéficient de la défragmentation car ils partagent le disque optimisé en lecture seule du réplica.

Prérequis

- Vérifiez que les applications que vous prévoyez de déployer sur les clones liés sont installés sur la machine virtuelle.

- Vérifiez que View Agent avec View Composer Agent est installé sur la machine virtuelle.

Procédure

1. Dans vSphere Client, sélectionnez la machine virtuelle parente et sélectionnez **Ouvrir la console**.
2. Ouvrez une session sur le système d'exploitation client Windows 7 ou Windows 8 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**.

Les opérations de défragmentation n'auront pas lieu sur des machines virtuelles de clone lié créées à partir de cette machine virtuelle parente.

Désactiver le service Windows Update sur des machines virtuelles Windows 7 et Windows 8

La désactivation du service Windows Update peut réduire le nombre de fichiers créés et les écritures se produisant lorsque des mises à jour sont téléchargées et installées. Cette action peut réduire la croissance de clone lié et réduire l'IOPS dans des clones liés et des machines virtuelles complètes.

Désactivez le service Windows Update si vous actualisez et recomposez les postes de travail de clone lié. Une opération d'actualisation restaure les disques du système d'exploitation à leurs snapshots d'origine, en supprimant les mises à jour Windows automatiques. Une opération de recomposition recrée les disques du système d'exploitation à partir d'un nouveau snapshot pouvant contenir des mises à jour Windows, ce qui rend les mises à jour Windows automatiques redondantes.

Ne désactivez pas le service Windows Update si vous n'utilisez pas la recomposition pour installer des mises à jour Windows dans les clones liés.

Prérequis

Vérifiez que les mises à jour Windows les plus récentes sont téléchargées et installées sur la machine virtuelle.

Procédure

1. Dans vSphere Client, sélectionnez la machine virtuelle parente et sélectionnez **Ouvrir la console**.
2. Ouvrez une session sur le système d'exploitation client Windows 7 ou Windows 8 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 7 et Windows 8

La désactivation du service de stratégie de diagnostic Windows peut réduire le nombre d'écritures système et diminuer la croissance des machines de clone lié.

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

Procédure

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

2 Ouvrez une session sur le système d'exploitation client Windows 7 ou Windows 8 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 7 et Windows 8

En désactivant les fonctions de prérécupération et Superfetch de Windows, vous pouvez éviter de générer des fichiers de prérécupération et le temps système associé aux opérations de prérécupération et Superfetch. Cette action peut réduire la croissance des machines de clone lié et réduire l'IOPS sur des machines virtuelles complètes et des clones liés.

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.

Prérequis

Pour plus d'informations sur l'utilisation de l'éditeur de Registre Windows sous Windows 7 et Windows 8, consultez le site Web Microsoft TechNet.

Procédure

1 Démarrez l'éditeur de Registre Windows sur la machine virtuelle Windows 7 ou Windows 8 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 7 et Windows 8

La désactivation de la fonctionnalité de sauvegarde du Registre Windows, `RegIdleBackup`, peut réduire le nombre d'écritures système et diminuer la croissance des machines de clone lié.

Procédure

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

2 Ouvrez une session sur le système d'exploitation client Windows 7 ou Windows 8 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 7 et Windows 8

Vous n'avez pas à utiliser la fonction de Restauration du système Windows si vous utilisez l'actualisation de View Composer pour restaurer des disques du système d'exploitation de clone lié sur leurs snapshots d'origine.

Lorsque le système d'exploitation est inactif, la Restauration du système n'a pas un impact visible sur la croissance du disque du système d'exploitation. Toutefois, lorsque le système d'exploitation est utilisé, la Restauration du système génère des points de restauration basés sur l'utilisation du système, ce qui a un impact important sur la croissance du disque du système d'exploitation.

La fonction de Restauration du système Windows est la même que l'actualisation de View Composer.

Il est recommandé de désactiver la Restauration du système Windows et d'éviter une croissance inutile dans vos clones liés.

Si vous n'utilisez pas l'actualisation, évaluez s'il est plus utile de laisser la Restauration du système active dans votre environnement View.

Procédure

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

2 Ouvrez une session sur le système d'exploitation client Windows 7 ou Windows 8 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 7 et Windows 8

Microsoft Windows Defender peut contribuer à la croissance du disque du système d'exploitation de clone lié et à l'augmentation de l'IOPS dans des clones liés et des machines virtuelles complètes. Désactivez Windows Defender si vous installez un autre logiciel anti-espion sur la machine virtuelle.

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.

Procédure

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

2 Ouvrez une session sur le système d'exploitation client Windows 7 ou Windows 8 en tant qu'administrateur.

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

4 Sélectionnez **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 7 et Windows 8

Windows Internet Explorer utilise la tâche Microsoft Feeds Synchronization pour mettre à jour des flux RSS dans les navigateurs Web des utilisateurs. Cette tâche peut contribuer à la croissance de clone lié. Désactivez cette tâche si vos utilisateurs n'ont pas besoin de mises à jour automatiques des flux RSS dans leurs navigateurs.

Microsoft Feeds Synchronization peut entraîner 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. Dans cette situation, vous devez toujours désactiver Microsoft Feeds Synchronization pour contrôler la croissance de disque persistant.

Procédure

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

2 Ouvrez une session sur le système d'exploitation client Windows 7 ou Windows 8 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 de machines virtuelles pour View Composer

Pour déployer un pool de postes de travail de clone lié, vous devez préparer une machine virtuelle parente qui répond aux exigences du service View Composer.

- Préparer une machine virtuelle parente page 51

  Le service View Composer requiert une machine virtuelle parente à partir de laquelle vous générez une image de base pour créer et gérer un pool de postes de travail de clone lié.

- Activation de Windows sur des machines virtuelles de clone lié page 54

  Pour vous assurer que View Composer active correctement les systèmes d'exploitation Windows 8, Windows 7 et Windows Vista sur des machines de clone lié, 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 54

  L'option de mise en veille prolongée Windows crée un fichier système volumineux qui peut augmenter la taille des disques du système d'exploitation de clone lié créés à partir de la machine virtuelle parente. La désactivation de l'option de mise en veille prolongée réduit la taille des clones liés.

- Configurer une machine virtuelle parente pour utiliser le stockage local page 55

  Lorsque vous préparez une machine virtuelle parente pour View Composer, vous pouvez configurer cette dernière et ses clones liés afin de stocker des fichiers d'échange de machine virtuelle dans la banque de données locale. Cette stratégie facultative vous permet de bénéficier du stockage local.

- Conserver une trace de la taille du fichier d'échange de la machine virtuelle parente page 56

  Lorsque vous créez un pool de clone lié, vous pouvez rediriger les fichiers d'échange et temporaires du système d'exploitation client des clones liés vers un disque séparé. Vous devez configurer ce disque pour qu'il soit plus volumineux que le fichier d'échange sur le système d'exploitation client.

- Augmenter la limite du délai d'expiration des scripts de personnalisation QuickPrep page 57

  View Composer termine un script de post-synchronisation ou de désactivation QuickPrep qui prend plus de 20 secondes. Vous pouvez augmenter la limite du délai d'expiration de ces scripts en modifiant la valeur de registre Windows `ExecScriptTimeout` sur la machine virtuelle parente.

Préparer une machine virtuelle parente

Le service View Composer requiert une machine virtuelle parente à partir de laquelle vous générez une image de base pour créer et gérer un pool de postes de travail de clone lié.

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 de machines virtuelles pour un déploiement de postes de travail distants », page 23.

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.

Important Pour utiliser les fonctionnalités prises en charge dans View Manager 4.5 ou version ultérieure, telles que la redirection de données supprimables sur un disque séparé et la personnalisation de machines de clone lié avec Sysprep, vous devez déployer les machines à partir d'une machine virtuelle parente sur laquelle View Agent 4.5 ou version ultérieure est installé.

Vous ne pouvez pas utiliser View Composer pour déployer des machines exécutant Windows Vista Édition Intégrale ou Windows XP Professionnel SP1.

- 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.

- Si la machine virtuelle parente s'exécute sous Windows XP, et qu'Active Directory s'exécute sous Windows Server 2008, appliquez un correctif de mise à jour sur la machine virtuelle Windows XP. Consultez l'article 944043 du support Microsoft à l'adresse suivante : http://support.microsoft.com/kb/944043/en-us.

  Si vous n'installez pas le pack de compatibilité du contrôleur de domaine en lecture seule (RODC) Windows Server 2008 pour Windows XP, les clones liés déployés à partir de cette machine virtuelle parente ne parviennent pas à joindre le domaine.

- Lorsque vous installez View Agent sur la machine virtuelle parente, sélectionnez l'option **View Composer Agent**. Reportez-vous à la section « Installer View Agent sur une machine virtuelle », page 30.

  Pour mettre à jour View 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 View 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 qui exécutent Windows 8, Windows 7 ou Windows Vista, configurez une clé de licence en volume et activez le système d'exploitation de la machine virtuelle parente avec l'activation du volume. Reportez-vous à la section « Activation de Windows sur des machines virtuelles de clone lié », page 54.

- Si la machine virtuelle parente exécute Windows 7 ou Windows 8, vérifiez que vous avez suivi les meilleures pratiques pour optimiser le système d'exploitation. Reportez-vous à la section « Optimisation de Windows 7 et Windows 8 pour les machines virtuelles de clone lié », page 43.

- 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. Le service View Composer ne prend pas en charge les partitions de disque multiples. Plusieurs disques virtuels sont pris en charge.

  REMARQUE 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 liés qui sont créés ou recomposés à partir de la machine virtuelle ne contiendront pas le disque indépendant.
- 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 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 8.1 et Windows Server 2008 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.

Vous pouvez déployer un pool de clone lié à partir de la machine virtuelle parente.

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 machines virtuelles de clone lié

Pour vous assurer que View Composer active correctement les systèmes d'exploitation Windows 8, Windows 7 et Windows Vista sur des machines de clone lié, 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 8, Windows 7 ou Windows Vista avec l'activation du volume, vous utilisez un service de gestion des clés (KMS), qui requiert 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.

REMARQUE Les machines Windows XP avec des licences en volume ne requièrent pas d'activation.

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.

L'outil QuickPrep de View Composer implémente l'activation comme suit :

1 Il appelle un script pour supprimer l'état de licence existant sur la machine virtuelle de clone lié.

2 Il redémarre le système d'exploitation client.

3 Il appelle un script qui utilise la licence KMS pour activer le système d'exploitation sur le clone.

Chaque fois que QuickPrep s'exécute sur un clone lié, l'activation a lieu.

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

L'option de mise en veille prolongée Windows crée un fichier système volumineux qui peut augmenter la taille des disques du système d'exploitation de clone lié créés à partir de la machine virtuelle parente. La désactivation de l'option de mise en veille prolongée réduit la taille des clones liés.

L'option de mise en veille prolongée de Windows crée un fichier système masqué, `Hiberfil.sys`. Windows utilise ce fichier pour stocker une copie de la mémoire système sur le disque dur lorsque le paramètre de veille hybride est activé. Lorsque vous créez un pool de clone lié, le fichier est créé sur le disque du système d'exploitation sur chaque clone lié.

Sur des machines virtuelles Windows 7 ou Windows 8, ce fichier peut atteindre 10 Go.

AVERTISSEMENT Lorsque vous activez la mise en veille prolongée, le paramètre de veille hybride ne fonctionne pas. Les utilisateurs peuvent perdre des données si le paramètre de veille hybride est activé et qu'une coupure de courant se produit.

Prérequis

Familiarisez-vous avec la fonction de mise en veille prolongée de Windows. Consultez le site Web du support Microsoft. Pour plus d'informations sur la désactivation de la mise en veille prolongée sous Windows 8, Windows 7 ou Windows Vista, consultez le site Web du support Microsoft et recherchez comment désactiver et réactiver la mise en veille prolongée sur un ordinateur exécutant Windows.

Procédure

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

2 Ouvrez une session sur le système d'exploitation client Windows en tant qu'administrateur.

3 Désactivez l'option de mise en veille prolongée.

Système d'exploitation	Action
Windows 8, Windows 7 ou Windows Vista	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.
Windows XP	a Cliquez sur **Démarrer > Exécuter**. b Saisissez **`cmd`** et cliquez sur **OK**. c À l'invite de commande, saisissez **`powercfg.exe /hibernate off`** et appuyez sur Entrée. d Saisissez **`exit`** et appuyez sur Entrée.

4 Fermez la session sur le système d'exploitation client.

Lorsque vous créez des machines de clone lié à partir de la machine virtuelle parente, le fichier `Hiberfil.sys` n'est pas créé sur les disques de système d'exploitation de clone lié.

Configurer une machine virtuelle parente pour utiliser le stockage local

Lorsque vous préparez une machine virtuelle parente pour View Composer, vous pouvez configurer cette dernière et ses clones liés afin de stocker des fichiers d'échange de machine virtuelle dans la banque de données locale. Cette stratégie facultative vous permet de bénéficier du stockage local.

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 67.

Prérequis

Préparez la machine virtuelle parente pour répondre aux exigences du service View Composer. Reportez-vous à la section « Préparer une machine virtuelle parente », page 51.

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.

Lorsque vous déployez un pool à partir de cette machine virtuelle parente, les clones liés utilisent la banque de données de fichiers d'échange de l'hôte ESXi local.

Conserver une trace de la taille du fichier d'échange de la machine virtuelle parente

Lorsque vous créez un pool de clone lié, vous pouvez rediriger les fichiers d'échange et temporaires du système d'exploitation client des clones liés vers un disque séparé. Vous devez configurer ce disque pour qu'il soit plus volumineux que le fichier d'échange sur le système d'exploitation client.

Lorsqu'un clone lié configuré avec un disque distinct pour les fichiers supprimables est mis hors tension, View remplace le disque temporaire par une copie du disque temporaire d'origine que View Composer a créé avec le pool de clone lié. Cette fonction peut ralentir la croissance des clones liés. Toutefois, cette fonction ne peut agir que si vous configurez le disque de fichier supprimable pour qu'il soit suffisamment volumineux pour contenir les fichiers d'échange du système d'exploitation client.

Avant de configurer le disque de fichier supprimable, vous devez connaître la taille maximale de fichier d'échange dans la machine virtuelle parente. Les clones liés ont la même taille de fichier d'échange que la machine virtuelle parente à partir de laquelle ils sont créés.

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 « Préparer une machine virtuelle parente », page 51.

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 une machine virtuelle parente pour utiliser le stockage local », page 55.

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 QuickPrep

View Composer termine un script de post-synchronisation ou de désactivation QuickPrep qui prend plus de 20 secondes. Vous pouvez augmenter la limite du délai d'expiration de ces scripts en modifiant la valeur de registre Windows `ExecScriptTimeout` sur la machine virtuelle parente.

La limite augmentée du délai d'expiration est propagée aux clones liés créés à partir de la machine virtuelle parente. Les scripts de personnalisation QuickPrep peuvent s'exécuter sur les clones liés à l'heure que vous spécifiez.

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

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.

Prérequis

- Installez View Agent avec l'option **View Composer Agent** sur la machine virtuelle parente.
- Vérifiez que la machine virtuelle parente est préparée pour créer un pool de clone lié. Reportez-vous à la section « Préparer une machine virtuelle parente », page 51.

Procédure

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

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

   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.

La valeur du délai d'expiration est augmentée. Vous n'avez pas à redémarrer Windows pour que cette valeur prenne effet.

Suivant

Prenez un snapshot de la machine virtuelle parente et créez un pool de clone lié.

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 59.

Remarque Vous ne créez pas de pool de clone lié depuis un modèle de machine virtuelle.

Création de spécifications de personnalisation

Les spécifications de personnalisation sont facultatives, mais elles peuvent faciliter considérablement les déploiements de pools automatisés en fournissant des informations de configuration de propriétés générales, telles que des paramètres de licence, d'association de domaines et de protocole DHCP.

Les spécifications de personnalisation vous permettent de personnaliser les postes de travail distants à mesure qu'ils sont créés dans View Administrator. Vous créez de nouvelles spécifications de personnalisation en utilisant l'assistant Customization Specification (Spécification de personnalisation) dans vSphere Client. Vous pouvez également utiliser l'assistant Customization Specification (Spécification de personnalisation) pour importer des fichiers `sysprep.ini` personnalisés existants.

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)*.

Assurez-vous que les spécifications de personnalisation sont exactes avant de les utiliser dans View Administrator. Dans vSphere Client, déployez et personnalisez une machine virtuelle depuis votre modèle à l'aide des spécifications de personnalisation. Testez entièrement la machine virtuelle, notamment DHCP et l'authentification, avant de créer des postes de travail distants.

Remarque Pour appliquer des spécifications de personnalisation à des pools de postes de travail qui utilisent Windows XP, vous devez installer des outils Microsoft Sysprep sur votre machine vCenter Server.

Vous n'avez pas à installer des outils Sysprep dans vCenter Server pour les pools de postes de travail qui utilisent Windows 8, Windows 7 ou Vista. Les outils Sysprep sont intégrés à ces systèmes d'exploitation.

Lorsque vous utilisez une spécification de personnalisation Sysprep pour associer un poste de travail Windows 8 ou Windows 7 à un domaine, vous devez utiliser le nom de domaine complet (FQDN) du domaine Active Directory. Vous ne pouvez pas utiliser le nom NetBIOS du domaine Active Directory.

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.

Pour créer un pool de clones liés, reportez-vous à la section « Pools de postes de travail de clone lié », page 67

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 : ■ 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. ■ Dans un pool à attribution flottante, les utilisateurs reçoivent des machines différentes chaque fois qu'ils ouvrent une session. Pour plus d'informations, reportez-vous à « Affectation d'utilisateur dans des pools de postes de travail », page 115.	
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. Si vous n'activez pas l'attribution automatique, vous devez attribuer une machine à chaque utilisateur de manière explicite. 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. 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. 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. 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 dans le document *Administration de View*. **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. 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. 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 124. 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 64 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 128.	
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. Pour plus d'informations, reportez-vous à « Dénomination manuelle de machines ou fourniture d'un mode d'attribution de nom », page 116.	
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. 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. Pour plus d'informations, reportez-vous à « Utilisation d'un mode d'attribution de nom pour des pools de postes de travail automatisés », page 119.	

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. 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 116. 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. Le nombre minimal de machines est créé lorsque vous créez le pool. 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 193.	
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. 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. Pour les clusters, vous pouvez utiliser des magasins des données partagés ou locaux. 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. Cette fonction est prise en charge sur vSphere 5.0 et supérieur. Cette fonction est activée par défaut. Pour plus d'informations, reportez-vous à « Configurer View Storage Accelerator pour des pools de postes de travail », page 207.	
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. 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.

Pour créer un pool de clones liés, reportez-vous à la section « Pools de postes de travail de clone lié », page 67

Prérequis

- Préparez un modèle de machine virtuelle que View utilisera pour créer les machines. View Agent doit être installé sur le modèle. Reportez-vous à la section Chapitre 3, « Création et préparation de machines virtuelles », page 23.
- 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 59.
- 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 124.
- Si vous prévoyez de fournir un accès à vos applications et postes de travail via Workspace, 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, Workspace ne reconnaîtra pas l'authentificateur SAML que vous configurez dans View et vous ne pourrez pas configurer le pool dans Workspace.

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 141.

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 124

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

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

Paramètre	Pool automatisé, affectation dédiée	Pool automatisé, affectation flottante
Automatic logoff after disconnect (Fermeture de session automatique après la déconnexion)	Oui	Oui
Autoriser les utilisateurs à réinitialiser leurs machines	Oui	Oui
Autoriser plusieurs sessions par utilisateur		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
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 créer 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 : ■ 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. ■ Dans un pool à attribution flottante, les utilisateurs reçoivent des machines différentes chaque fois qu'ils ouvrent une session. Pour plus d'informations, reportez-vous à « Affectation d'utilisateur dans des pools de postes de travail », page 115.	
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. 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. 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. 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. 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 dans le document *Administration de View*. **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.	

Tableau 5-1. Feuille de calcul : options de configuration pour créer un pool de postes de travail de clone lié (suite)

Option	Description	Indiquez votre valeur ici
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. 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. 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 124. 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 80. 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 128.	
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. Pour plus d'informations, reportez-vous à « Dénomination manuelle de machines ou fourniture d'un mode d'attribution de nom », page 116.	
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. 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. Pour plus d'informations, reportez-vous à « Utilisation d'un mode d'attribution de nom pour des pools de postes de travail automatisés », page 119.	

Tableau 5-1. Feuille de calcul : options de configuration pour créer un pool de postes de travail de clone lié (suite)

Option	Description	Indiquez votre valeur ici
Nombre max. de machines	Si vous utilisez un mode d'attribution de nom, spécifiez le nombre total de machines dans le pool. 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 116. 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 prêtes et provisionnées pendant l'exécution des opérations de View Composer. Ce paramètre vous permet de conserver des machines provisionnées et prêtes à accepter des demandes de connexion des utilisateurs pendant que View Composer actualise, recompose ou rééquilibre les machines dans le pool. Cette valeur doit être inférieure au **Nombre min. de machines** que vous spécifiez si vous provisionnez des machines à la demande. Reportez-vous à la section « Maintien des machines de clone lié provisionnées et prêtes lors des opérations de View Composer », page 86.	
Provisionner des machines à la demande ou 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. ■ **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**. ■ **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.	

Tableau 5-1. Feuille de calcul : options de configuration pour créer un pool de postes de travail de clone lié (suite)

Option	Description	Indiquez votre valeur ici
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. 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. 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. 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. **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.	
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. 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.	

Tableau 5-1. Feuille de calcul : options de configuration pour créer un pool de postes de travail de clone lié (suite)

Option	Description	Indiquez votre valeur ici
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. 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 « Conserver une trace de la taille du fichier d'échange de la machine virtuelle parente », page 56. 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. 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. **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 193.	
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.	
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 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. Pour plus d'informations, reportez-vous à « Stockage de réplicas et de clones liés View Composer sur des magasins de données séparés », page 206. 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.	

Tableau 5-1. Feuille de calcul : options de configuration pour créer un pool de postes de travail de clone lié (suite)

Option	Description	Indiquez votre valeur ici
Machine virtuelle parente	Sélectionnez la machine virtuelle parente du pool. **Remarque** Vous ne pouvez pas utiliser View Composer pour déployer des machines exécutant Windows Vista Édition Intégrale ou Windows XP Professionnel SP1.	
Snapshot (image par défaut)	Sélectionnez le snapshot de la machine virtuelle parente à utiliser comme image de base pour le pool. 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. 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. 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 139.	
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 créer 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. 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 lié », page 197. 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 sur des banques de données locales », page 205. 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 139. Pour plus d'informations sur les disques créés pour des clones liés, reportez-vous à « Disques de données de clone lié », page 204. **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. 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 203. **Remarque** Ce paramètre n'a aucun effet si vous utilisez Virtual SAN.	

Tableau 5-1. Feuille de calcul : options de configuration pour créer 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. Cette fonction est prise en charge sur vSphere 5.0 et supérieur. Cette fonction est activée par défaut. Pour plus d'informations, reportez-vous à « Configurer View Storage Accelerator pour des pools de postes de travail », page 207.	
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. 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. 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. VAAI n'est pas pris en charge sur les machines disposant de la version matérielle virtuelle 9 ou version ultérieure, car les disques du système d'exploitation sont toujours à optimisation d'espace, même lorsque vous désactivez l'opération de récupération d'espace. Cette fonction est prise en charge sur vSphere 5.0 et supérieur. Pour plus d'informations, reportez-vous à « Utilisation de View Composer Array Integration avec la technologie de snapshot NFS natif (VAAI) », page 210.	

Tableau 5-1. Feuille de calcul : options de configuration pour créer un pool de postes de travail de clone lié (suite)

Option	Description	Indiquez votre valeur ici
Récupérer l'espace disque de machine virtuelle	(Disponible uniquement si vous n'utilisez pas Virtual SAN) 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. 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. Pour plus d'informations, reportez-vous à « Récupérer de l'espace disque sur des machines virtuelles de clone lié », page 208.	
Initier la récupération lorsque l'espace inutilisé de la machine virtuelle dépasse :	(Disponible uniquement si vous n'utilisez pas Virtual SAN) 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. 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. Par exemple : **2** Go. 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. 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. Pour plus d'informations, reportez-vous à « Définir des durées d'interruption pour les opérations ESXi sur des machines virtuelles View », page 211.	

Tableau 5-1. Feuille de calcul : options de configuration pour créer 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. 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. 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. 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. Par exemple : **`CN=Computers`** 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. 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. Les comptes d'ordinateur existants doivent être situés dans le conteneur Active Directory que vous spécifiez avec le paramètre **Conteneur Active Directory**. 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. Pour plus d'informations, reportez-vous à « Utiliser des comptes d'ordinateur Active Directory existants pour des clones liés », page 86.	

Tableau 5-1. Feuille de calcul : options de configuration pour créer 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. Sysprep est pris en charge pour les clones liés uniquement sur le logiciel vSphere 4.1 ou supérieur. 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. Pour plus d'informations, reportez-vous à « Choisir QuickPrep ou Sysprep pour personnaliser des machines de clone lié », page 82.	
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. 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. 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 59

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. Consultez le document *Installation de View*.
- Vérifiez que les paramètres de View Composer pour vCenter Server sont configurés dans View Administrator. Consultez le 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. View Agent doit être installé sur la machine virtuelle parente. Reportez-vous à la section Chapitre 3, « Création et préparation de machines virtuelles », page 23.
- 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 67.
- 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 124.
- Si vous prévoyez de fournir un accès à vos applications et postes de travail via Workspace, 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, Workspace ne reconnaîtra pas l'authentificateur SAML que vous configurez dans View et vous ne pourrez pas configurer le pool dans Workspace.

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 141.

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 124.

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 plusieurs sessions par utilisateur		Oui
Supprimer ou actualiser la machine à la fermeture de session		Oui
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

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
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 82.

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 85.

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. 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. 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. Pour plus d'informations, reportez-vous à « Personnalisation de machines de clone lié avec QuickPrep », page 83.	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.
Associe l'ordinateur de clone lié au domaine Active Directory.	Associe l'ordinateur de clone lié au domaine Active Directory. 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.

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

QuickPrep	Spécification de personnalisation (Sysprep)
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. Pour plus d'informations, reportez-vous à « Recomposition de clones liés personnalisés avec Sysprep », page 85.
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 en volume KMS pour activer des machines de clone lié Windows 8, Windows 7 et Windows Vista. Pour plus de détails, 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 84

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 QuickPrep », page 57.

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 et prêtes lors des 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 et prêtes à accepter les demandes de connexion de vos utilisateurs, même lorsque des opérations de maintenance de View Composer sont en cours. Vous pouvez définir un nombre minimal de machines provisionnées et prêtes pendant que View Composer actualise, recompose ou rééquilibre les machines virtuelles de clone lié dans un pool.

Lorsque vous spécifiez **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 prêtes pendant que View Composer exécute l'opération. Vous pouvez spécifier le nombre minimal de machines devant être prêtes lors de la création ou de la modification d'un pool de clones liés.

Les recommandations suivantes s'appliquent à ce paramètre :

- 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 prêtes lors des opérations de View Composer sur une valeur inférieure à la valeur **Nombre min. de machines**. Si le nombre minimal est inférieur, votre pool peut se retrouver avec un nombre total de machines inférieur au nombre minimal de machines que vous voulez maintenir provisionnées et prêtes 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 prêtes. Dans ce cas, les opérations de maintenance de View Composer ne pourraient pas avoir lieu.
- Si vous définissez un nombre minimal important de machines prêtes 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 prêtes 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 prêtes est 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.
- 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.

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

Lorsque vous créez ou modifiez un pool de postes de travail, 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 approvisionnés.

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 un nouveau pool de postes de travail ou modifiez un pool existant. Si vous modifiez un pool 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. 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, reportez-vous au document *Administration de View*.

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

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 que vous 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`**, le provisionnement 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 manuels

6

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.

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. View Agent doit être installé et en cours d'exécution sur chaque machine.

Tableau 6-1. Feuille de calcul : options de configuration pour créer un pool de postes de travail manuel

Option	Description	Indiquez votre valeur ici
Affectation d'utilisateur	Choisissez le type d'affectation d'utilisateur : ■ 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. ■ Dans un pool à attribution flottante, les utilisateurs reçoivent des machines différentes chaque fois qu'ils ouvrent une session. Pour plus d'informations, reportez-vous à « Affectation d'utilisateur dans des pools de postes de travail », page 115.	
vCenter Server	Système vCenter Server qui gère les machines. 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. 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. 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. 3 Installez View Agent sur chaque machine à inclure dans le pool de postes de travail. Pour utiliser PCoIP avec des machines qui sont des machines virtuelles ou des ordinateurs physiques non gérés, vous devez utiliser un matériel Teradici. **Remarque** Lorsque vous activez des postes de travail Windows Server 2008 R2 dans View Administrator, View Administrator affiche toutes les machines Windows Server 2008 R2 disponibles, notamment celles sur lesquelles le Serveur de connexion View et d'autres serveurs View Server sont installés, comme sources de machines potentielles. 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. View 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.	

Tableau 6-1. Feuille de calcul : options de configuration pour créer un pool de postes de travail manuel (suite)

Option	Description	Indiquez votre valeur ici
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. 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.	
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. 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 124. 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 93	

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. View 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 de machines virtuelles », page 23.

  Pour préparer des machines virtuelles et des ordinateurs physiques non gérés, reportez-vous à Chapitre 2, « Préparation de machines non gérées », page 17.

- 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 89.

- 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 124.

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 141.

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. View 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 de machines virtuelles », page 23

  Pour préparer une machine virtuelle ou un ordinateur physique non géré, reportez-vous à Chapitre 2, « Préparation de machines non gérées », page 17

- 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 89.

- 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 124.

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 141.

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 6-2 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 124

Tableau 6-2. 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		

Tableau 6-2. 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
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 plusieurs sessions par utilisateur		Oui		Oui
Protocole d'affichage par défaut	Oui	Oui	Oui Pour utiliser PCoIP avec une machine n'est pas gérée par vCenter Server, vous devez installer le matériel Teradici sur la machine.	Oui 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
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 7

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.

Dans View, un hôte RDS est un serveur disposant du rôle Services Bureau à distance Microsoft, du service Hôte de session Bureau à distance Microsoft et sur lequel View Agent est installé. 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. Lorsque View 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. PCoIP fournit 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.

View 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 8, « Création de batteries de serveurs », page 103.

3 Créez un pool d'applications ou un pool de postes de travail RDS. Reportez-vous à la section Chapitre 9, « Création de pools d'applications », page 107 ou Chapitre 10, « Création de pools de postes de travail RDS », page 111.

4 Autoriser les utilisateurs et les groupes. Reportez-vous à la section Chapitre 12, « Autorisation d'utilisateurs et de groupes », page 141.

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 100.

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 que View affiche automatiquement la liste des applications installées, vous devez installer les applications de manière à ce 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, View 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 SP1

Les services Bureau à distance (RDS) constituent l'un des rôles dont peut disposer Windows Server 2008 R2 Service Pack 1 (SP1). Vous devez installer ce rôle pour configurer un hôte RDS.

Prérequis

- Vérifiez que l'hôte RDS exécute Windows Server 2008 R2 SP1.
- Vérifiez que l'hôte RDS fait partie du domaine Active Directory pour le déploiement de View.
- Installez le correctif cumulatif Microsoft documenté dans http://support.microsoft.com/kb/2775511.

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

Limitez les utilisateurs à une seule session de poste de travail. Reportez-vous à la section « Limiter les utilisateurs à une seule session », page 98.

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 de View.

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

Limitez les utilisateurs à une seule session de poste de travail. Reportez-vous à la section « Limiter les utilisateurs à une seule session », page 98.

Limiter les utilisateurs à une seule session

View 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.

Prérequis

- Installez le rôle des services Bureau à distance (RDS), comme expliqué dans « Installer les services Bureau à distance sur Windows Server 2008 R2 SP1 », page 97 ou « Installer les services Bureau à distance sur Windows Server 2012 ou 2012 R2 », page 97.

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 View Agent sur l'hôte RDS. Reportez-vous à la section « Installer View Agent sur un hôte des services Bureau à distance (Remote Desktop Services, RDS) », page 98.

Installer View Agent sur un hôte des services Bureau à distance (Remote Desktop Services, RDS)

View Agent communique avec le Serveur de connexion View et prend en charge le protocole d'affichage PCoIP. Vous devez installer View 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 SP1 », page 97 ou « Installer les services Bureau à distance sur Windows Server 2012 ou 2012 R2 », page 97.

- Limitez les utilisateurs à une seule session de poste de travail. Reportez-vous à la section « Limiter les utilisateurs à une seule session », page 98.
- Familiarisez-vous avec les options de configuration personnalisée de View Agent. Reportez-vous à la section « Options d'installation personnalisée de View Agent pour un hôte RDS », page 100.
- Téléchargez le fichier du programme d'installation de View Agent sur la page des produits VMware, à l'adresse http://www.vmware.com/products/.

Procédure

1 Connectez-vous en tant qu'administrateur.

2 Pour démarrer le programme d'installation de View 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 les options d'installation personnalisée désirées.

4 Dans la zone de texte **Serveur**, tapez 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 l'hôte RDS dans cette instance du Serveur de connexion View. Après l'inscription, l'instance du Serveur de connexion View spécifiée et toutes les instances supplémentaires incluses dans le même groupe que le Serveur de connexion View peuvent communiquer avec l'hôte RDS.

5 Sélectionnez une méthode d'authentification pour inscrire l'hôte RDS dans l'instance du Serveur de connexion View.

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 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**.

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.

6 Suivez les invites et terminez l'installation.

Suivant

Créez une batterie de serveurs. Reportez-vous à la section Chapitre 8, « Création de batteries de serveurs », page 103.

Options d'installation personnalisée de View Agent pour un hôte RDS

Lorsque vous installez View Agent sur un hôte RDS, vous pouvez sélectionner des options d'installation personnalisée. En outre, View 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.

Tableau 7-1. Option d'installation personnalisée de View Agent pour un hôte RDS

Option	Description
vCenter Operations Manager Agent	Permet à View d'utiliser le produit VMware vCenter Operations Manager pour View.

Tableau 7-2. Fonctionnalités de View 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. 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.
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.
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.

Pour découvrir d'autres fonctionnalités prises en charge sur les hôtes RDS, reportez-vous à « Matrice de prise en charge des fonctionnalités pour View 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 254.

- Vérifiez que les fichiers d'administration ADMX RDS de View sont ajoutés à Active Directory. Reportez-vous à la section « Ajouter les fichiers ADMX des services Bureau à distance à Active Directory », page 237.

- Familiarisez-vous avec les paramètres de stratégie de groupe. Reportez-vous à la section « Paramètres de redirection de ressources et de périphériques RDS », page 240.

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 > Afficher les services RDSH > 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. View 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 254.

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 > Règles > 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 254.

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, View 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 View.

Tableau 7-3. Options de performances désactivées par View

Options de performances désactivées par View
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 View correspondent à quatre paramètres View dans le Registre. Le tableau suivant montre les paramètres View 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 View sur **`false`**.

Tableau 7-4. Paramètres de View associés aux options de performances Windows

Paramètre View	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

Création de batteries de serveurs 8

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 pour servir des groupes d'utilisateurs de taille variable ou ayant différents besoins en termes de postes de travail ou d'applications.

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, View équilibre la charge des sessions de postes de travail RDS et des sessions d'applications entre tous les hôtes RDS de la batterie de serveurs.

- 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 View 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*.

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.

Feuille de calcul pour la création d'une batterie de serveurs

Lorsque vous créez une batterie de serveurs, l'assistant Ajouter une batterie de serveurs vous invite à configurer certaines options.

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 8-1. Feuille de calcul : Options de configuration pour la création d'une batterie de serveurs

Option	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. 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 dans le document *Administration de View*.	
Protocole d'affichage par défaut	Spécifiez **PCOIP** ou **RDP**. Ce paramètre ne s'applique qu'aux pools de postes de travail. Le protocole d'affichage des pools d'applications est toujours **PCoIP**. Si vous sélectionnez **RDP** et que vous prévoyez d'utiliser cette batterie de serveurs pour héberger des pools d'applications, vous devez définir l'option **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**. Cette option ne s'applique qu'aux pools de postes de travail RDS. Si vous sélectionnez **Oui**, vous autorisez les utilisateurs à choisir le protocole d'affichage quand ils se connectent à un poste de travail RDS depuis Horizon Client. La valeur par défaut est **Oui**.	

Tableau 8-1. Feuille de calcul : Options de configuration pour la création d'une batterie de serveurs (suite)

Option	Description	Indiquez votre valeur ici
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**.	

Créer une batterie de serveurs

Vous créez une batterie de serveurs 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 7, « Configuration des hôtes de services Bureau à distance », page 95.
- 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 », page 104.

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 Définissez les paramètres de la batterie de serveurs, puis cliquez sur **Suivant**.

4 Sélectionnez les hôtes RDS à ajouter à la batterie de serveurs, puis cliquez sur **Suivant**.

5 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 9, « Création de pools d'applications », page 107 ou Chapitre 10, « Création de pools de postes de travail RDS », page 111.

Création de pools d'applications 9

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 9.

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.

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 9-1. 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 7, « Configuration des hôtes de services Bureau à distance », page 95.
- Créez une batterie de serveurs qui contient les hôtes RDS. Reportez-vous à la section Chapitre 8, « Création de batteries de serveurs », page 103.
- 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 107.

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 12, « Autorisation d'utilisateurs et de groupes », page 141.

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.

Création de pools de postes de travail RDS 10

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 deux protocoles d'affichage RDP et PCoIP.
- 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.

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 7, « Configuration des hôtes de services Bureau à distance », page 95.
- Créez une batterie de serveurs qui contient les hôtes RDS. Reportez-vous à la section Chapitre 8, « Création de batteries de serveurs », page 103.
- Décidez comment configurer les paramètres du pool. Reportez-vous à la section « Paramètres des pools de postes de travail RDS », page 112.

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 141.

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 124. Les paramètres de pool suivants s'appliquent à un pool de postes de travail RDS.

Tableau 10-1. Paramètres d'un pool de postes de travail RDS

Paramètre	Valeur par défaut
État	Activé
Restrictions du serveur de connexion	Aucune

Tableau 10-1. Paramètres d'un pool de postes de travail RDS (suite)

Paramètre	Valeur par défaut
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 11

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

Vous pouvez configurer un pool de postes de travail afin que les utilisateurs disposent d'attributions dédiées ou flottantes sur les machines du pool. Vous devez choisir une affectation d'utilisateur pour les pools automatisés qui contiennent des machines virtuelles complètes, des pools de clone lié automatisés et des pools manuels.

Avec une attribution dédiée, View attribue à chaque utilisateur autorisé une machine du pool. Lorsqu'un utilisateur se connecte au pool, il ouvre toujours une session sur la même machine. Les paramètres et les données de l'utilisateur sont enregistrés entre les sessions. Aucun autre utilisateur du pool ne peut accéder à la machine.

Avec une attribution flottante, View attribue de manière dynamique les machines du pool aux utilisateurs autorisés. Les utilisateurs se connectent à une machine différente chaque fois qu'ils ouvrent une session. Lorsqu'un utilisateur ferme sa session, la machine est renvoyée au pool.

Vous pouvez configurer des machines à attribution flottante pour qu'elles soient supprimées dès que les utilisateurs ferment leur session. La suppression automatique vous permet de ne conserver que les machines virtuelles dont vous avez besoin en même temps. Vous pouvez uniquement utiliser la suppression automatique dans des pools automatisés que vous provisionnez avec un mode d'attribution de nom de machine et un nombre total de machines.

Les machines à attribution flottante vous permettent de réduire les coûts de licence logicielle.

Dénomination manuelle de machines ou fourniture d'un mode d'attribution de nom

Vous pouvez provisionner les machines dans un pool automatisé en spécifiant manuellement une liste de noms de machines ou en fournissant un mode d'attribution de nom et le nombre de machines que vous voulez dans le pool. Ces deux approches offrent des avantages différents.

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.

Vous devez utiliser l'une de ces méthodes de nommage pour approvisionner des pools automatisés qui contiennent des machines virtuelles complètes ou des clones liés.

Tableau 11-1 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 11-1. Dénomination manuelle de machines ou prestation d'un mode d'attribution de nom

Fonction	Prestation d'un mode d'attribution de nom de machine	Dénomination manuelle de machines
Noms de machines	View génère les noms de machines. Vous fournissez un mode d'attribution de nom. View ajoute un numéro unique pour identifier chaque machine. Pour plus d'informations, reportez-vous à « Utilisation d'un mode d'attribution de nom pour des pools de postes de travail automatisés », page 119.	Vous spécifiez une liste de noms de machines. 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. Pour plus d'informations, reportez-vous à « Spécifier une liste de noms de machines », page 118.
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. Pour plus d'informations, reportez-vous à « Ajouter des machines à un pool automatisé provisionné par une liste de noms », page 121.
Approvisionnement à la demande	Disponible. 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. View peut également créer et provisionner toutes les machines lorsque vous créez le pool.	Non disponible. View crée et provisionne toutes les machines que vous spécifiez dans votre liste lorsque le pool est créé.

Tableau 11-1. Dénomination manuelle de machines ou prestation d'un mode d'attribution de nom (suite)

Fonction	Prestation d'un mode d'attribution de nom de machine	Dénomination manuelle de machines
Personnalisation initiale	Disponible. Lorsqu'une machine est provisionnée, View peut exécuter une spécification de personnalisation que vous sélectionnez.	Disponible. Lorsqu'une machine est provisionnée, View peut exécuter une spécification de personnalisation que vous sélectionnez.
Personnalisation manuelle de machines dédiées	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. 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. Pour plus d'informations, reportez-vous à « Personnalisation manuelle des machines », page 122.
Taille de pool dynamique ou fixe	Dynamique. 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. 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.	Fixe. Le pool contient le nombre de machines que vous indiquez dans la liste de noms de machines. Vous ne pouvez pas sélectionner le paramètre **Supprimer la machine à la fermeture de session** si vous nommez les machines manuellement.
Machines de rechange	Vous pouvez spécifier un nombre de machines de rechange que View maintient sous tension pour les nouveaux utilisateurs. 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. 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.	Vous pouvez spécifier un nombre de machines de rechange que View maintient sous tension pour les nouveaux utilisateurs. View ne crée pas de nouvelles machines de rechange pour conserver le nombre spécifié. 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.	Vous pouvez spécifier des noms de machines pour des pools à attribution dédiée et flottante. **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. Reportez-vous à « 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 11-2. 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 119.

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**

Lorsque View crée une machine, 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 les noms de machines suivants : **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 11-3. 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 118.

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 121.

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 119.

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.

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**.

View ajoute les nouvelles machines au pool.

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 libérer pour les utilisateurs auxquels elles sont attribuées ou les rendre disponibles à tous les utilisateurs autorisés du pool.

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 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 11-4. 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. ■ **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. Lorsque cet état est effectif, les postes de travail distants sont indisponibles.
Restrictions du serveur de connexion	■ **Aucune**. Le pool de postes de travail peut être accédé par n'importe quelle instance du Serveur de connexion View. ■ **Avec balises**. Sélectionnez une ou plusieurs balises Serveur de connexion View pour rendre le pool de postes de travail accessible uniquement aux instances du Serveur de connexion View qui comportent ces balises. Vous pouvez utiliser les cases à cocher pour sélectionner plusieurs balises. Si vous prévoyez de fournir un accès à vos postes de travail via Workspace et si vous configurez des limitations du Serveur de connexion View, il est possible que Workspace App Portal affiche les postes de travail aux utilisateurs alors que ces postes de travail sont en réalité limités. Les utilisateurs de Workspace 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. Pour la description des options de stratégie d'alimentation, reportez-vous à « Règles d'alimentation pour des pools de postes de travail », page 128 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 128
Automatically logoff after disconnect (Fermeture de session automatique après la déconnexion)	■ **Immédiatement**. La session des utilisateurs est fermée dès que ceux-ci se déconnectent. ■ **Jamais**. La session des utilisateurs n'est jamais fermée. ■ **Après**. Durée après laquelle la session des utilisateurs est fermée lorsque ceux-ci se déconnectent. Saisissez la durée en minutes. 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 les utilisateurs à réinitialiser leurs machines	Permet d'autoriser les utilisateurs à réinitialiser leurs propres postes de travail sans assistance administrative.
Autoriser plusieurs sessions par utilisateur	Permet d'autoriser un utilisateur à se connecter simultanément à plusieurs postes de travail du pool.

Tableau 11-4. Descriptions des paramètres de pool de postes de travail (suite)

Paramètre	Options
Supprimer la machine après la fermeture de session	Indiquez si vous souhaitez supprimer les machines virtuelles complètes à attribution flottante. ■ **Non**. Les machines virtuelles restent dans le pool de postes de travail quand les utilisateurs ferment leur session. ■ **Oui**. Les machines virtuelles sont désactivées et supprimées dès que les utilisateurs ferment leur 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. ■ **Jamais**. Les machines virtuelles restent dans le pool et ne sont pas actualisées quand les utilisateurs ferment leur session. ■ **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`. ■ **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.
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. ■ **Jamais**. Le disque du système d'exploitation n'est jamais actualisé. ■ **Toujours**. Le disque du système d'exploitation est actualisé chaque fois que l'utilisateur ferme sa session. ■ **Tous les**. Le disque du système d'exploitation est actualisé à intervalles réguliers sur un nombre spécifié de jours. Saisissez le nombre de jours. 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. ■ **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. 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. 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.
Protocole d'affichage par défaut	Sélectionnez le protocole d'affichage que vous souhaitez que le Serveur de connexion View utilise pour communiquer avec les clients. **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.

Tableau 11-4. Descriptions des paramètres de pool de postes de travail (suite)

Paramètre	Options
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. Pour activer cette fonction, vous devez sélectionner PCoIP comme protocole et désactiver le paramètre **Autoriser les utilisateurs à choisir un protocole** (sélectionnez **Non**). 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 sur des postes de travail Windows 7 ou supérieur », page 134. Si votre déploiement de View n'est pas exécuté sur vSphere 5.0 ou version ultérieure, ce paramètre est indisponible et inactif dans View Administrator. Lorsque vous sélectionnez cette fonctionnalité, vous pouvez configurer la quantité de VRAM attribuée aux machines du pool. Vous pouvez sélectionner un maximum de deux moniteurs pour vos machines qui sont utilisées en tant que postes de travail distants. La valeur **Résolution max. d'un écran** est définie sur 1 920 x 1 200 pixels. Vous ne pouvez pas configurer cette valeur. **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. Pour plus d'informations, reportez-vous à « Configuration du rendu 3D sur des postes de travail Windows 7 ou supérieur », page 134, « Options de rendu 3D », page 135 et à « Meilleures pratiques pour la configuration du rendu 3D », page 136.
Max number of monitors (Nombre max. d'écrans)	Si vous utilisez PCoIP comme protocole d'affichage, vous pouvez sélectionner le **Nombre max. d'écrans** sur lesquels les utilisateurs peuvent afficher le poste de travail. 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. Lorsque le paramètre **Convertisseur 3D** est sélectionné, vous pouvez sélectionner au plus deux écrans. **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.
Max resolution of any one monitor (Résolution max. d'un écran)	Si vous utilisez PCoIP comme protocole d'affichage et si vous ne sélectionnez pas le paramètre **Convertisseur 3D**, vous devez spécifier la **Résolution max. d'un écran**. 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. Lorsque le paramètre **Convertisseur 3D** est sélectionné, vous ne pouvez pas modifier la **Résolution max. d'un écran**. La résolution est définie sur 1 920 x 1 200 pixels. **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.

Tableau 11-4. Descriptions des paramètres de pool de postes de travail (suite)

Paramètre	Options
HTML Access	Sélectionnez **Activé** pour autoriser les utilisateurs à se connecter à des postes de travail distants à partir de leur navigateur Web. Lorsqu'un utilisateur se connecte via la page du portail Web VMware Horizon ou via Workspace App Portal, 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. Pour utiliser HTML Access, vous devez installer HTML Access dans votre déploiement de View. Pour plus d'informations, reportez-vous au document *Utilisation de HTML Access*, disponible sur https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html. Pour utiliser HTML Access avec Workspace, vous devez coupler le Serveur de connexion View à un serveur d'authentification SAML, comme expliqué dans le document *Administration de View*. Workspace 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. ■ **Ne pas contrôler**. La qualité est déterminée par les paramètres de page Web. ■ **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). ■ **Moyenne**. Ce paramètre se traduit par des économies de bande passante modérées. ■ **Élevée**. Ce paramètre se traduit par des économies de bande passante moindres. Pour plus d'informations, reportez-vous à la section « Qualité et limitation d'Adobe Flash », page 127.
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. ■ **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 2500 millisecondes. Ce paramètre correspond au plus grand nombre d'images ignorées. Pour plus d'informations, reportez-vous à la section « Qualité et limitation d'Adobe Flash », page 127.
Remplacer les paramètres globaux 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.
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. 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.

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 11-5 montre les paramètres de qualité du rendu Adobe Flash disponibles.

Tableau 11-5. Paramètres de qualité d'Adobe Flash

Paramètre de qualité	Description
Ne pas contrôler	La qualité est déterminée par les paramètres de page Web.
Faible	Ce paramètre se traduit par les meilleures économies de bande passante.
Moyenne	Ce paramètre se traduit par des économies de bande passante modérées.
Élevée	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 11-6 montre les paramètres de limitation d'Adobe Flash disponibles.

Tableau 11-6. 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 2500 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 règle d'alimentation pour les machines virtuelles d'un pool de postes de travail si les machines virtuelles sont gérées par vCenter Server.

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 11-7 décrit les stratégies d'alimentation disponibles.

Tableau 11-7. 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. ■ View ne modifie pas l'état d'alimentation de la machine virtuelle après la fermeture d'une session par un utilisateur. 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. ■ View n'applique aucun état d'alimentation après l'exécution d'une tâche administrative. 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. 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. 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 131. 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.
Désactiver	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 View 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 11-8 indique à quel moment View applique la stratégie d'alimentation configurée.

Tableau 11-8. 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. **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. 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. **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. 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. 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. **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. 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 131.

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 View 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 11-9 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 11-9. 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 11-10 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 11-10. 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 11-11 décrit le pool automatisé d'affectation dédiée dans cet exemple.

Tableau 11-11. 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 sur des postes de travail Windows 7 ou supérieur

Lorsque vous créez ou modifiez un pool de postes de travail Windows 7 ou supérieur, vous pouvez configurer un rendu graphique 3D pour vos postes de travail. Les postes de travail peuvent tirer parti de vSGA (Virtual Shared Graphics Acceleration) et de vDGA (Virtual Dedicated Graphics Acceleration), fonctionnalités de vSphere qui utilisent des cartes graphiques physiques installées sur les hôtes ESXi et qui gèrent les ressources de processeur graphique entre les machines virtuelles.

Lorsque vous sélectionnez les options basées sur le matériel **Convertisseur 3D**, les utilisateurs peuvent bénéficier d'applications 3D pour la conception, la modélisation et le multimédia, qui exigent généralement du matériel de processeur graphique pour être exécutées correctement. Le paramètre **Convertisseur 3D** offre également une option logicielle qui fournit des améliorations graphiques pouvant prendre en charge des applications moins gourmandes en ressources, telles que Windows AERO, Microsoft Office et Google Earth.

Exigences pour le rendu 3D

Pour activer le rendu graphique 3D matériel ou logiciel, 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 comme protocole d'affichage par défaut
- Les utilisateurs ne doivent pas être autorisés à choisir leur propre protocole

Pour prendre en charge le rendu 3D basé sur le matériel, un pool doit répondre aux exigences supplémentaires suivantes :

- Pour utiliser vSGA, les machines virtuelles doit s'exécuter sur ESXi 5.1 ou des hôtes de version ultérieure, et doivent être gérées par vCenter Server 5.1 ou un logiciel de version ultérieure. Cette fonctionnalité permet à plusieurs machines virtuelles de partager les GPU physiques sur des hôtes ESXi. Vous pouvez utiliser des applications 3D pour la conception, la modélisation et le multimédia.
- Pour utiliser vDGA, les machines virtuelles doivent s'exécuter sur ESXi 5.5 ou des hôtes de version ultérieure, disposer d'un matériel de version 9 ou ultérieure et être gérées par vCenter Server 5.5 ou un logiciel de version ultérieure. Cette fonctionnalité dédie un seul GPU (processeur graphique) physique sur un hôte ESXi à une seule machine virtuelle. Utilisez cette fonctionnalité si vous avez besoin de graphiques de workstation haut de gamme accélérés par le matériel.

  Pour utiliser vDGA, 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.
- 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.

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.

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.

Configuration du rendu 3D

Vous sélectionnez des options pour déterminer la façon dont View gère le rendu 3D. Pour plus d'informations, reportez-vous à « Options de rendu 3D », page 135.

Lorsque vous activez le paramètre **Convertisseur 3D**, vous pouvez configurer la quantité de VRAM attribuée aux machines virtuelles du pool en déplaçant le curseur dans la boîte de dialogue Configurer VRAM pour des invités 3D. La taille VRAM minimale est de 64 Mo. Pour les machines virtuelles avec la version matérielle virtuelle 9, la taille VRAM par défaut est de 96 Mo et vous pouvez configurer une taille maximale de 512 Mo. Pour les machines virtuelles avec la version matérielle virtuelle 8, la taille VRAM par défaut est de 64 Mo et vous pouvez configurer une taille maximale de 128 Mo.

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**.

Lorsque vous activez le paramètre **Convertisseur 3D**, vous pouvez configurer le paramètre **Nombre max. d'écrans** pour un ou deux écrans. Vous ne pouvez pas sélectionner plus de deux écrans. De plus, le paramètre **Résolution max. d'un écran** est défini sur 1 920 x 1 200 pixels.

Options de rendu 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.

Tableau 11-12. 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) pour une machine virtuelle détermine le type de rendu graphique 3D obtenu. View ne contrôle pas le rendu 3D. Dans vSphere Web Client ou vSphere Client, vous pouvez configurer les options **Automatique**, **Logiciel** ou **Matériel**. Ces options ont le même effet que lorsque vous les définissez dans View Administrator. 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 ces paramètres pour une machine virtuelle dans vSphere Web Client ou vSphere Client.
Automatique	Le rendu 3D est activé. L'hôte ESXi contrôle le type de rendu 3D qui a lieu. 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. 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 137.

Tableau 11-12. Options du convertisseur 3D pour les pools exécutés sur vSphere 5.1 ou supérieur (suite)

Option	Description
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. Dans la boîte de dialogue Configurer VRAM pour des clients 3D, vous pouvez utiliser le curseur pour augmenter la quantité de VRAM réservée.
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. 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. IMPORTANT Si vous configurez l'option **Matériel**, tenez compte des contraintes potentielles suivantes : ■ 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. ■ Une machine ne peut pas être déplacée par vMotion vers un hôte ESXi sur lequel le matériel de processeur graphique n'est pas configuré. ■ Pour utiliser vSGA (Virtual Shared Graphics Acceleration), tous les hôtes ESXi du cluster doivent être de version 5.1 ou ultérieure. Si une machine virtuelle est créée sur un hôte ESXi 5.0 dans un cluster mixte, la machine virtuelle n'est pas mise sous tension. ■ Pour utiliser vDGA (Virtual Dedicated Graphics Acceleration), tous les hôtes ESXi du cluster doivent être de version 5.5 ou ultérieure, et les machines virtuelles doivent être de version matérielle 9 ou ultérieure. 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 137.
Désactivé	Le rendu 3D est inactif.

Tableau 11-13. 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. 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.

L'option **Automatique** est le meilleur choix pour les déploiements de View qui exigent le rendu 3D. 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.

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.

Avec l'option **Matériel**, vous devez contrôler strictement votre environnement vSphere :

- Pour vSGA (Virtual Shared Graphics Acceleration), tous les hôtes ESXi doivent être de version 5.1 ou ultérieure et doivent disposer d'une carte de processeur graphique.
- Pour vDGA (Virtual Dedicated Graphics Acceleration), tous les hôtes ESXi doivent être de version 5.5 ou ultérieure et doivent disposer d'une carte de processeur graphique.

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.

Sélectionnez l'option **Gérer à l'aide de vSphere Client** pour prendre en charge une configuration mélangée de rendu 3D et de tailles de VRAM pour les machines virtuelles dans un pool. Dans vSphere Web Client, vous pouvez configurer des machines virtuelles individuelles avec différentes options et valeurs VRAM.

Sélectionnez l'option **Logiciel** si vous ne disposez que 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.

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.
```

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, nommés Services Terminal Server sur les systèmes Windows XP, 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 de View Agent, l'authentification unique et d'autres opérations de gestion des sessions de View.

Prérequis

Vérifiez que le fichier de modèle d'administration (ADM) de configuration de View Agent est installé dans Active Directory. Reportez-vous à la section « Utilisation des fichiers de modèle d'administration de stratégie de groupe View », page 216.

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. b Dans la page Paramètres du pool de postes de travail, sélectionnez **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**. b Dans l'onglet **Paramètres du pool de postes de travail**, sélectionnez **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 > Règles > Modèles d'administration > Modèles d'administration classiques (ADM) > Configuration de VMware View 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 de View.

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.

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.

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, reportez-vous à la section « Attribuer plusieurs étiquettes réseau à un pool de postes de travail » dans le chapitre « Utilisation de View PowerCLI » dans le document *Intégration de View*.

Autorisation d'utilisateurs et de groupes 12

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.

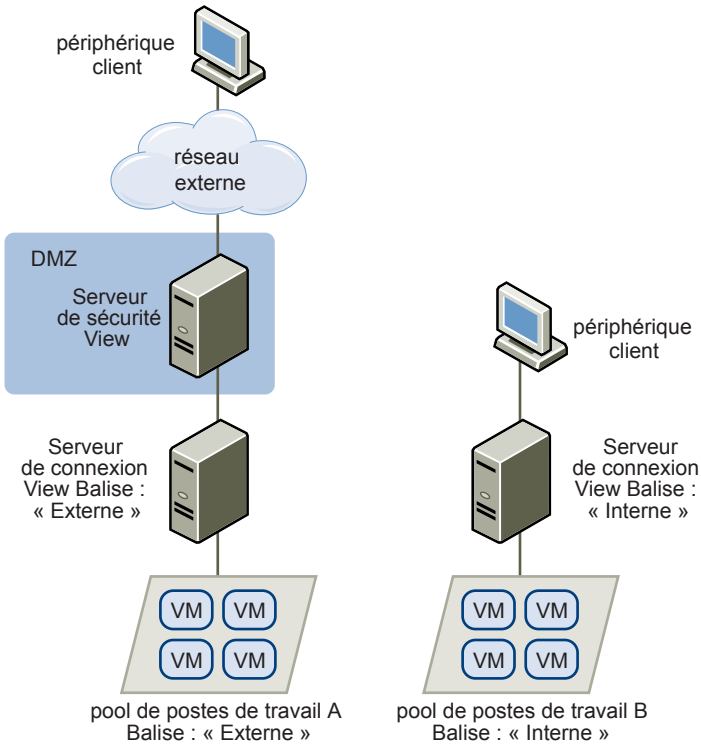
Pour empêcher les utilisateurs externes d'accéder à certains postes de travail, vous pouvez configurer des autorisations limitées comme suit :

- 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 12-1 illustre cette configuration.

Figure 12-1. 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 12-1 montre comment la fonction d'autorisations limitées détermine quand un Serveur de connexion View peut accéder à un pool de postes de travail.

Tableau 12-1. 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 Workspace, et si vous configurez des limitations du Serveur de connexion View, il est possible que Workspace App Portal affiche les postes de travail aux utilisateurs alors que ces postes de travail sont en réalité limités. Lorsqu'un utilisateur Workspace tentera d'ouvrir une session sur un poste de travail, celle-ci ne se lancera 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 13

Certaines fonctionnalités de poste de travail distant qui sont installées avec View 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, Redirection d'URL Flash, Audio/Vidéo en temps réel, Redirection multimédia (MMR) de Windows 7 et Redirection USB.

Pour plus d'informations sur HTML Access, reportez-vous au document *Utilisation de HTML Access*, qui se trouve dans la page Web Documentation de VMware Horizon Client.

Pour plus d'informations sur la Redirection USB, reportez-vous à Chapitre 14, « Utilisation de périphériques USB avec des postes de travail distants », page 173.

Ce chapitre aborde les rubriques suivantes :

Configurer 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 de modèle d'administration pour la configuration de View Agent », page 218.

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 appareils portables sur lesquels il est installé doivent satisfaire 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 View Agent sur une machine virtuelle », page 30.
- Systèmes d'exploitation : Windows XP SP3 (32 bits), Windows Vista (32 bits), Windows 7 (32 ou 64 bits), Windows 8 (32 ou 64 bits), Windows 8.1 (32 ou 64 bits) ou Windows Server 2008 R2

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 de View Agent et distribuer le module aux machines virtuelles
- Exécuter le programme d'installation de View 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 que View 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 de View 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=""a network share to store the admin install package"" UNITY_DEFAULT_APPS=""the list of default favorite apps that should be set in the registry"""
  ```

  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 de View 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=""the list of default favorite apps that should be set in the registry"""
  ```

  Remarque La commande précédente combine l'installation de View Agent à la spécification de la liste d'applications préférées par défaut. Vous n'avez pas à installer View 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 View 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.

Configurer la redirection d'URL flash pour le flux de multidiffusion ou 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 151

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 153

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 153

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 154

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 154

La fonctionnalité Redirection d'URL Flash est activée lorsque vous effectuez une installation silencieuse de View Agent avec l'argument de ligne de commande `FlashURLRedirection`. 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 fonctionnalité Redirection d'URL Flash en tapant l'argument de ligne de commande `FlashURLRedirection` au cours d'une installation silencieuse de View Agent 6.0 ou version ultérieure. Reportez-vous à la section « Propriétés de l'installation silencieuse pour View Agent », page 37.
- 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 154.

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 les instructions d'installation de View Agent, reportez-vous à « Propriétés de l'installation silencieuse pour View Agent », page 37.

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. Vérifiez que le fichier est installé dans le répertoire `/usr/lib` ou `/usr/local/lib`. b Installez le fichier `libflashplayer.so`, ou assurez-vous que ce fichier est déjà installé. Assurez-vous que le fichier est installé dans le répertoire du plug-in Flash approprié de votre système d'exploitation Linux. 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 fonctionnalité Redirection d'URL Flash est activée lorsque vous effectuez une installation silencieuse de View Agent avec l'argument de ligne de commande `FlashURLRedirection`. 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`.

Configurer 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.

Remarque Audio/Vidéo en temps réel installe également une version antérieure de la webcam virtuelle VMware. Vous pouvez voir deux versions de la webcam virtuelle VMware dans certaines applications de conférence. La version antérieure se nomme VMware Virtual Webcam (legacy).

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

Après que vous avez installé View 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 166.

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 157.

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 une 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 View Agent sur une machine virtuelle », page 30.
Logiciel Horizon Client	Horizon Client 2.2 pour Windows ou versions ultérieures Horizon Client 2.2 pour Linux ou version ultérieure. Cette fonctionnalité n'est accessible qu'avec la version d'Horizon Client pour Linux fournie par certains partenaires. Horizon Client 2.3 pour Mac OS X ou versions ultérieures
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. ■ 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 View Agent est installé.
Protocole d'affichage pour View	PCoIP 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 View 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 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 View Agent et spécifier les noms de famille de périphériques `entrée audio` et `vidéo` 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 179.

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 la liste **Connecter un périphérique USB** ou **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

- Assurez-vous qu'un microphone USB ou d'un autre type est installé et opérationnel sur votre système client.
- Assurez-vous que vous utilisez le protocole d'affichage 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.
- Assurez-vous que vous utilisez le protocole d'affichage 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-20YY-MM-DD-XXXXXX.txt`
Windows 7 ou Windows 8	`C:\Users\%username%\AppData\Local\VMware\VDM\Logs\debug-20YY-MM-DD-XXXXXX.txt`

Le format du fichier journal est `debug-20AA-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 161.

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.
- Assurez-vous que vous utilisez le protocole d'affichage 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 13-1. 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.

Tableau 13-1. Syntaxe des commandes de configuration de la fonctionnalité Audio/Vidéo en temps réel (suite)

vdmadmin	Description
`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 la section « Sélectionner un microphone par défaut sur un système client Mac OS X », page 159. 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.
- Assurez-vous que vous utilisez le protocole d'affichage 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) 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 163.

Prérequis

- Assurez-vous qu'un microphone USB ou d'un autre type est installé et opérationnel sur votre système client.
- Assurez-vous que vous utilisez le protocole d'affichage 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.
- Assurez-vous qu'un microphone USB ou d'un autre type est installé et opérationnel sur votre système client.
- Assurez-vous que vous utilisez le protocole d'affichage 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 169.

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 View Agent sur une machine virtuelle », page 30.
- 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 253.
- 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 168.

Procédure

1. Téléchargez le fichier View GPO Bundle `.zip` à partir du site de téléchargement de VMware Horizon (avec View) à l'adresse http://www.vmware.com/go/downloadview.

   Le fichier se nomme `VMware-Horizon-View-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**, cliquez avec le bouton droit sur GPO et sélectionnez **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 **Ajouter/supprimer des 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 de l'ordinateur > Règles > Modèles d'administration > Modèles d'administration classiques > Configuration de VMware View Agent > Configuration de View RTAV**.

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 de View 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. Lorsque ce paramètre n'est pas configuré ou est désactivé, Audio/Vidéo en temps réel est activé. 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. La valeur minimale est d'une image par seconde. La valeur maximale est de 25 images par seconde. 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. 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. 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. 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. 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. 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. 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. 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. 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. Lorsque ce paramètre n'est pas configuré ou est désactivé, la largeur d'image par défaut est de 320 pixels. 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. 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. Lorsque ce paramètre n'est pas configuré ou est désactivé, la hauteur d'image par défaut est de 240 pixels. 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. 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 13-2 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 View 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 13-2. Résultats de l'exemple de bande passante pour envoyer de données Audio/Vidéo en temps réel d' Horizon Client à View 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

Gérer l'accès à la redirection multimédia (MMR) Windows 7

View fournit la fonctionnalité MMR de Windows 7 pour les postes de travail et les clients Windows 7, et la fonctionnalité Wyse MMR pour les postes de travail Windows XP et Windows Vista.

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.

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.

Cette stratégie affecte la fonctionnalité MMR sur des postes de travail Windows 7, Windows XP et Windows Vista.

Pour savoir comment définir des stratégies globales dans View Administrator, reportez-vous à « Règles de View », page 215.

Configuration requise pour la redirection multimédia Windows 7

Pour prendre en charge la redirection multimédia (MMR) Windows 7, le déploiement de votre View doit répondre à certaines exigences matérielles et logicielles.

Poste de travail View	■ Les postes de travail doivent tourner sur des systèmes d'exploitation Windows 7, 64 ou 32 bits. ■ Le **Rendu 3D** doit être activé sur le pool de postes de travail. ■ La version du matériel virtuel des machines virtuelles poste de travail doit être 8 ou plus. ■ Les utilisateurs doivent effectuer la lecture de leurs vidéos avec Windows Media Player 12 ou version ultérieure.
Logiciel Horizon Client	Horizon Client 2.2 pour Windows ou versions ultérieures
Ordinateur Horizon Client ou périphérique d'accès client	■ Les clients doivent tourner sur des systèmes d'exploitation Windows 7 ou Windows 8, 64 ou 32 bits. ■ Les clients doivent disposer de cartes vidéo compatibles DXVA (DirectX Video Acceleration) qui peuvent décoder les vidéos sélectionnées.

- Windows Media Player 12 ou version ultérieure doit être installé sur les clients pour permettre la redirection vers le matériel local.

Formats multimédias pris en charge

Les formats multimédias doivent être conformes à la norme de compression vidéo H.264. Les formats de fichiers M4V, MP4 et MOV sont pris en charge. Vos postes de travail virtuels doivent utiliser l'un de ces formats de fichiers et les décodeurs locaux de ces formats doivent exister sur les systèmes client.

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.

Pour une comparaison du composant de redirection multimédia (MMR) Windows 7 et du composant Wyse MMR qui fonctionne sur les postes de travail Windows XP et Windows Vista, reportez-vous à « Prise en charge de la redirection multimédia par les systèmes d'exploitation des postes de travail », page 171.

Prise en charge de la redirection multimédia par les systèmes d'exploitation des postes de travail

Les composants de redirection multimédia (MMR) Windows 7 et MMR Wyse sont installés avec View Agent. Le composant MMR Wyse fonctionne sous les postes de travail Windows XP et Windows Vista. Quelques caractéristiques et exigences du composant MMR Windows 7 sont légèrement différentes de celles du composant Wyse MMR.

Tableau 13-3. Prise en charge de la redirection multimédia par les systèmes d'exploitation des postes de travail View

Système d'exploitation de poste de travail	Exigences de machine virtuelle	Formats multimédias pris en charge	Clients pris en charge	Redirection audio
Windows XP, Windows Vista	Windows Media Player 10 ou une version ultérieure doit être installée.	Plusieurs formats sont pris en charge. Par exemple : MPEG2-1 ; MPEG2 ; MPEG-4 Part 2 ; WMV 7, 8 et 9 ; WMA ; AVI ; ACE ; MPT3 ; WAV	Windows XP, Windows Vista, Windows 7 Windows Media Player 10 ou une version ultérieure doit être installée.	Le flux audio est redirigé vers le système client.
Windows 7	La version du matériel virtuel des postes de travail doit être 8 ou plus. Le **Rendu 3D** doit être activé. Windows Media Player 12 ou une version ultérieure doit être installée.	Compression H.264 standard dans les formats M4V, MP4 ou MOV.	Windows 7, Windows 8 Les clients doivent disposer de cartes vidéo compatibles DXVA (DirectX Video Acceleration) qui peuvent décoder les vidéos sélectionnées. Windows Media Player 12 ou une version ultérieure doit être installée.	Le flux audio n'est pas redirigé. L'audio est livré sur PCoIP à partir du poste de travail distant au système client.
Windows 8	Non pris en charge	Non pris en charge	Non pris en charge	Non pris en charge

Pour plus d'informations sur la configuration système requise de MMR sur les périphériques Horizon Client, reportez-vous au document *Utilisation de VMware Horizon Client pour Windows*.

Vérifier que les clients peuvent lancer Windows 7 MMR

Windows 7 MMR utilise l'établissement d'une liaison entre le système Horizon Client et le poste de travail pour valider les demandes de redirection multimédia. Lorsque certaines conditions réseau sont réunies, cet établissement de liaison peut prendre du temps, ce qui empêche le lancement de la fonction MMR. Pour garantir que Windows 7 MMR puisse être lancé, vous pouvez configurer une clé de registre Windows sur le poste de travail afin d'augmenter le délai accordé pour l'établissement de liaison de validation.

La clé de registre Windows contrôle la valeur TTL (Time to Live) de l'établissement de liaison, définie en millisecondes. La clé est au format REG_DWORD (hex). La valeur par défaut est de 5 000 millisecondes (cinq secondes).

Avant de déployer Windows 7 MMR pour les utilisateurs d'View, testez quelques systèmes clients pour vérifier si le délai par défaut accordé pour effectuer l'établissement de liaison est adapté à votre environnement. Si vos conditions réseau exigent un délai d'établissement de liaison supérieur à cinq secondes, augmentez la valeur TTL.

Procédure

1 Lancez l'éditeur du Registre Windows sur le poste de travail distant.

2 Accédez à la clé de registre de Windows qui contrôle l'établissement de liaison de validation MMR.

Option	Description
Windows 7 64 bits	`HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware,Inc.\VMware VDPService\handshakeTTL`
Windows 7 32 bits	`HKEY_LOCAL_MACHINE\Software\VMware,Inc.\VMware VDPService\handshakeTTL`

3 Augmentez la valeur `handshakeTTL` en indiquant un nombre supérieur à 5 000.

4 Redémarrez Windows Media Player sur le poste de travail pour que la valeur mise à jour entre en vigueur.

Utilisation de périphériques USB avec des postes de travail distants

14

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 de RDP ou du protocole d'affichage PCoIP. Un poste de travail distant peut recevoir jusqu'à 32 périphériques USB.

Lorsque vous utilisez cette fonctionnalité, la plupart des périphériques USB associés 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 poste de travail distant. Seuls quelques types de périphériques USB peuvent être partagés entre le 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 fonctionnalité Redirection USB est disponible dans les pools de postes de travail qui sont déployés sur des machines mono-utilisateur. Elle n'est pas disponible dans des pools de postes de travail RDS.

Remarque 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.

Ce chapitre aborde les rubriques suivantes :

- « Utilisation de règles pour contrôler la redirection USB », page 179
- « Résolution de problèmes de redirection USB », page 189

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, ainsi qu'avec Horizon Client 3.1 ou version ultérieure, vous pouvez connecter des périphériques USB 3.0 à des ports USB 3.0 sur la machine cliente. Les périphériques USB 3.0 sont pris en charge uniquement avec un flux simple. Comme la prise en charge multi-flux n'est pas mise en œuvre dans cette version, les performances du périphérique 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 peuvent ne pas être adaptés à la redirection USB vers un poste de travail distant :

- 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.
- 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 même, des lecteurs et graveurs de CD/DVD USB, qui nécessitent une vitesse de transmission stable des données pour que l'opération de gravure s'effectue correctement, ainsi que des scanners et des périphériques tactiles tels que les tablettes de signature, ne fonctionnent pas correctement sur un réseau latent de type réseau étendu.
- La redirection de scanners USB dépend de l'état du réseau, et les numérisations peuvent être anormalement longues.

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 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.

Remarque 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.

---

1 Lors de l'exécution de l'assistant d'installation de View Agent sur la source du poste de travail distant, veillez à inclure le composant Redirection USB.

   Ce composant est inclus par défaut. VMware recommande de toujours inclure ce composant. 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.

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 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 de View 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 179.

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 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 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, 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 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, 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 un poste de travail distant. La connexion est établie par tunnel à l'aide du port HTTPS 443 avec le serveur de sécurité, puis les connexions ultérieures pour le trafic USB entre le serveur et le poste de travail distant utilisent le port TCP 32111. Les performances du périphérique USB sont légèrement dégradées lorsque la connexion par tunnel est employée.

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 182.

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*.

Désactivation de la redirection USB

Certaines applications sensibles à la sécurité nécessitent que la redirection USB soit désactivée. 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 :

- Dans View Administrator, modifiez la stratégie **Accès USB** pour qu'un pool spécifique autorise ou refuse son accès.
- Dans View Administrator, après avoir défini la stratégie au niveau du pool de postes de travail, vous pouvez remplacer la stratégie pour une machine virtuelle spécifique du pool.
- Lors de l'installation de View Agent, désélectionnez le composant **Redirection USB**. VMware ne recommande pas cette stratégie, car elle offre moins de flexibilité que l'utilisation des paramètres de la stratégie.
- Définissez la stratégie `Exclure tous les périphériques` sur **`true`**, du côté agent ou du côté client, selon le cas.

Si vous définissez la stratégie `Exclure tous les périphériques` sur **`true`**, Horizon Client empêche la redirection de tous les périphériques USB. Vous pouvez utiliser d'autres paramètres de règle pour autoriser la redirection de périphériques spécifiques ou de familles de périphériques. Si vous définissez la stratégie sur **`false`**, Horizon Client autorise la redirection de tous les périphériques USB sauf ceux qui sont bloqués par d'autres paramètres de stratégie. Vous pouvez définir la stratégie dans View Agent et Horizon Client. Le tableau suivant décrit comment la stratégie `Exclure tous les périphériques` que vous pouvez définir pour View Agent et Horizon Client se combinent pour produire une stratégie efficace pour l'ordinateur client. Par défaut, tous les périphériques USB sont autorisés à être redirigés, sauf blocage contraire.

Tableau 14-1. Effet de la combinaison de règles Exclure tous les périphériques

Règle Exclure tous les périphériques sur View Agent	Stratégie Exclure tous les périphériques dans Horizon Client	Règle Exclure tous les périphériques effective combinée
`false` ou non défini (inclure tous les périphériques USB)	**`false`** ou non défini (inclure tous les périphériques USB)	Inclure tous les périphériques USB
`false` (inclure tous les périphériques USB)	**`true`** (exclure tous les périphériques USB)	Exclure tous les périphériques USB
`true` (exclure tous les périphériques USB)	Aucun ou non défini	Exclure tous les périphériques USB

Si vous avez défini la stratégie `Désactiver le téléchargement d'une configuration distante` sur **`true`**, la valeur d'`Exclure tous les périphériques` dans View Agent n'est pas transmise à Horizon Client, mais View Agent et Horizon Client appliquent la valeur locale d'`Exclure tous les périphériques`.

Ces stratégies sont incluses dans le fichier de modèle d'administration de configuration de View Agent (`vdm_agent.adm`). Pour plus d'informations, reportez-vous à la section « Paramètres USB du modèle d'administration de configuration de View Agent », page 186.

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. 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 14-2. Emplacements des fichiers journaux

Client ou Agent	Chemin d'accès aux fichiers journaux
Client Windows	`%PROGRAMDATA%\VMware\VDM\logs\debug-*.txt` `C:\Windows\Temp\vmware-SYSTEM\vmware-usbarb-*.log`
Agent Windows (sur un poste de travail distant)	`%PROGRAMDATA%\VMware\VDM\logs\debug-*.txt`
Client Mac OS X	`/var/root/Library/Logs/VMware/vmware-view-usbd-xxxx.log` `/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 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 le poste de travail distant (View 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 la disposition de la redirection, et pour que View Agent empêche le transfert de certains périphériques USB à partir d'un ordinateur client.

Si d'anciennes versions de View Agent ou d'Horizon Client sont installées, certaines fonctionnalités des stratégies de redirection USB ne sont pas disponibles. Tableau 14-3 explique comment View applique les stratégies pour différentes combinaisons de View Agent et d'Horizon Client.

Tableau 14-3. Compatibilité des paramètres de stratégie USB

Version de View 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 View Agent et à Horizon Client. Vous pouvez utiliser les paramètres de stratégie USB de View Agent pour empêcher le transfert de périphériques USB vers un poste de travail. View 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.
5.1 ou version ultérieure	5.0.x ou version antérieure	Les paramètres de stratégie USB s'appliquent uniquement à View Agent. Vous pouvez utiliser les paramètres de stratégie USB de View 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 de View Agent. Les paramètres de Registre existants pour la redirection USB par Horizon Client demeurent valides.
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 de View Agent pour empêcher le transfert des périphériques USB vers un poste de travail. View 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 View 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 `Autoriser le fractionnement automatique de périphérique` détermine si Horizon Client tente de fractionner automatiquement des périphériques USB composites. Par défaut, le fractionnement automatique est désactivé.

Tableau 14-4. Effet de la combinaison de règles de désactivation du fractionnement automatique

Règle Autoriser le fractionnement automatique de périphérique sur View 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
`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 de View Agent (`vdm_agent.adm`). Pour plus d'informations, reportez-vous à la section « Paramètres USB du modèle d'administration de configuration de View Agent », page 186.

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 14-5 indique les modificateurs définissant la façon dont Horizon Client gère un paramètre de stratégie de fractionnement de périphérique View 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 14-5. Modificateurs de fractionnement pour des paramètres de règle de fractionnement de périphérique sur View Agent

Modificateur	Description
m (fusionner)	Horizon Client applique le paramètre de stratégie de fractionnement de périphérique View Agent en plus du paramètre de stratégie de fractionnement de périphérique Horizon Client.
o (remplacer)	Horizon Client applique le paramètre de stratégie de fractionnement de périphérique View Agent à la place du paramètre de stratégie de fractionnement de périphérique Horizon Client.

Tableau 14-6 montre des exemples de la façon dont Horizon Client traite les paramètres de stratégie `Exclure le périphérique du fractionnement ID de fournisseur/de produit` lorsque vous spécifiez différents modificateurs de fractionnement.

Tableau 14-6. 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/produit sur View 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**

View Agent n'applique pas les paramètres de règle 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 View Agent, définissez la stratégie `Autoriser le fractionnement automatique de périphérique` sur `Autoriser – Remplacer le paramètre du client`.
- Pour View 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 View Agent, définissez la stratégie `Autoriser le fractionnement automatique de périphérique` sur `Autoriser – Remplacer le paramètre du client`.
- 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 View Agent et Horizon Client déterminent les périphériques USB pouvant être redirigés d'un ordinateur client vers 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, Horizon Client télécharge les paramètres de stratégie USB de View Agent et les utilise conjointement aux 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 de View Agent (`vdm_agent.adm`). Pour plus d'informations, reportez-vous à la section « Paramètres USB du modèle d'administration de configuration de View Agent », page 186.

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 View Agent pour un paramètre applicable par l'agent, s'il existe un paramètre de stratégie de filtre équivalent pour Horizon Client.

Tableau 14-7. Modificateurs de filtre pour des paramètres exécutables par un agent

Modificateur	Description
m (fusionner)	Horizon Client applique le paramètre de stratégie de filtre View Agent en plus du paramètre de stratégie de filtre 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 `Exclure tous les périphériques`. Si la stratégie `Exclure tous les périphériques` est définie du côté de l'agent, elle remplace le paramètre du client.
o (remplacer)	Horizon Client utilise le paramètre de stratégie de filtre View 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 en guise de 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 View Agent pour un paramètre interprété par le client.

Tableau 14-8. 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 Horizon Client, Horizon Client utilise le paramètre de stratégie de filtre View Agent. S'il existe un paramètre de stratégie de filtre Horizon Client, Horizon Client applique celui-ci et ignore celui de View Agent.
`Override` (**o** dans le paramètre de registre)	Horizon Client utilise le paramètre de stratégie de filtre View Agent à la place d'un paramètre de stratégie de filtre Horizon Client équivalent.

View Agent n'applique pas les paramètres de règle 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 `Autoriser les cartes à puce` lorsque vous spécifiez différents modificateurs de filtre.

Tableau 14-9. Exemples d'application de modificateurs de filtre sur des paramètres interprétés par un client

Paramètre Autoriser les cartes à puce sur View 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 `Désactiver le téléchargement d'une configuration distante` sur la valeur **`true`**, Horizon Client ignore les paramètres de stratégie de filtre qu'il reçoit de View Agent.

View 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 de View Agent. Horizon Client ne signale pas que View 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 `Exclure tous les périphériques` sur **`true`**. Toutefois, si vous avez configuré un paramètre de règle de filtre sur View Agent afin d'exclure le périphérique, le poste de travail bloque toute tentative de redirection du périphérique sur 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 de View Agent, ainsi que des valeurs de modificateur que vous appliquez aux paramètres de View 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 `Exclure le chemin d'accès` et `Inclure le chemin d'accès` 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 View Agent, celui-ci évalue et applique les paramètres de stratégie de filtre dans l'ordre de priorité suivant sur 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

View 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 View 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, View Agent bloque celui-ci si vous configurez une stratégie pour que View 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 178.

- 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 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.

Remarque Certains périphériques ne lisent pas certaines familles de périphériques.

Tableau 14-10. 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.
`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 de View Agent

Vous pouvez définir des paramètres de stratégie USB pour View Agent et Horizon Client. Lors de la connexion, Horizon Client télécharge les paramètres de stratégie USB depuis View Agent et les utilise avec les paramètres de stratégie USB de 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 de View Agent (`vdm_agent.adm`) contient des paramètres de stratégie liés aux composants d'authentification et d'environnement de View Agent, notamment la redirection USB. Les paramètres s'appliquent au niveau de l'ordinateur. De préférence, View Agent lit les paramètres depuis le GPO au niveau de l'ordinateur. Sinon, il les lit depuis le 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 stratégie pour le fractionnement de périphériques USB composites dans le fichier de modèle d'administration pour la configuration de View Agent. View Agent n'applique pas ces paramètres. View 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 180.

Tableau 14-11. Modèle pour la configuration de View Agent : paramètres de fractionnement de périphérique

Paramètre	Propriétés
`Allow Auto Device Splitting` Propriété : `AllowAutoDeviceSplitting`	Autorise le fractionnement automatique de périphériques USB composites. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
`Exclude Vid/Pid Device From Split` 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*]... Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (**`*`**) à la place de chiffres dans un ID. Par exemple : **`o:vid-0781_pid-55**`** La valeur par défaut n'est pas définie.
`Split Vid/Pid Device` 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 {`m`|`o`}`:vid-`*xxxx*`_pid-`*yyyy*`(exintf:`*zz*[`;exintf:`*ww*]) ou {`m`|`o`}`:vid-`*xxxx*`_pid-`*yyyy*`(exintf:`*zz*[`;exintf:`*ww*]) 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. Par exemple : **`o:vid-0781_pid-554c(exintf:01;exintf:02)`** **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. La valeur par défaut n'est pas définie.

Paramètres USB appliqués par View 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 de View Agent. View Agent utilise les paramètres pour décider si un périphérique USB peut être transmis à la machine hôte. View 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 View 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 182.

Tableau 14-12. Modèle pour la configuration de View Agent : paramètres appliqués par un agent

Paramètre	Propriétés
`Exclude All Devices` 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. 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. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
`Exclude Device Family` Propriété : `ExcludeFamily`	Exclut des familles de périphériques de la transmission. Le format du paramètre est {`m`|`o`}`:`*family_name_1*[`;`*family_name_2*]... Par exemple : **`o:bluetooth;smart-card`** 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. La valeur par défaut n'est pas définie.
`Exclude Vid/Pid Device` 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*]... Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (`*`) à la place de chiffres dans un ID. Par exemple : **`m:vid-0781_pid-****;vid-0561_pid-554c`** La valeur par défaut n'est pas définie.
`Include Device Family` Propriété : `IncludeFamily`	Inclut des familles de périphériques pouvant être transmises. Le format du paramètre est {`m`|`o`}`:`*family_name_1*[`;`*family_name_2*]... Par exemple : **`m:storage`** La valeur par défaut n'est pas définie.
`Include Vid/Pid Device` 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*]... Vous devez spécifier des numéros d'ID au format hexadécimal. Vous pouvez utiliser le caractère générique (`*`) à la place de chiffres dans un ID. Par exemple : **`o:vid-0561_pid-554c`** 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 de View Agent. View Agent n'applique pas ces paramètres. View 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 14-13. Modèle pour la configuration de View Agent : paramètres interprétés par un client

Paramètre	Propriétés
`Allow Audio Input Devices` Propriété : `AllowAudioIn`	Permet la transmission de périphériques d'entrée audio. La valeur par défaut est indéfinie, ce qui correspond à **`true`**.
`Allow Audio Output Devices` Propriété : `AllowAudioOut`	Permet la transmission de périphériques de sortie audio. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.

Tableau 14-13. Modèle pour la configuration de View Agent : paramètres interprétés par un client (suite)

Paramètre	Propriétés
`Allow HIDBootable` 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). 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. La valeur par défaut n'est pas définie.
`Allow Keyboard and Mouse Devices` Propriété : `AllowKeyboardMouse`	Permet la transmission de claviers avec périphériques de pointage intégrés (souris, Trackball ou pavé tactile). La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
`Allow Smart Cards` Propriété : `AllowSmartcard`	Permet la transmission de périphériques à carte à puce. La valeur par défaut est indéfinie, ce qui correspond à **`false`**.
`Allow Video Devices` Propriété : `AllowVideo`	Permet la transmission de périphériques vidéo. 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 180.
- La redirection USB n'est pas prise en charge pour les systèmes Windows 2008 ou pour les postes de travail distants sur hôtes de session Bureau à distance.
- 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 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 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 http://kb.vmware.com/kb/1011600.
- Windows Mobile Device Center peut empêcher la redirection de périphériques USB pour des sessions RDP. Reportez-vous à 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 http://kb.vmware.com/kb/1022076.
- Pour certains périphériques audio, vous devrez éventuellement modifier les paramètres de règle ou de Registre. Reportez-vous à 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 http://kb.vmware.com/kb/1022836.
- Un processus ou un service sur le système local a ouvert le périphérique avant votre connexion au poste de travail distant.
- Un périphérique USB redirigé arrête de fonctionner si vous reconnectez une session de poste de travail, même si le poste de travail 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 de poste de travail.
- 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 178.
- 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 15

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 View Composer augmente les économies de stockage, car toutes les machines virtuelles d'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 4.1 ou version ultérieure

Avec vSphere 4.1 ou version ultérieure, vous pouvez désormais utiliser également les fonctionnalités suivantes :

- vStorage Thin Provisioning, qui vous permet de commencer avec une quantité d'espace disque minimale nécessaire et d'agrandir le disque pour ajouter de l'espace ultérieurement ;
- Le stockage étagé qui vous permet de distribuer des disques virtuels dans l'environnement View sur des niveaux de stockage haute performance et de stockage à coûts réduits, afin d'optimiser les performances et de réduire les coûts ;
- Le stockage local sur l'hôte ESXi pour les fichiers d'échange de la machine virtuelle dans le système d'exploitation invité.

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 32 hôtes ESXi.

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.

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, 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 les pools de postes de travail de clone lié ou les pools de postes de travail de clone complet.

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.

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, consultez le document *Stockage vSphere*.
2. Lors de la création d'un pool de postes de travail dans View Administrator, sous **Gestion des stratégies de stockage**, sélectionnez **Utiliser vSphere Virtual SAN**, et sélectionnez la banque de données Virtual SAN à utiliser.

   Après la sélection de **Utiliser vSphere 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 tous les pools de poste de travail, 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.
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.

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*.

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.

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.

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 exigences de Virtual SAN, reportez-vous à « Utilisation de Virtual SAN » dans le document *Stockage de vSphere*.

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 du 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. Ces stratégies sont créées à la fois pour les pools de postes de travail de clone lié et les pools de postes de travail de clone complet.

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.

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, un clone complet est d'abord créé depuis 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 clones liés d'un LUN à un autre ou des clones liés à une banque de données Virtual SAN ou d'une banque de données Virtual SAN à 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, vous ne pouvez pas sélectionner manuellement différentes banques de données pour les réplicas ou clones liés. 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.

Disques supprimables pour fichiers d'échange et temporaires

Lorsque vous créez un pool de clone lié, vous pouvez également configurer de façon facultative un disque virtuel supprimable séparé pour stocker les fichiers d'échange et temporaires du système d'exploitation client 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.

Banques de données Virtual SAN pouvant agréger les disques de stockage locaux à partir d'un cluster vSphere

Virtual SAN virtualise les disques de stockage physiques et locaux disponibles sur les hôtes ESXi dans une seule banque de données partagée par tous les hôtes dans un cluster vSphere. Une banque de données Virtual SAN se compose de disques à circuit intégré (SSD) et de disques durs, aussi appelés disques de données. Les disques SSD sont utilisés pour la mise en cache des lectures et pour la mise en mémoire tampon des écritures. Les disques de données sont utilisés pour le stockage persistant. Cette stratégie fournit un stockage haute performance avec mise en cache automatique, de sorte que vous spécifiez uniquement une banque de données lors de la création d'un pool de postes de travail, et les différents composants, comme les fichiers, réplicas, données utilisateur et fichiers de système d'exploitation de la machine virtuelle sont placés sur les disques SSD ou de données appropriés.

Remarque La fonctionnalité Virtual SAN nécessite vSphere 5.5 Update 1 ou version ultérieure, ainsi que le matériel adapté. Reportez-vous au Guide de comptabilité VMware.

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. Virtual SAN présente le disque virtuel dans la banque de données logique pour satisfaire aux exigences spécifiées. Virtual SAN contrôle également la conformité de la stratégie pendant le cycle de vie de la machine virtuelle et génère des rapports sur cet aspect. 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.

Remarque Lorsque vous créez un pool de postes de travail de clone lié, un clone complet est d'abord créé depuis la machine virtuelle parente. C'est à partir de ce clone ou réplica que les clones liés sont créés. Si vous utilisez une banque de données Virtual SAN, une copie supplémentaire du réplica et des clones liés sera créée par défaut conformément à la stratégie de disponibilité.

Dimensionnement du stockage pour des pools de postes de travail de clone lié

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 lié. Un tableau dans l'assistant Ajouter un pool de postes de travail montre une estimation générale des exigences de stockage des disques de clone lié lors de la création du pool et en fonction de la croissance des clones liés.

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 et de réplicas. Vous pouvez décider des magasins de données à utiliser en comparant l'espace libre réel et les exigences estimées pour les disques de clone lié.

Les formules que View utilise ne peuvent fournir qu'une estimation générale de l'utilisation du stockage. La croissance de stockage réelle de vos clones liés dépend de nombreux facteurs :

- Quantité de mémoire affectée à la machine virtuelle parente
- Fréquence des opérations d'actualisation
- Taille du fichier d'échange du système d'exploitation client
- Si vous redirigez des fichiers temporaires et d'échange vers un disque séparé
- Si vous configurez des disques persistants de View Composer séparés
- Charge de travail sur les machines de clone lié, 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 liés, configurez vos pools de clones liés pour que des ensembles particuliers de banques 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 des disques du système d'exploitation de clone lié 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 banques de données dans de grands déploiements, reportez-vous au document *Planification de l'architecture de View*.

Recommandations sur le dimensionnement des pools de clone lié

Lorsque vous créez ou modifiez un pool de postes de travail de clone lié, la page Sélectionner des banques de données de clone lié 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 des disques de clone lié

Tableau 15-1 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.

Tableau 15-1. Exemple de tableau de dimensionnement des disques de clone lié

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 de clone lié atteignent 50 % de la machine virtuelle parente.

La colonne **Max. recommandé** montre le stockage recommandé lorsque des disques de clone lié 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** 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 sur le dimensionnement

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 le pool de clone lié.

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 liés. 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 liés que vous ajoutez au pool.

Par exemple, si vous ajoutez 100 clones liés 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 une nouvelle banque de données, mais que vous conservez la même taille de pool de postes de travail ou que vous diminuez le nombre de clones liés, les recommandations de dimensionnement indiquent 0. Les valeurs égales à 0 indiquent qu'aucun nouveau clone ne doit être créé dans la banque de données sélectionnée. 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 liés 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 des pools de clone lié », page 200.

Recommandations sur le dimensionnement et surcharge de 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 203.

Formules de dimensionnement des pools de clone lié

Des formules de dimensionnement du stockage peuvent vous aider à estimer la taille de disques de clone lié relative à l'espace libre sur les magasins de données que vous sélectionnez pour les disques du système d'exploitation, les disques persistants de View Composer et les réplicas.

Formules de dimensionnement du stockage

Tableau 15-2 présente les formules qui calculent les estimations de taille des disques de clone lié lorsque vous créez un pool et au fur et à mesure que les machines de clone lié 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 liés lorsque vous modifiez un pool ou stockez des réplicas sur un magasin de données séparé », page 201.

Tableau 15-2. Formules de dimensionnement du stockage des disques de clone lié 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 de clones liés 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 15-3 indique comment les formules de dimensionnement calculent l'estimation des exigences de stockage pour l'exemple de pool de postes de travail de clone lié.

Tableau 15-3. Exemple d'estimation de dimensionnement des disques de clone lié 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 liés lorsque vous modifiez un pool ou stockez des réplicas sur un magasin de données séparé

View calcule différentes formules de dimensionnement lorsque vous modifiez un pool de postes de travail de clone lié existant ou lorsque vous stockez des réplicas dans une banque de données distincte, et non lorsque 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 de clone lié.

Dans ces cas-là, View n'inclut pas d'espace pour les réplicas lorsqu'il calcule des recommandations de stockage pour des disques de clone lié.

Tableau 15-4 montre les formules qui calculent les tailles estimées de disques de clone lié lorsque vous modifiez un pool ou stockez des réplicas sur un magasin de données séparé.

Tableau 15-4. Formules de dimensionnement du stockage des disques de clone lié 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 de clones liés 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 15-5 montre comment les formules de dimensionnement calculent des exigences de stockage estimées pour le pool de clone lié en exemple.

Tableau 15-5. Exemple d'estimation de dimensionnement des disques de clone lié 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

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.

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 approvisionnant de façon trop conservatrice ou éviter de risquer que les clones liés n'aient plus d'espace disque et provoquent l'échec de leurs applications de poste de travail.

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 15-6 montre les niveaux de surcharge de stockage que vous pouvez définir.

Tableau 15-6. 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.

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 ne fonctionne qu'avec des pools de clone lié.

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 », page 202.

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**. 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**. 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 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, 3 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 sur des banques de données locales

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 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 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 que vous configurez.

Pour configurer un grand pool de postes de travail, 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 liés View Composer sur des magasins de données séparés

Vous pouvez placer des réplicas et des clones liés View Composer sur des magasins de données séparés avec différentes caractéristiques de performance. Cette configuration flexible peut accélérer les opérations intensives telles que l'approvisionnement de plusieurs clones liés à la fois ou l'exécution d'une analyse antivirus.

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). Étant donné que View Composer ne crée qu'un seul réplica pour chaque snapshot d'image de base View Composer sur chaque cluster ESXi, les réplicas ne nécessitent pas un grande quantité d'espace de stockage. Un disque électronique peut augmenter la vitesse à laquelle ESXi lit le disque du système d'exploitation d'un réplica lors de l'exécution simultanée d'une tâche sur plusieurs clones liés.

Vous pouvez stocker des clones liés 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 pour le stockage des nombreux clones liés d'un pool volumineux. ESXi n'a pas besoin d'effectuer des opérations de lecture simultanées et intensives sur un clone lié.

La configuration de réplicas et de clones liés de cette façon peut réduire l'impact des tempêtes d'E/S qui se produisent quand de nombreux clones liés sont créés à la fois. 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 liés d'un pool sur des magasins de données séparés :

- Vous ne pouvez spécifier qu'un magasin de données réplica séparé pour chaque pool.
- Si une banque de données réplica est partagée, elle doit être accessible à partir de tous les hôtes ESXi du cluster.
- Si les magasins de données de clone lié sont partagés, le magasin de données réplica doit être partagé. Le réplica ne peut pas résider sur une banque de données locale.

  Si les banques de données de clones liés sont locales, VMware vous recommande vivement 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.

  REMARQUE Cette limitation ne s'applique pas si vous utilisez des banques de données Virtual SAN qui agrègent des disques de stockage locaux sur tous les hôtes ESXi du cluster. Avec les banques de données Virtual SAN, le stockage est à la fois local et partagé.

Considérations sur la disponibilité pour le stockage de réplicas sur un magasin de données séparé ou des magasins de données partagés

Vous pouvez stocker des réplicas View Composer sur un magasin de données séparé ou sur les mêmes magasins de données que des machines virtuelles de clone lié. Ces configurations affectent la disponibilité du pool de différentes façons.

Lorsque vous stockez des réplicas sur les mêmes magasins de données que les clones liés, View Composer crée un réplica séparé sur chaque magasin de données pour améliorer la disponibilité. Si un magasin de données devient indisponible, seuls les clones liés sur ce magasin de données sont affectés. Les clones liés sur d'autres magasins de données sont toujours exécutés.

Lorsque vous stockez des réplicas sur un magasin de données séparé, tous les clones liés 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 des machines virtuelles de clone lié, vous pouvez configurer une solution haute disponiblité pour la banque de données sur laquelle vous stockez les réplicas.

Configurer View Storage Accelerator pour des pools de postes de travail

Vous pouvez configurer des pools de postes de travail 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.

View Storage Accelerator est activé pour un pool par défaut. Vous pouvez activer ou désactiver View Storage Accelerator lorsque vous créez ou modifiez un pool.

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.

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.

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 s'est vu affecter le privilège **Général > Agir comme vCenter Server** 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. Consultez le document *Administration de View*.

Procédure

1 Dans View Administrator, affichez la page Options de stockage avancées.

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**, puis cliquez sur l'onglet **Stockage avancé**. 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 des durées d'interruption pour les opérations ESXi sur des machines virtuelles View », page 211.

Récupérer de l'espace disque sur des machines virtuelles de clone lié

Dans vSphere 5.1 et supérieur, vous pouvez configurer la fonction de récupération d'espace disque pour les pools de postes de travail de clone lié. 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.

À mesure que les utilisateurs interagissent avec leur poste de travail, 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 leurs postes de travail.

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 » dans le document *Mises à niveau de View*.

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.

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 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 ou XP, 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**, puis 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 » dans le 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 des durées d'interruption pour les opérations ESXi sur des machines virtuelles View », page 211.

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 de View Composer Array Integration avec la technologie de snapshot NFS natif (VAAI)

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 clone lié. Cette fonction utilise la technologie de snapshot NFS natif pour cloner des machines virtuelles.

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 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.

- 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. VAAI n'est pas pris en charge sur les machines disposant de la version matérielle virtuelle 9 ou version ultérieure, car ces disques du système d'exploitation sont toujours à optimisation d'espace, même lorsque vous désactivez l'opération de récupération d'espace.
- 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 des durées d'interruption pour les opérations ESXi sur des machines virtuelles View

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.

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.

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

16

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 de View Agent, d'Horizon Client pour Windows et des fonctionnalités qui affectent les machines mono-utilisateur, les hôtes RDS ou le protocole d'affichage PCoIP.

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.

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 215.

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 215.

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 215.

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 16-1 décrit chaque paramètre de stratégie View.

Tableau 16-1. Règles de View

Règle	Description
Redirection multimédia (MMR)	Détermine si MMR est activé pour les systèmes client. MMR est un filtre de Microsoft DirectShow qui permet de transférer des données multimédias 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. La valeur par défaut est **Refuser**. Si les systèmes clients disposent de ressources insuffisantes pour gérer le décodage multimédia local, laissez le paramètre défini sur **Refuser**. MMR ne fonctionne pas correctement si le matériel d'affichage vidéo du système client ne prend pas en charge la superposition. 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. 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. 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. La valeur par défaut est **Autoriser** avec une priorité **Moyenne**.

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-View-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 VMware Horizon (avec View) à l'adresse http://www.vmware.com/go/downloadview.

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 16-2. Afficher les fichiers de modèle d'administration ADM et ADMX

Nom du modèle	Fichier de modèle	Description
configuration de View Agent	`vdm_agent.adm`	Contient des paramètres de stratégie liés aux composants d'authentification et d'environnement de View Agent. Reportez-vous à la section « Paramètres de modèle d'administration pour la configuration de View Agent », page 218.
Configuration d'Horizon Client	`vdm_client.adm`	Contient des paramètres de stratégie liés à Horizon Client pour Windows. 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. 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. Consultez le document *Administration de View*.
configuration commune de View	`vdm_common.adm`	Contient des paramètres de stratégie communs à tous les composants View. 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. Reportez-vous à la section « Paramètres de modèle d'administration pour les variables de session PCoIP de View », page 224.
Afficher les variables de session cliente PCoIP	`pcoip.client.adm`	Contient des paramètres de stratégie liés au protocole d'affichage PCoIP qui affectent Horizon Client pour Windows. Consultez le document *Utilisation de VMware Horizon Client pour Windows*.
Configuration de View Persona Management	`ViewPM.adm`	Contient des paramètres de stratégie liés à View Persona Management. Reportez-vous à la section « Paramètres de stratégie de groupe View Persona Management », page 276.
Afficher les services Bureau à distance	`vmware_rdsh.admx` `vmware_rdsh_server.admx`	Contient des paramètres de stratégie liés aux services Bureau à distance. Reportez-vous à la section « Utilisation de stratégies de groupe des services Bureau à distance », page 237.

Paramètres de modèle d'administration pour la configuration de View Agent

Le fichier de modèle d'administration de la configuration de View Agent (`vdm_agent.adm`) contient des paramètres de stratégie liés aux composants d'authentification et d'environnement de View Agent.

Ce fichier ADM est disponible dans un fichier groupé `.zip` nommé `VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip`, que vous pouvez télécharger à partir du site de téléchargement de VMware Horizon (avec View) à l'adresse http://www.vmware.com/go/downloadview.

Le tableau suivant décrit les paramètres de stratégie du fichier de modèle d'administration de configuration de View 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 16-3. Paramètres de modèle pour la configuration de View 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 View avec RDP. Lorsque ce paramètre est désactivé, View Agent autorise uniquement les connexions gérées par View via Horizon Client. 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)`. 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`. Ce paramètre est activé par défaut.
`AllowSingleSignon`	X		Détermine si une authentification unique (SSO) est utilisée pour connecter des utilisateurs à des postes de travail View. Lorsque ce paramètre est activé, l'utilisateur doit entrer uniquement ses informations d'identification lorsqu'il se connecte à Horizon Client. Lorsqu'il est désactivé, les utilisateurs doivent s'authentifier de nouveau lorsque la connexion à distance est effectuée. Ce paramètre est activé par défaut.
`CommandsToRunOnConnect`	X		Spécifie une liste de commandes ou de scripts de commande à exécuter lorsqu'une session est connectée pour la première fois. Pour plus d'informations, reportez-vous à « Exécution de commandes sur des postes de travail View », page 223.
`CommandsToRunOnDisconnect`	X		Spécifie la liste des commandes ou des scripts de commande à exécuter lorsqu'une session est déconnectée. Pour plus d'informations, reportez-vous à « Exécution de commandes sur des postes de travail View », page 223.

Tableau 16-3. Paramètres de modèle pour la configuration de View Agent (suite)

Paramètre	Ordinateur	Utilisateur	Propriétés
`CommandsToRunOnReconnect`	X		Spécifie une liste de commandes ou de scripts de commande à exécuter lorsqu'une session est reconnectée après une déconnexion. Pour plus d'informations, reportez-vous à « Exécution de commandes sur des postes de travail View », page 223.
`Connect using DNS Name`	X		Détermine si du Serveur de connexion View utilise le nom DNS à la place de l'adresse IP de l'hôte lors de la connexion. Ce paramètre est généralement activé lors d'une situation faisant appel à une traduction d'adresses réseau ou à un pare-feu dans laquelle Horizon Client ou le Serveur de connexion View ne peut pas utiliser directement l'adresse IP du poste de travail distant. Ce paramètre est désactivé par défaut.
`ConnectionTicketTimeout`	X		Spécifie la durée en secondes pendant laquelle le ticket de connexion View est valide. Les périphériques Horizon Client utilisent un ticket de connexion pour la vérification et l'authentification unique lorsqu'ils se connectent à View 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 View, 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. 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. MMR est un filtre de Microsoft DirectShow 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. MMR ne fonctionne pas correctement si le matériel d'affichage vidéo d'Horizon Client ne prend pas en charge la superposition. Ce paramètre est activé par défaut.

Tableau 16-3. Paramètres de modèle pour la configuration de View Agent (suite)

Paramètre	Ordinateur	Utilisateur	Propriétés
`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. 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. 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. 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. Ce paramètre est activé par défaut.
`Force MMR to use software overlay`	X		Détermine si la fonction de redirection multimédia (MMR) utilise une superposition logicielle à la place d'une superposition matérielle. MMR utilise le matériel d'affichage vidéo avec la prise en charge de la superposition pour de meilleures performances. Comme les superpositions matérielles n'existent en général que sur l'écran principal d'un système à plusieurs écrans, la vidéo n'est pas affichée quand elle est glissée de l'écran principal vers un écran secondaire. L'activation de ce paramètre force MMR à utiliser une superposition matérielle sur tous les écrans. Ce paramètre est désactivé par défaut.
`ShowDiskActivityIcon`	X		Ce paramètre n'est pas pris en charge dans cette version.
`Toggle Display Settings Control`	X		Détermine s'il convient de désactiver l'onglet **Paramètres** dans le panneau de configuration **Affichage** lorsqu'une session client utilise le protocole d'affichage PCoIP. Ce paramètre est activé par défaut.

Paramètres USB pour View Agent

Reportez-vous à la section « Paramètres USB du modèle d'administration de configuration de View Agent », page 186.

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.

View Agent écrit les informations de l'ordinateur client dans le chemin d'accès `HKCU\Volatile Environment` du registre système des postes de travail distants déployés sur des machines mono-utilisateur.

Pour les postes de travail distants déployés dans des sessions RDS, View 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` de View 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 223.

Tableau 16-4 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 16-4. 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) RDS	Windows, Linux, Mac, Android, iOS, Metro
`ViewClient_MAC_Address`	Adresse MAC du système client.	VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac, Android
`ViewClient_Machine_Name`	Nom de machine du système client.	VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac, Android, iOS, Metro
`ViewClient_Machine_Domain`	Domaine du système client.	VDI (machine mono-utilisateur) RDS	Windows, Metro
`ViewClient_LoggedOn_Username`	Nom d'utilisateur utilisé pour se connecter au système client.	VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac
`ViewClient_LoggedOn_Domainname`	Nom de domaine utilisé pour se connecter au système client.	VDI (machine mono-utilisateur) RDS	Windows, Metro 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) 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) 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) RDS	La valeur est envoyée directement par le Serveur de connexion View, elle n'est pas recueillie par Horizon Client.

Tableau 16-4. Informations sur le système client (suite)

Clé de Registre	Description	Postes de travail pris en charge	Systèmes clients pris en charge
`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) 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) 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) 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. Pour désactiver la synchronisation du fuseau horaire, activez le paramètre de stratégie de groupe `Disable Time Zone Synchronization` de View Agent.	VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac, Android, iOS
`ViewClient_Windows_Timezone`	Heure GMT standard. Pour désactiver la synchronisation du fuseau horaire, activez le paramètre de stratégie de groupe `Disable Time Zone Synchronization` de View Agent.	VDI (machine mono-utilisateur) RDS	Windows, Metro
`ViewClient_Broker_DomainName`	Nom de domaine utilisé pour s'authentifier auprès du Serveur de connexion View.	VDI (machine mono-utilisateur) 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) 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'`ID matériel du client unique` utilisé comme lien vers la clé de licence.	VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac, Android, iOS, Metro
`ViewClient_Displays.Number`	Spécifie le nombre de moniteurs utilisés actuellement par le client.	VDI (machine mono-utilisateur) 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) 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) RDS	Windows

Tableau 16-4. Informations sur le système client (suite)

Clé de Registre	Description	Postes de travail pris en charge	Systèmes clients pris en charge
`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) 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) RDS	Windows
`ViewClient_Mouse.NumButtons`	Spécifie le nombre de boutons pris en charge par la souris.	VDI (machine mono-utilisateur) 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) RDS	Windows
`ViewClient_Protocol`	Spécifie le protocole en cours d'utilisation.	VDI (machine mono-utilisateur) RDS	Windows, Linux, Mac, Android, iOS, Metro
`ViewClient_Language`	Spécifie la langue du système d'exploitation.	VDI (machine mono-utilisateur) 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 16-4 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` de View 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 modèle d'administration pour les variables de session PCoIP de View

Le fichier de modèle d'administration pour les variables de session PCoIP de View (`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–View–Extras–Bundle–x.x.x–yyyyyyy.zip`, que vous pouvez télécharger à partir du site de téléchargement de VMware Horizon (avec View) à l'adresse http://www.vmware.com/go/downloadview.

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 des variables de session 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.

Variables de la session générale PCoIP de View

Le fichier de modèle d'administration pour les variables de session PCoIP de View contient des paramètres de stratégie de groupe qui configurent des caractéristiques de session générale telles que la qualité d'image PCoIP, les périphériques USB et les ports réseau.

Tableau 16-5. Variables de la session générale PCoIP de View

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 : ■ **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.) ■ **Désactivé dans les deux sens** ■ **Activé dans les deux sens** ■ **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.) 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. Ce paramètre s'applique uniquement à View Agent. 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. Ce paramètre s'applique uniquement aux clients Windows et Linux lorsque la version View 5.0 ou ultérieure est installée pour Horizon Client, View Agent et le Serveur de connexion View. 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. Lorsque vous activez ce paramètre, vous pouvez configurer une taille de cache d'images client comprise entre 50 Mo minimum et 300 Mo maximum. La valeur par défaut est 250 Mo.
`Configure PCoIP event log cleanup by size in MB`	Active la configuration du nettoyage du journal des événements PCoIP par taille en Mo. 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. Lorsque cette stratégie est désactivée ou non configurée, la valeur par défaut du nettoyage du journal des événements par taille est de 100 Mo. 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.

Tableau 16-5. Variables de la session générale PCoIP de View (suite)

Paramètre	Description
`Configure PCoIP event log cleanup by time in days`	Active la configuration du nettoyage du journal des événements PCoIP par durée en jours. 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. Lorsque cette stratégie est désactivée ou non configurée, la valeur par défaut du nettoyage du journal des événements est de 7 jours. 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). 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. Lorsque ce paramètre est modifié lors d'une session PCoIP active, le nouveau paramètre prend effet immédiatement.

Tableau 16-5. Variables de la session générale PCoIP de View (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. 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. 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. La valeur **Qualité d'image minimale** ne peut pas dépasser la valeur **Qualité d'image initiale maximale**. 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. Ces valeurs de qualité d'image ne s'appliquent qu'à l'hôte léger et n'ont aucun effet sur un client léger. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, les valeurs par défaut sont utilisées. Lorsque ce paramètre est modifié lors d'une session PCoIP active, le nouveau paramètre prend effet immédiatement.

Tableau 16-5. Variables de la session générale PCoIP de View (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. Cocher l'une des cases désactive l'algorithme de cryptage associé. Vous devez activer au moins un algorithme. Ce paramètre s'applique 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 **Désactiver le cryptage AES-128-GCM** est toujours remplacée pour que le cryptage AES-128-GCM soit activé. 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. 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 16-5. Variables de la session générale PCoIP de View (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. 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 (|). 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. 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`**. Pour des règles de classe, utilisez l'un des formats suivants : **Autoriser tous les périphériques USB** — Format : **`23XXXXXX`** ; Exemple : **`23XXXXXX`** **Autoriser tous les périphériques USB avec un ID de classe spécifique** — Format : **`22`*`class`*`XXXX`** ; Exemple : **`22aaXXXX`** **Autoriser une sous-classe spécifique** — Format : **`21`*`class`*`–`*`subclass`*`XX`** ; Exemple : **`21aabbXX`** **Autoriser un protocole spécifique** — Format : **`20`*`class`*`–`*`subclass`*`–`*`protocol`** ; Exemple : **`20aabbcc`** 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`**. 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. Ce paramètre s'applique à View 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. Par défaut, tous les périphériques sont autorisés et aucun n'est interdit.

Tableau 16-5. Variables de la session générale PCoIP de View (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. 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. Vous pouvez spécifier un maximum de 15 canaux virtuels à utiliser dans des sessions PCoIP. 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`**. 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`**. 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. Le paramètre des canaux virtuels s'applique à l'agent et au client. Les canaux virtuels doivent être activés sur l'agent et sur le client pour que les canaux virtuels puissent être utilisés. 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 s'applique uniquement à l'agent. 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. 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. 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. Lorsque le paramètre `Configurer l'en-tête de transport PCoIP` est activé, les priorités de session de transport suivantes sont disponibles : ■ **Élevée** ■ **Moyenne** (valeur par défaut) ■ **Faible** ■ **Non défini** 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 16-5. Variables de la session générale PCoIP de View (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. 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. 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. 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`. Ce paramètre s'applique uniquement à View Agent. 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. 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. **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. 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. 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`. 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. Ce paramètre s'applique uniquement à View Agent. 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. 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. **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 16-5. Variables de la session générale PCoIP de View (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. 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. Ce paramètre s'applique uniquement à View Agent. 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. 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. Sur un système Windows XP ou Windows Vista, la console peut afficher une session PCoIP 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. Ce paramètre s'applique 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. 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. 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. Ce paramètre ne s'applique qu'à View Agent et au pilote audio Teradici. 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. Ce paramètre s'applique uniquement à View Agent.

Variables de bande passante de la session PCoIP de View

Le fichier de modèle d'administration pour les variables de session PCoIP de View contient des paramètres de stratégie de groupe qui configurent des caractéristiques de bande passante de la session PCoIP.

Tableau 16-6. 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. 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 attendues. Par exemple, avec une configuration VDI mono-utilisateur (une seule session PCoIP) qui se connecte via une connexion Internet de 4 Mbits/s, définissez cette valeur sur 4 Mbits (ou 10 % de moins) pour laisser de la marge au reste du trafic réseau. S'il est prévu que plusieurs sessions PCoIP partagent un lien, comprenant plusieurs utilisateurs VDI ou une configuration RDS, vous pouvez souhaiter régler le paramètre en conséquence. Toutefois, si vous diminuez cette valeur, cela limitera la bande passante maximale de chaque session active. La définition de cette valeur empêche l'agent d'essayer de transmettre à un débit supérieur à la capacité du lien, ce qui risque d'entraîner une perte de paquets excessive et une dégradation de l'expérience utilisateur. Cette valeur est symétrique. Elle force le client et l'agent à utiliser la plus faible des deux valeurs qui sont définies du côté du client et de l'agent. Par exemple, la définition d'une bande passante maximale de 4 Mbits/s force l'agent à transmettre à un débit plus faible, même si le paramètre est configuré sur le client. 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. La valeur par défaut lorsque ce paramètre n'est pas configuré est de 900000 kilobits par seconde. Ce paramètre s'applique à View 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. 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. 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. 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. Ce paramètre s'applique à View Agent et au client, mais il n'affecte que le point de terminaison sur lequel il est configuré. Lorsque ce paramètre est modifié lors d'une session PCoIP active, la modification prend effet immédiatement.

Tableau 16-6. 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. 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. 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. 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. Ce paramètre s'applique à View 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. Si ce paramètre est désactivé ou qu'il n'est pas configuré, le client utilise la valeur par défaut dans la négociation avec View Agent.

Tableau 16-6. 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. 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. 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. Ce paramètre s'applique uniquement à View Agent. Vous devez activer le son sur les deux points de terminaison avant que ce paramètre ne prenne effet. En outre, ce paramètre n'a pas d'effet sur l'audio USB. 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. Ce paramètre s'applique à View 4.6 et supérieur. Il n'a aucun effet sur les versions antérieures de View. 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. 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. 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. Lorsque ce paramètre est modifié lors d'une session PCoIP active, la modification prend effet immédiatement. Pour plus d'informations sur la fonction de développement sans perte PCoIP, reportez-vous à la section « Fonction de développement sans perte PCoIP de View », page 236.

Variables de la session PCoIP de View pour le clavier

Le fichier de modèle d'administration pour les variables de session PCoIP de View contient des paramètres de stratégie de groupe qui configurent des caractéristiques de session PCoIP affectant l'utilisation du clavier.

Tableau 16-7. 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. 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. Ce paramètre s'applique à View Agent uniquement et n'a aucun effet sur un client. 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). 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. 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. 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. Lorsque ce paramètre est désactivé ou qu'il n'est pas configuré, la séquence de touches Ctrl+Alt+Inser est utilisée comme SAS. Ce paramètre s'applique à View Agent uniquement et n'a aucun effet sur un client.

Fonction de développement sans perte PCoIP de View

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 `Désactiver le développement sans perte`. Reportez-vous à la section « Variables de bande passante de la session PCoIP de View », page 233.

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.

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 254.

Procédure

1 Téléchargez le fichier View GPO Bundle `.zip` à partir du site de téléchargement de VMware Horizon (avec View) à l'adresse http://www.vmware.com/go/downloadview.

  Le fichier se nomme `VMware-Horizon-View-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 copier les fichiers RDS ADMX sur votre hôte Active Directory ou RDS.

  a Copiez les fichiers `vmware_rdsh.admx` et `vmware_rdsh_server.admx` dans le dossier `C:\Windows\PolicyDefinitions` sur votre hôte Active Directory ou RDS.

  b (Facultatif) Si vous souhaitez localiser les paramètres de stratégie, copiez les fichiers ADML, `vmware_rdsh.adml` et `vmware_rdsh_server.adml` dans le sous-dossier approprié 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 > Règles > Modèles d'administration > Composants Windows > Services RDSH de View > Hôte de session Bureau à distance**.

4 (Facultatif) Configurez les paramètres de stratégie de groupe dans le dossier **Services RDSH de 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 16-8. 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. 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. 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.
	Par défaut, la virtualisation IP des services Bureau à distance est désactivée.
	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 :
	`explorer.exe`
	`mstsc.exe`
	Si vous désactivez ou si vous ne configurez pas ce paramètre de stratégie, la virtualisation IP des services Bureau à distance est désactivée.

Tableau 16-8. 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. 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. 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. 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. 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 16-9. 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. Si vous activez ce paramètre de stratégie, la planification de répartition de charge équilibrée du temps processeur est désactivée. 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 16-10. 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. 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). 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 16-11. 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. 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. 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 : 1 Serveurs de licences qui sont spécifiés dans l'outil Configuration d'hôte de session Bureau à distance 2 Serveurs de licences qui sont publiés dans les Services de domaine Active Directory 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 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. 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. Si vous activez ce paramètre de stratégie, ces notifications ne s'afficheront pas sur le serveur Hôte de session Bureau à distance. 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. Vous pouvez utiliser ce paramètre de stratégie pour sélectionner l'un des deux modes de licence : par utilisateur ou par périphérique.

Tableau 16-11. 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. 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. 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. 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 16-12. 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. **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**. 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. 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. 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. 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 16-12. 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. **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. 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. 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 16-12. 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. 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. 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. **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. 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. 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. 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. 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 16-12. Paramètres de stratégie de groupe des profils RDS (suite)

Paramètre	Description
	Remarques : 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. 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 16-13. 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. 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. 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 16-14. 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. 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. 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. 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. **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 16-15. 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. 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. Si l'état est défini sur Activé, les dossiers temporaires par session de l'utilisateur sont conservés lorsque celui ferme une session. 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. 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. **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. 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`. 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. 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. 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 2008 R2
- Postes de travail qui sont déployés 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 View 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`.

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`.

Dans Horizon 6.0.1 ou version ultérieure, les versions 32 bits et 64 bits de `TPVMGPoACmap.dll` sont disponibles dans un fichier `.zip` groupé nommé `VMware-Horizon-View-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 VMware Horizon (avec View) 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 de 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 250.
- 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 251.
- 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 254 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 View 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**. b Cliquez avec le bouton droit sur l'UO qui contient vos postes de travail View et sélectionnez **Propriétés**. c Sous l'onglet **Stratégie de groupe**, cliquez sur **Ouvrir** pour ouvrir le plug-in Gestion de stratégie de groupe. 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**. 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 `Mappage par connexion automatique d'imprimantes supplémentaires pour VMware View` pour mapper des imprimantes à des postes de travail distants.

`Mappage par connexion automatique d'imprimantes supplémentaires pour VMware View` est une table de traductions de noms qui identifie des imprimantes et définit les règles de traduction associées. Tableau 16-16 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 16-16. 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. Pour spécifier des adresses IP dans une plage spécifique, utilisez la notation suivante : ***ip_address-ip_address*** Par exemple : **`10.112.116.0-10.112.119.255`** Pour spécifier toutes les adresses IP dans un sous-réseau spécifique, utilisez la notation suivante : *ip_address/subnet_mask_bits* Par exemple : **`10.112.4.0/22`** Cette notation spécifie les adresses IPv4 utilisables comprises entre 10.112.4.1 et 10.112.7.254. Saisissez un astérisque pour inclure toutes les adresses IP.
`Client Name`	Règle de traduction spécifiant un nom d'ordinateur. Par exemple : **`Ordinateur de Marie`** 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 : ■ Les clients Windows utilisent des traits d'union : **`01-23-45-67-89-ab`** ■ Les clients Linux utilisent des deux-points : **`01:23:45:67:89:ab`** Saisissez un astérisque pour inclure toutes les adresses MAC.
`User/Group`	Règle de traduction spécifiant un nom d'utilisateur ou de groupe. Pour spécifier un utilisateur ou un groupe particulier, utilisez la notation suivante : *\\domain\user_or_group* Par exemple : **`\\mondomaine\Marie`** 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. Par exemple : **`PRINTER-2-CLR`** Le nom mappé n'a pas à correspondre au nom de l'imprimante sur le système client. 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.
`Printer Driver`	Nom du pilote qu'utilise l'imprimante. Par exemple : **`HP Color LaserJet 4700 PS`** **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_`**. Par exemple : **`IP_10.114.24.1`** Le port par défaut est 9001. Vous pouvez spécifier un port différent du port par défaut en ajoutant le numéro de port à l'adresse IP. Par exemple : **`IP_10.114.24.1:9004`**
`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 16-17 montre un exemple de deux lignes de tableau de traduction.

Tableau 16-17. 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**. b Cliquez avec le bouton droit sur l'unité d'organisation qui contient vos machines View et sélectionnez **Propriétés**. 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 254.

Procédure

1 Téléchargez le fichier View GPO Bundle `.zip` à partir du site de téléchargement de VMware Horizon (avec View) à l'adresse http://www.vmware.com/go/downloadview.

  Le fichier se nomme `VMware-Horizon-View-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 254.

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 des stratégies de groupe, développez les dossiers **Configuration de l'ordinateur**, **Règles**, **Modèles d'administration : Définitions de stratégie** et **Système**.

4 Double-cliquez sur le dossier **Stratégie de groupe**.

5 Dans le volet de droite, double-cliquez sur **Mode de traitement par boucle de rappel de la stratégie de groupe utilisateur**.

6 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.

7 Cliquez sur **OK** pour enregistrer vos modifications.

Configuration de profils d'utilisateur avec View Persona Management 17

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 sur les systèmes d'exploitation Windows XP SP3, Windows Vista, Windows 7 et Windows 8.

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 les systèmes de vos utilisateurs de Windows XP à Windows 7 ou Windows 8 et migrer vos utilisateurs d'ordinateurs physiques vers View pour la première fois.
- Dans un déploiement de View existant, vous pouvez effectuer une mise à niveau de postes de travail View Windows XP vers des postes de travail View Windows 7 ou Windows 8.
- 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.

Le Tableau 17-1 montre différents scénarios de migration et présente les tâches que vous devez effectuer dans chaque scénario.

Tableau 17-1. 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 :
Ordinateurs physiques Windows XP	Postes de travail View Windows 7 ou Windows 8	1 Configurez les postes de travail View Windows 7 ou Windows 8 avec View Persona Management pour vos utilisateurs. Reportez-vous à la section « Configuration d'un déploiement de View Persona Management », page 262. **Remarque** Ne restaurez pas les postes de travail View Windows 7 ou Windows 8 pour vos utilisateurs avant d'avoir effectué l'étape 2. 2 Exécutez l'utilitaire de migration de profil View V1 à V2. ■ Pour les profils source, spécifiez les profils locaux sur les ordinateurs physiques Windows XP. ■ Pour les profils de destination, spécifiez le référentiel de profils distant que vous avez configuré pour le déploiement de View. Pour plus d'informations, reportez-vous au document *Migration des profils d'utilisateur View*. 3 Autorisez vos utilisateurs à ouvrir une session sur leurs postes de travail View Windows 7 ou Windows 8.
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 : ■ View Persona Management ■ RTO Virtual Profiles ■ profils itinérants de Windows Dans ce scénario, les profils d'utilisateur d'origine doivent être conservés dans un référentiel de profils distant.	Postes de travail View Windows 7 ou Windows 8	1 Configurez les postes de travail View Windows 7 ou Windows 8 avec View Persona Management pour vos utilisateurs. Reportez-vous à la section « Configuration d'un déploiement de View Persona Management », page 262. **Remarque** Ne restaurez pas les postes de travail View Windows 7 ou Windows 8 pour vos utilisateurs avant d'avoir effectué l'étape 2. 2 Exécutez l'utilitaire de migration de profil View V1 à V2. ■ Pour les profils source, spécifiez le référentiel de profils distant pour les systèmes Windows XP. ■ Pour les profils de destination, spécifiez le référentiel de profils distant que vous avez configuré pour le déploiement de View. Pour plus d'informations, reportez-vous au document *Migration des profils d'utilisateur View* 3 Autorisez vos utilisateurs à ouvrir une session sur leurs postes de travail View Windows 7.

Tableau 17-1. 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. View Agent 5.*x* ne peut pas être installé sur les systèmes hérités.	Postes de travail View Windows XP	1 Configurez des postes de travail View Windows XP avec View Persona Management pour vos utilisateurs. Reportez-vous à la section « Configuration d'un déploiement de View Persona Management », page 262. 2 Installez le logiciel View Persona Management autonome sur les systèmes Windows XP. Reportez-vous à la section « Installer View Persona Management autonome », page 266. 3 Configurez les systèmes Windows XP hérités pour utiliser le même référentiel de profils distant que les postes de travail View. Reportez-vous à la section « Configurer un référentiel de profils d'utilisateur », page 263. 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 et les postes de travail View. Reportez-vous à la section « Ajouter le fichier de modèle d'administration de View Persona Management », page 267. 4 Restaurez vos postes de travail View Windows XP pour vos utilisateurs.
Ordinateurs physiques ou machines virtuelles Windows 7 ou Windows 8. View Agent 5.*x* ne peut pas être installé sur les systèmes hérités.	Postes de travail View Windows 7 ou Windows 8	1 Configurez les postes de travail View Windows 7 ou Windows 8 avec View Persona Management pour vos utilisateurs. Reportez-vous à la section « Configuration d'un déploiement de View Persona Management », page 262. 2 Installez le logiciel View Persona Management autonome sur les systèmes Windows 7 ou Windows 8. Reportez-vous à la section « Installer View Persona Management autonome », page 266. 3 Configurez les systèmes Windows 7 ou Windows 8 hérités pour utiliser le même référentiel de profils distant que les postes de travail View. Reportez-vous à la section « Configurer un référentiel de profils d'utilisateur », page 263. 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 et les postes de travail View. Reportez-vous à la section « Ajouter le fichier de modèle d'administration de View Persona Management », page 267. 4 Restaurez vos postes de travail View Windows 7 ou Windows 8 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 utilisateur, installez View 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 View 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 View 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 264.
- 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 264

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 17-2. 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 17-3. 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 View Agent avec l'option View Persona Management

Pour utiliser View Persona Management avec des postes de travail View, vous devez installer View Agent avec l'option d'installation de **View Persona Management** sur les machines virtuelles que vous utilisez pour créer des pools de postes de travail.

Pour un pool automatisé, vous installez View Agent avec l'option d'installation de **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 View 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.

Remarque Un utilisateur ne peut pas accéder au même profil si l'utilisateur bascule entre des postes de travail qui ont des profils d'utilisateur v1 et v2. Windows XP utilise les profils v1. Windows 8 et Windows 7 utilisent des profils v2.

Par exemple, si un utilisateur ouvre une session sur un poste de travail Windows XP puis sur un poste de travail Windows 7, la machine virtuelle Windows 7 ne peut pas lire le profil v1 qui a été créé lors de la session de poste de travail Windows XP.

Vous pouvez utiliser l'utilitaire de ligne de commande de migration de profil View pour migrer des profils Windows XP vers des profils Windows 7 ou Windows 8. Reportez-vous au document *Migration des profils d'utilisateur View*.

Prérequis

- Vérifiez que vous effectuez l'installation sur une machine virtuelle Windows 8, Windows 7, Windows Vista ou Windows XP. View Persona Management ne fonctionne pas sur des hôtes Microsoft RDS.

  L'installation de View 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 266.

- 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 View Agent avec l'option di'nstallation **View Persona Management**.
- Sur des machines virtuelles Windows XP, téléchargez et installez le service UPHClean (User Profile Hive Cleanup) de Microsoft sur le système d'exploitation client. Reportez-vous à la section « Installation de UPHClean sur des machines Windows XP qui utilisent View Persona Management », page 266.
- Familiarisez-vous avec l'installation de View Agent. Reportez-vous à la section « Installer View Agent sur une machine virtuelle », page 30 ou « Installer View Agent sur une machine non gérée », page 18.

Procédure

- Lorsque vous installez View 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 267.

Installation de UPHClean sur des machines Windows XP qui utilisent View Persona Management

Le service UPHClean (User Profile Hive Cleanup) de Microsoft garantit que les sessions utilisateur sont complètement terminées lorsqu'un utilisateur ferme une session. UPHClean nettoie les handles de clé de registre pouvant être isolés par d'autres processus et applications. Ce service permet de s'assurer que la ruche de registre de l'utilisateur est déchargée pour qu'elle puisse être chargée correctement et que le persona local puisse être supprimé.

Si vous configurez View Persona Management sur des machines virtuelles Windows XP, téléchargez et installez UPHClean dans le système d'exploitation client.

Vous pouvez télécharger le service UPHClean à l'emplacement suivant : http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=6676.

Le service UPHClean est inclus avec les systèmes d'exploitation Windows 7 et Windows Vista. Vous n'avez pas à installer le service sur ces systèmes d'exploitation.

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 8, Windows 7, Windows Vista ou Windows XP SP3. 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 » dans le 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 35.

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. b Acceptez les termes de licence VMware. c Cliquez sur **Installer**. Par défaut, View Persona Management est installé dans le répertoire `C:\Program Files\VMware\VMware View Persona Management`. d Cliquez sur **Terminer**.
Installation silencieuse	Ouvrez une invite de commande Windows sur la machine et tapez la commande d'installation sur une ligne. Par exemple : `VMware-personamanagement-y.y.y-xxxxxx.exe /s /v"/qn /l*v ""c:\persona.log"" ALLUSERS=1"` 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 253.

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 que View Agent est installé avec l'option de configuration de View Persona Management sur le système. Reportez-vous à la section « Installer View Agent avec l'option View Persona Management », page 265.
- Vérifiez que vous pouvez ouvrir une session en tant qu'administrateur sur le système.

Procédure

1 Téléchargez le fichier View GPO Bundle `.zip` à partir du site de téléchargement de VMware Horizon (avec View) à l'adresse http://www.vmware.com/go/downloadview.

   Le fichier se nomme `VMware-Horizon-View-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 270.

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 253.
- 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 que View 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 View Agent avec l'option View Persona Management », page 265.

Procédure

1. Téléchargez le fichier View GPO Bundle `.zip` à partir du site de téléchargement de VMware Horizon (avec View) à l'adresse http://www.vmware.com/go/downloadview.

   Le fichier se nomme `VMware-Horizon-View-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 277.
- 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 268.
- 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 269.

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).
Active Directory server (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 XP ou Windows Server 2003	Développez les dossiers suivants : **Modèles d'administration**, **Configuration de VMware View Agent**, **Gestion de persona**
Windows Vista et supérieur ou Windows Server 2008 et supérieur	Développez les dossiers suivants : **Modèles d'administration**, **Modèles d'administration classiques (ADM)**, **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 que View 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 View Agent avec l'option View Persona Management », page 265.
- 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 268 et « Configurer des stratégies View Persona Management », page 270.

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 View 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 si vous désinstallez View Agent complètement, les profils d'utilisateur locaux sont supprimés des machines des utilisateurs qui n'ont actuellement aucune session ouverte. Pour les utilisateurs qui ont une session actuellement ouverte, les profils d'utilisateur (2 occurrences) sont téléchargés à partir du référentiel de profils distants au cours du processus de 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 274.
- 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 275.
- 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 275.
- 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 277.

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 262.

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'objet 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)** apparaît uniquement dans Windows Vista et les versions suivantes et Windows Server 2008 et les versions suivantes.

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-View-Extras-Bundle-x.x.x-yyyyyyy.zip`, que vous pouvez télécharger à partir du site de téléchargement de VMware Horizon (avec View) à l'adresse http://www.vmware.com/go/downloadview.

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 17-4. Emplacement des paramètres de View Persona Management dans la fenêtre Stratégie de groupe

Système d'exploitation	Emplacement
Windows Vista et supérieur ou Windows Server 2008 et supérieur	**Configuration ordinateur** > **Modèles d'administration** > **Modèles d'administration classiques (ADM)** > **Configuration de VMware View Agent** > **Persona Management**
Windows XP ou Windows Server 2003	**Configuration ordinateur** > **Modèles d'administration** > **Configuration de VMware View Agent** > **Persona Management**

Les paramètres de stratégie de groupe sont contenus dans ces dossiers :

- Roaming & Synchronization (Itinérance et synchronisation)
- 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. Lorsque ce paramètre est activé, View Persona Management gère des profils d'utilisateur. 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. 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. Lorsque ce paramètre est activé, vous pouvez utiliser **Partager un chemin d'accès** pour déterminer l'emplacement du référentiel de profils d'utilisateur. 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. Par exemple : `\\server.domain.com\VPRepository` 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%` 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. 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 263. Par défaut, le chemin de profil d'utilisateur Active Directory est utilisé. 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. 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. Vous pouvez également cocher une case pour supprimer les dossiers de paramètres locaux de chaque utilisateur lorsque le profil d'utilisateur est supprimé. Lorsque vous utilisez Windows 8, Windows 7 ou Windows Vista, cocher cette case supprime le dossier `AppData\Local`. Dans Windows XP, cocher cette case supprime le dossier `Paramètres locaux`. 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 272. 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. Pour Windows 8, Windows 7 ou Windows Vista, cette stratégie affecte le dossier `AppData\Local`. Pour Windows XP, cette stratégie affecte le dossier `Local Settings (Paramètres locaux)`. 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. 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. Spécifiez des chemins liés à la racine du profil local. Ne spécifiez pas de lecteur dans un nom de chemin d'accès. Par exemple : `Application Data\Microsoft\Certificates` 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. Les chemins de dossier sélectionnés doivent résider dans les dossiers que vous spécifiez dans le paramètre **Fichiers et dossiers à précharger**. 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. 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**. 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**. Les chemins de dossier sélectionnés doivent résider dans les dossiers que vous spécifiez dans le paramètre **Synchronisation de profils itinérants de Windows**. 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. 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. Spécifiez des chemins liés à la racine du profil local. Ne spécifiez pas de lecteur dans un nom de chemin d'accès. 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**. Les chemins de dossier sélectionnés doivent résider dans les dossiers que vous spécifiez dans le paramètre **Fichiers et dossiers exclus du déplacement**. 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. Lorsque l'opération est terminée, une notification contextuelle apparaît 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`. **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. 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. Reportez-vous à la section « Gérer les profils d'utilisateur sur les ordinateurs portables autonomes », page 275.
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. 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. 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. 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**. Les chemins de dossier sélectionnés doivent résider dans les dossiers que vous spécifiez dans le paramètre **Dossiers à télécharger en arrière-plan**. 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. 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. 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. 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 273.
- 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 sur *nom de dossier*** 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 17-5.

  Pour les dossiers redirigés existants, consultez « Octroi d'un accès à des dossiers redirigés existants à des administrateurs de domaine », page 282.

Vous pouvez spécifier des chemins de dossier qui sont exclus de la redirection de dossier. Reportez-vous à la section Tableau 17-5.

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

Certains dossiers sont disponibles uniquement dans les systèmes d'exploitation Windows Vista et supérieurs.

Tableau 17-5. 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. 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. Dans certains scénarios, des fichiers et des dossiers spécifiques doivent rester dans le profil d'utilisateur local. 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**. 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**. 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**. 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 17-5.

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. 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. 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. 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. Par défaut, cette valeur est de 50 Mo. 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. 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.

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. Sur des ordinateurs Windows 8 et Windows 7, le chemin d'accès par défaut est `ProgramData\VMware\VDM\logs\`*`filename`*. Sur des ordinateurs Windows XP, le chemin d'accès par défaut est *`All Users`*`\Application Data\VMware\VDM\logs\`*`filename`*. 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. Par défaut, les messages de journalisation sont envoyés vers le fichier journal.
Logging flags (Indicateurs de journalisation)	Détermine les types de messages à journaliser. Lorsque ce paramètre est configuré, vous pouvez sélectionner un ou tous les types de message de journalisation à générer : ■ messages d'erreur de journalisation ; ■ messages d'information de journalisation ; ■ messages de débogage de journalisation. Par défaut, des types de message de journalisation d'erreur et d'information sont générés.
Debug flags (Indicateurs de débogage)	Détermine les types de messages de débogage à journaliser. View Persona Management traite les messages de débogage comme il traite les messages de journalisation. Lorsque ce paramètre est activé, vous pouvez sélectionner un ou tous les types de message de débogage à générer : ■ messages d'erreur de débogage ; ■ messages d'information de débogage ; ■ messages de port de débogage ; Par défaut, aucun message de débogage n'est généré.
Profondeur d'historique des journaux	Détermine le nombre de fichiers journaux d'historique conservés par View Persona Management. Vous pouvez conserver entre un et dix fichiers journaux d'historique au maximum. 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. 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. Par défaut, le fichier journal n'est pas téléchargé sur le partage réseau.

Dépannage de machines et de pools de postes de travail 18

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 292.
- 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 de View 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 de View 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

  « Des machines virtuelles sont bloquées dans l'état d'approvisionnement », page 290.
- 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 (RDP ou PCoIP) n'est pas bloqué. Reportez-vous à la section « Problèmes de connexion entre des machines et des instances du Serveur de connexion View », page 298.
- 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.

Résolution des problèmes de création de pool de postes de travail

Vous pouvez utiliser plusieurs procédures pour le diagnostic et la résolution de problèmes liés à la création de pools de postes de travail.

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 clone lié échoue et l'erreur suivante se produit : `La machine virtuelle avec la spécification entrée existe déjà`
- Dans View Administrator, les machines de clone lié sont bloquées dans un état `Suppression`. Vous ne pouvez pas redémarrer la commande Supprimer dans View Administrator, car les machines sont déjà dans l'état `Suppression`.

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` se trouve sur l'ordinateur sur lequel View Composer est installé dans l'emplacement suivant :

- Ordinateurs 32 bits : *`Install_drive`*`\Program Files\VMware\VMware View Composer`
- Ordinateurs 64 bits : *`Install_drive`*`\Program Files (x86)\VMware\VMware View Composer`

IMPORTANT Seuls les administrateurs View Composer expérimentés doivent utiliser 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 machine virtuelle de View LDAP, consultez l'article 2015112 de la base de connaissances VMware : *Manually deleting linked clones or stale virtual desktop entries from VMware View Manager 4.5 and later (Supprimer manuellement des clones liés ou des entrées de poste de travail virtuel périmées de VMware View Manager 4.5 et supérieur).*

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 expérimentés de View Composer doivent utiliser l'utilitaire `SviConfig`. Cet utilitaire est conçu pour résoudre des problèmes liés au service View Composer.

L'utilitaire `SviConfig` se trouve dans l'emplacement suivant sur l'ordinateur sur lequel View Composer est installé :

- Ordinateurs 32 bits : *`Install_drive`*`\Program Files\VMware\VMware View Composer`
- Ordinateurs 64 bits : *`Install_drive`*`\Program Files (x86)\VMware\VMware View Composer`

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 vous ne définissez pas ce paramètre, l'authentification Windows est utilisée.
- `Password (Mot de passe)`. Mot de passe de l'utilisateur qui se connecte à la base de données. Si vous ne définissez pas ce paramètre et que l'authentification Windows n'est pas utilisée, un message demande ensuite d'entrer le mot de passe.
- `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.

Effectuez ces étapes :

1 Redémarrez le service View Composer.

2 Dans une invite de commande Windows sur l'ordinateur de View Composer, exécutez la commande `SviConfig FindUnusedReplica` suivante :

```
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.

Les clones liés Windows XP ne parviennent pas à joindre le domaine

Les machines virtuelles de clone lié Windows XP risquent de ne pas parvenir à joindre le domaine si votre service Active Directory s'exécute sur Windows Server 2008.

Problème

Lorsque des machines de clone lié sont provisionnées, les clones liés ne parviennent pas à joindre le domaine. View Administrator affiche des messages d'erreur d'approvisionnement de View Composer. Par exemple :

```
5/17/10 3:11:50 PM PDT: View Composer agent initialization state error (18): Failed to join the
domain (waited 565 seconds) (5/17/10 3:11:50 PM PDT : erreur d'état d'initialisation de l'agent
View Composer (18) : impossible de joindre le domaine (attendu 565 secondes))
```

Cause

Ce problème peut se produire si votre Active Directory s'exécute sur Windows Server 2008. La compatibilité descendante du contrôleur de domaine en lecture seule Windows Server 2008 (RODC) avec des machines virtuelles
Windows XP n'est pas possible.

Solution

1 Recherchez dans le journal de View Composer le message d'erreur suivant :

```
0x4f1: The system detected a possible attempt to compromise security. Please ensure that you can contact the server that authenticated you. (0x4f1 : le système a détecté une tentative possible de compromission de la sécurité. Vérifiez que vous pouvez contacter le serveur qui vous a authentifié.)
```

Par défaut, le fichier journal de View Composer est généré dans le répertoire `Temp` de Windows : `C:\Windows\Temp\vmware-viewcomposer-ga-new.log`

2 Sur la machine virtuelle parente, appliquez la mise à jour de compatibilité du contrôleur de domaine en lecture seule Windows Server 2008 pour Windows XP.

Consultez l'article 944043 du support Microsoft à l'adresse suivante : http://support.microsoft.com/kb/944043/en-us.

3 Prenez un snapshot de la machine virtuelle parente mise à jour.

4 Recomposez les machines de clone lié à partir de la machine virtuelle parente mise à jour et du snapshot.

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 18-1 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 18-1. Erreurs d'approvisionnement de View Composer

Erreur	Description
0	La règle a été appliquée correctement. **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.

Tableau 18-1. Erreurs d'approvisionnement de View Composer (suite)

Erreur	Description
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. 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. PnP monte jusqu'à trois disques, en fonction de la configuration du pool : ■ Disque persistant de View Composer ■ Disque non persistant pour rediriger des fichiers temporaires et d'échange du système d'exploitation client ■ 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. 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.
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. Cette erreur peut être temporaire. Si le clone lié joint le domaine, le mot de passe est correct. 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.

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 View agent and Connection Server (Une erreur d'approvisionnement s'est produite pour la machine Machine_Name : erreur de personnalisation due à une absence de communication réseau entre l'agent View et le serveur de connexion)`
- `Provisioning error occurred on Pool Desktop_ID because of a networking problem with a View Agent (Une erreur d'approvisionnement s'est produite sur le pool Desktop_ID à cause d'un problème de réseau avec un View 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, que View 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 ou l'URL externe du tunnel sécurisé est configurée pour pointer vers un hôte du serveur de sécurité ou du Serveur de connexion View différent. Lorsque vous configurez ces deux URL externes sur un hôte du serveur de sécurité ou du Serveur de connexion View, les deux URL externes doivent être des adresses de 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.

Port	Description
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, activez PCoIP Secure Gateway et assurez-vous que l'URL externe PCoIP est correctement configurée.
  a Cliquez sur **Configuration de View > Serveurs**.
  b Sélectionnez le serveur de sécurité dans l'onglet **Serveurs de sécurité** ou l'instance du Serveur de connexion View dans l'onglet **Serveurs de connexion**, puis 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 Dans la zone de texte **URL externe PCoIP**, assurez-vous que l'URL contient l'adresse IP externe de l'instance du serveur de sécurité ou du Serveur de connexion View à laquelle 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 l'**URL externe PCoIP** et l'**URL externe** du tunnel sécurisé sont les adresses que les systèmes client utilisent pour atteindre cet hôte.

    Par exemple, si vous configurez un hôte du Serveur de connexion View, ne spécifiez pas d'**URL externe PCoIP** pour cet hôte ni d'**URL externe** du tunnel sécurisé pour un serveur de sécurité couplé.
  f Cliquez sur **OK**.
- 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 View agent and Connection Server (Une erreur d'approvisionnement s'est produite pour la machine Machine_Name : erreur de personnalisation due à une absence de communication réseau entre l'agent View et le serveur de connexion)`
- `Provisioning error occurred on Pool Desktop_ID because of a networking problem with a View Agent (Une erreur d'approvisionnement s'est produite sur le pool Desktop_ID à cause d'un problème de réseau avec un View 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, que View 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 180.
- La redirection USB n'est pas prise en charge pour les systèmes Windows 2008 ou pour les postes de travail distants sur hôtes de session Bureau à distance.
- 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 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 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 http://kb.vmware.com/kb/1011600.
- Windows Mobile Device Center peut empêcher la redirection de périphériques USB pour des sessions RDP. Reportez-vous à 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 http://kb.vmware.com/kb/1022076.
- Pour certains périphériques audio, vous devrez éventuellement modifier les paramètres de règle ou de Registre. Reportez-vous à 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 http://kb.vmware.com/kb/1022836.
- Un processus ou un service sur le système local a ouvert le périphérique avant votre connexion au poste de travail distant.
- Un périphérique USB redirigé arrête de fonctionner si vous reconnectez une session de poste de travail, même si le poste de travail 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 de poste de travail.
- 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 178.
- 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.

Résolution des problèmes GINA sur des machines Windows XP

Sur les machines Windows XP, des problèmes peuvent se produire avec le chaînage de fichiers de bibliothèque de liens dynamiques (dll) GINA (Graphical Identification and Authentication) de VMware View.

Problème

Les problèmes suivants peuvent se produire sur des machines Windows XP :

- Une machine ne démarre pas
- Lorsqu'une machine démarre ou s'arrête, l'erreur suivante s'affiche : `Cannot start gina.dll module. A required component is missing: gina.dll. Please install the application again. (Impossible de démarrer le module gina.dll. Un composant requis est manquant : gina.dll. Veuillez installer de nouveau l'application.)`
- Lorsque vous démarrez une machine, une invite d'ouverture de session inattendue s'affiche
- Vous ne pouvez pas ouvrir de session sur votre machine

Cause

Des problèmes de démarrage et d'ouverture de session peuvent se produire sur des machines Windows XP lorsque les fichiers `dll` GINA de View ne sont pas chaînés correctement avec des dll GINA tierces susceptibles de résider sur les machines virtuelles.

Pour vous assurer que le GINA est chaîné correctement, vous devez configurer le GINA `WinLogon` pour qu'il s'agisse du GINA View et vous assurer que le fichier `vdmGinaChainDLL` est créé et qu'il contient les GINA tiers.

Si vous n'avez pas installé de logiciel qui chaîne vers un GINA différent, le fichier par défaut est `msgina.dll`, qui se trouve à `%systemroot%\system32\msgina.dll` sur la machine virtuelle.

Solution

1 Ouvrez une session sur la machine virtuelle parente, le modèle de machine virtuelle ou la machine View.

2 Cliquez sur **Démarrer > Exécuter**, tapez **`Regedit`** et appuyez sur Entrée.

3 Recherchez la clé de Registre Windows suivante :

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Current Version\Winlogon\GinaDLL
```

4 Assurez-vous que la clé `GinaDLL` possède la valeur suivante :

install_directory\VMware\VMware View\Agent\bin\wsgina.dll

install_directory est le chemin où vous avez installé View Agent.

5 Si la valeur de chaîne `vdmGinaChainDLL` n'existe pas, créez-la.

a Recherchez la clé de Registre suivante :

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\Current Version
```

b Créez la clé `vdmGinaChainDLL`.

6 Placez les noms `dll` GINA tiers dans la clé `vdmGinaChainDLL`.

7 Si vous rencontrez toujours des problèmes avec les machines Windows XP, assurez-vous qu'aucune clé GINA spécifique du fournisseur n'est chargée dans le Registre.

Si des clés GINA tierces sont chargées, le GINA de chaînage peut toujours appeler le GINA par défaut, `msgina`. Certains produits de gestion de réseau et de logiciel de sécurité placent leurs fichiers `dlls` de remplacement GINA dans leurs propres répertoires d'installation, dans des chemins de Registre tels que le suivant :

```
HKEY_LOCAL_MACHINE\Software\Vendor_ID_or_Name\GINA_key_reference\GINA_Load_Instruction = msgina
```

Supprimez ces clés GINA de l'emplacement spécifique du fournisseur et placez-les dans la clé `vdmGinaChainDLL`.

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.

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

N

O

P

Q

R

S